Citrix Analytics für Sicherheit

Machine translated content

Disclaimer

Die offizielle Version dieses Inhalts ist auf Englisch. Für den einfachen Einstieg wird Teil des Inhalts der Cloud Software Group Dokumentation maschinell übersetzt. Cloud Software Group hat keine Kontrolle über maschinell übersetzte Inhalte, die Fehler, Ungenauigkeiten oder eine ungeeignete Sprache enthalten können. Es wird keine Garantie, weder ausdrücklich noch stillschweigend, für die Genauigkeit, Zuverlässigkeit, Eignung oder Richtigkeit von Übersetzungen aus dem englischen Original in eine andere Sprache oder für die Konformität Ihres Cloud Software Group Produkts oder Ihres Diensts mit maschinell übersetzten Inhalten gegeben, und jegliche Garantie, die im Rahmen der anwendbaren Endbenutzer-Lizenzvereinbarung oder der Vertragsbedingungen oder einer anderen Vereinbarung mit Cloud Software Group gegeben wird, dass das Produkt oder den Dienst mit der Dokumentation übereinstimmt, gilt nicht in dem Umfang, in dem diese Dokumentation maschinell übersetzt wurde. Cloud Software Group kann nicht für Schäden oder Probleme verantwortlich gemacht werden, die durch die Verwendung maschinell übersetzter Inhalte entstehen können.

Contents

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Was ist neu

June 18, 2024

Das Ziel von Citrix besteht darin, Citrix Analytics Kunden neue Funktionen und Produktaktualisierungen bereitzustellen, sobald sie verfügbar sind. Neue Releases bieten größeren Wert, daher gibt es keinen Grund, Updates zu verzögern.

Der Prozess ist für die Kunden transparent. Erste Updates werden nur auf interne Sites von Citrix angewendet und erst danach schrittweise auf Kundenumgebungen. Die schrittweise Bereitstellung von Updates in Wellen trägt dazu bei, die Produktqualität zu gewährleisten und die Verfügbarkeit zu maximieren.

15. April 2024

Neuer zusammenfassender Bericht

Sie haben jetzt die Möglichkeit, mehrere Berichte in einem einzigen zusammenfassenden Bericht zu konsolidieren, der für den gewünschten Zeitraum geplant werden kann. Mit dieser neuen Funktion stellen Sie Ihrem Publikum nur die erforderlichen grafischen Informationen zur Verfügung. Weitere Informationen finden Sie unter Zusammenfassender Bericht.

29. Januar 2024

Aktualisierungen im Feld “Workspace-App-Status”

- **Self-Service-Suche**: Sie können jetzt Abfragen durchführen, um den Support-Status einer Workspace App-Version zu ermitteln, indem Sie das neu eingeführte Feld **Workspace-App-Status** für die **Citrix Apps and Desktops**-Datenquelle verwenden.
- **Benutzer**: Die Spalte **Workspace-App-Status** wurde entfernt.

Weitere Informationen finden Sie unter Self-Service-Suche nach Apps und Desktops.

25. Januar 2024

Inkonsistenzen in der CAS-Benutzeroberfläche werden optimiert

Die folgenden Probleme wurden in der **Self-Service-Suchfunktion** für die Datenquelle **Apps and Desktops** behoben:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Ereignisse, die zuvor in einer Sitzung nicht in der richtigen Reihenfolge angezeigt wurden, werden jetzt korrekt angezeigt.
- Die Standardspalten wurden aktualisiert.

24. Januar 2024

Verbesserte Benutzerprofilereignisse in SIEM-Umgebungen

Zu den Benutzerprofilereignissen, die in Ihre SIEM-Umgebungen exportiert wurden, gehören jetzt:

- Einblicke in IP-Adressen
- Standortinformationen zu Citrix Virtual Apps and Desktops und Citrix DaaS (ehemals Citrix Virtual Apps and Desktops Service)

Mit diesen neuen Verbesserungen können Sie die IP-Adresse des Clients identifizieren, die für den Zugriff auf die Daten Ihres Unternehmens verwendet wird, und Informationen zum Benutzerstandort sowohl von Citrix Virtual Apps and Desktops als auch von Citrix DaaS sammeln.

Weitere Informationen finden Sie unter Risikoerkenntnisdaten für SIEM.

01. Dezember 2023

Seite mit Admin-E-Mail-Einstellungen für wöchentliche E-Mail- und SIEM-Benachrichtigungen

Mit der neuen Funktion **Admin-E-Mail-Einstellungen** können Sie benutzerdefinierte Verteilerlistenempfänger für Systemwarnungen konfigurieren. Diese Erweiterung stellt sicher, dass Administratoren nur die Systemwarnungen erhalten, die für sie relevant sind.

Weitere Informationen finden Sie unter E-Mail-Einstellungen für Administratoren.

Benutzer-Dashboard —Neuer Zeitfilter für die Anzahl der aktiven Benutzer und Aktualisierung des Übersichtsbereichs

Mit dem neuen Zeitfilter im **Benutzer-Dashboard** können Sie die Gesamtzahl der aktiven Benutzer in Ihrer Organisation für einen bestimmten Zeitraum anzeigen und ändern, wobei die Datenquellen berücksichtigt werden, für die Sie Citrix Analytics aktiviert haben.

Der erweiterte **Übersichtsbereich** im **Benutzer-Dashboard** zeigt die Gesamtzahl der Benutzer in Ihrer Organisation sowie die Anzahl der aktiven und inaktiven Benutzer an, die derzeit angemeldet sind.

Weitere Informationen finden Sie unter Benutzer-Dashboard.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Verbesserte benutzerdefinierte Berichte

- Sie können jetzt benutzerdefinierte Berichte mithilfe der in Citrix Analytics for Security verfügbaren Ereignisse und Erkenntnisse erstellen und planen. Benutzerdefinierte Berichte helfen Ihnen, Informationen von besonderem Interesse zu extrahieren und die Daten grafisch zu organisieren.
- Sie können jetzt die erweiterten Funktionen der Plattform für benutzerdefinierte Berichte verwenden, zu denen abfragebasierte Self-Service-Suchberichte, Vorlagen, bessere Visualisierungen, die Abdeckung aller Datenquellen und Metriken, die Planung von Berichten und das Exportieren von PDF-Dateien gehören.

Weitere Informationen finden Sie unter Benutzerdefinierte Berichte.

30. November 2023

Entfernung aller ShareFile-Funktionen in Citrix Analytics

Die folgenden ShareFile-Erkennungsfunktionen wurden entfernt:

- Links teilen
- Assoziierte Risikoindikatoren
- Richtlinien mit ihren Vorkommen
- Datenexportkonfigurationen für Content Collaboration
- Content Collaboration-Berichte
- Content Collaboration-Datenquelle für die Suche
- Gespeicherte Suchanfragen in Content Collaboration
- Datenquelle für Content Collaboration.

Die Entfernung dieser Funktionen kann zu einer vorübergehenden Inkonsistenz der Risikobewertung und der Benutzerzeitpläne führen. Alle anderen Funktionen von Citrix Analytics bleiben unverändert.

Erfahren Sie, wie ShareFile den Zugriff auf Sicherheitskontrollen direkt von ShareFile.com aus vereinfacht .

22. September 2023

Citrix Secure Browser-Datenquelle im benutzerdefinierten Indikator

Sie können jetzt Risikoindikatoren für die Citrix Secure Browser-Datenquelle erstellen, um die Aktivitäten eines Benutzers im Secure Browser zu verfolgen. Weitere Informationen finden Sie unter Benutzerdefinierte Indikatoren.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Erweiterung der wöchentlichen E-Mail mit SIEM-Datenexport

Die wöchentliche E-Mail wurde verbessert, um einen tieferen Einblick in die Sicherheitslage Ihres Unternehmens zu erhalten, indem der SIEM-Datenexport aktiviert wurde. Sie können jetzt mehr Datenquellen einbinden und aktivieren, um eine Vielzahl von Ereignissen in der Umgebung Ihrer Benutzer zu ermitteln. Die wöchentliche E-Mail enthält die folgenden Neuzugänge:

- Der Abschnitt mit der Datenübersicht zeigt den Status des Datenverbrauchs in der SIEM-Umgebung.
- Empfehlungen für Datenexporte basierend auf dem Verbrauchsstatus des Datenexports.

Weitere Informationen finden Sie unter Wöchentliche E-Mail-Benachrichtigung.

Verwendung der benutzerdefinierten Benachrichtigungseinstellungen des Administrators in E-Mails

Citrix Analytics for Security berücksichtigt jetzt die Benachrichtigungseinstellungen, die von benutzerdefinierten Administratoren in Citrix Cloud festgelegt wurden. Diese Erweiterung bietet benutzerdefinierten Administratoren mehr Flexibilität bei der Verwaltung ihrer Benachrichtigungseinstellungen. Diese Einstellung wird auch beim Versenden von Benachrichtigungs-E-Mails wie wöchentlichen E-Mails, Aktions-E-Mails für Administratoren benachrichtigen und Benachrichtigungen für Datenexporte genutzt.

Weitere Informationen finden Sie unter Administratorrollen für Security Analytics verwalten.

04. Juli 2023

Unterstützung von OR-Operatoren in Self-Service Search und Custom Indicator

Der **OR-Operator** ist jetzt in den Funktionen **Self-Service-Suche** und **Benutzerdefinierter Risikoindikator** verfügbar. Sie können den **OR-Operator** in Suchansichten wie Self-Service-Suchen und Abfragen mit benutzerdefinierten Indikatoren verwenden.

Weitere Informationen finden Sie unter Unterstützte Operatoren in Suchabfragen.

15. Juni 2023

VDA-Telemetrie in der Zwischenablage aktivieren

Ein Ereignis namens VDA.Clipboard wird ausgelöst, wenn Sie einen Zwischenablagevorgang in Citrix Apps and Desktops starten. Diese Zwischenablageprotokolle enthalten wichtige Informationen wie

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

den VDA-Namen, die Größe der Zwischenablage, den Formattyp der Zwischenablage, die Client-IP, den Vorgang in der Zwischenablage, die Betriebsrichtung der Zwischenablage und ob der Vorgang in der Zwischenablage zulässig war. Die VDA-Zwischenablage-Ereignisattribute sind auch in den Workflows Self-Service-Suche und Benutzerdefinierte Risikoindikatoren verfügbar.

- **Self-Service-Suche**: Sie können Berichte erstellen, Abfragen speichern und die VDA.Clipboard-Ereignisse zusammen mit all ihren Attributdetails überprüfen.
- **Benutzerdefinierte Risikoindikatoren**: Attribute für die Ereignisse in der VDA-Zwischenablage sind mit dem Workflow "Benutzerdefinierte Indikatoren"verfügbar. Sie können diese Ereignisschlüssel/Wert-Paare verwenden, um benutzerdefinierte Indikator-Trigger zu konfigurieren und automatisierte Richtlinien mit Aktionen einzurichten.

Sie können die Richtlinie **zur Sicherheitsüberwachung in der Zwischenablage** verwenden, um die Telemetrie der Zwischenablage und die Übertragung von Zwischenablageprotokollen an Citrix Analytics for Security zu aktivieren. Standardmäßig ist diese Richtlinie aktiviert. Um dies zu deaktivieren, navigieren Sie zur Richtlinienseite und deaktivieren Sie sie, um die Erfassung von Daten von den VDAs zu beenden.

Weitere Informationen finden Sie unter Telemetrie in der Zwischenablage für Citrix DaaS aktivieren.

14. Juni 2023

Verfügbarkeit von App-Lebenszyklus- und Registrierungsereignissen für die Sitzungsaufzeichnung in Citrix Analytics for Security

Die folgenden **App-Lifecycle** - und **Registrierungsereignisse** aus der **Sitzungsaufzeichnung** sind jetzt in Citrix Analytics for Security verfügbar:

- Citrix.EventMonitor.RegistryChange
- Citrix.EventMonitor.SessionLaunch
- Citrix.EventMonitor.SessionEnd
- Citrix.EventMonitor.Clipboard
- Citrix.EventMonitor.FileTransfer

Sie können diese Ereignisse anzeigen, benutzerdefinierte Indikatoren erstellen und diese Erei#gnisse in Ihre SIEM-Umgebungen exportieren.

Weitere Informationen finden Sie unter Ereignistypen und unterstützte Felder.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

08. Juni 2023

Behobene Probleme

- Einige Sitzungsanmeldeereignisse, die an Citrix Analytics for Security gesendet werden, haben keinen Benutzernamen. Dies führt dazu, dass die Spalte mit dem Benutzernamen für einige Ereignisse auf der Benutzeranmeldeseite von Self Service Search und Access Assurance als **NA** angezeigt wird. Manchmal führt dies auch dazu, dass eine eindeutige Benutzerzahl Null ist, obwohl die Gesamtzahl der Anmeldungen im Diagramm der Access Assurance-IP-Registrierungsorganisationen ungleich Null ist, wenn die Daten für einen kleinen Zeitraum wie **Letzte 1 Stunde** oder **Letzter 1 Tag**angezeigt werden. Dieses Problem ist jetzt behoben. [CAS-70954]
- Bei der Self-Service-Suche nach Apps und Desktops wird für Session.Logon- und Session.End-Benutzerereignisse die Dimension App-Name in Suchabfragen mit Bereitstellungsgruppennamen und nicht mit dem Namen der gestarteten Anwendung oder des gestarteten Desktops aufgefüllt, was für Administratoren irreführend sein kann. Die Dimension App-Name ist für Abfragen zu App.Start/App.End-Ereignissen nützlicher, da sie auf die Anwendungen verweist, die gestartet werden. Weitere Informationen finden Sie unter Self-Service-Suche nach Apps und Desktops. Dieses Problem ist jetzt behoben. [CAS-67968]
- Wenn Ihr Unternehmen in Citrix Cloud in der Heimatregion **Asien-Pazifik-Süd** eingebunden ist, sind die Content Collaboration-Ereignisse in Ihren Citrix Analytics-Mandanten nicht sichtbar. Dieses Problem ist jetzt behoben. [CAS-62317]
- Nur wenige Versionen der Citrix Workspace-App und des Citrix Receiver-Clients senden keine bestimmten Ereignisse an Citrix Analytics. Daher kann Citrix Analytics keine Erkenntnisse liefern und Risikoindikatoren für diese Ereignisse generieren. Dieses Problem ist jetzt behoben. Weitere Informationen finden Sie unter Test 6: Werden die Ereignisse für virtuelle Apps und Desktops an Analytics übertragen?. [CAS-16151]

29. Mai 2023

Citrix Analytics-Add-On für Splunk jetzt auf der Splunk Cloud Platform verfügbar

Splunk Integration for Citrix Analytics verwendet das Citrix Analytics Add-On für Splunk, um eine Verbindung zur Analyseumgebung herzustellen und geschäftskritische Daten in Ihre Splunk-Umgebung einzufügen.

Zuvor wurde das Add-on von Splunk nur für die Installation auf dem Splunk Enterprise-Layer geprüft, und die Kunden waren für die Konfiguration des Add-ons in ihrer on-premises Splunk-Umgebung

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

verantwortlich. Mit der neuesten Version von 2.1.2 verfügt das Add-on über die zusätzliche Splunk-Plattformkompatibilität mit Splunk Cloud. Kunden, die **Classic-Instances** mit IDM- oder **Victoria-Instances** verwenden, können diese Verbesserung der Plattformkompatibilität nutzen. Jetzt haben Kunden die Flexibilität, zwischen Splunk Enterprise oder Splunk Cloud zu wählen und gleichzeitig den Einsatz unseres Add-ons in Betracht zu ziehen, um die Splunk-Integration zu erleichtern.

Weitere Informationen finden Sie unter Splunk-Integration.

Sitzungsaufzeichnung von Ereignissen in SIEM

Die **Sitzungsaufzeichnungsereignisse** können jetzt in Form von **Risk Insight-Ereignissen** und **Data Source-Ereignissen** für Apps und Desktops nach SIEM exportiert werden. Die neu hinzugefügten Ereignistypen finden Sie in der Phase Datenereignisse für den Export auf der Seite **Datenexporte** .

Weitere Informationen finden Sie unter Richtlinien und Aktionen.

24. Mai 2023

Globale Aktion für Endbenutzer benachrichtigen

Die Funktion **Richtlinien und Aktionen** in Citrix Analytics unterstützt jetzt die globale Aktion **Endbenutzer benachrichtigen**, die mit integrierten oder benutzerdefinierten Risikoindikator-Triggern kombiniert werden kann. Administratoren können Richtlinien mit der Aktion **Endbenutzer benachrichtigen** erstellen, die E-Mail-Benachrichtigungen nur für Endbenutzer generiert. Diese Aktion kann für verschiedene Compliance-Anwendungsfälle verwendet werden, z. B. um die Benutzer über die unerlaubte Nutzung von Anwendungen zu benachrichtigen oder bei verdächtigem Verhalten auf ihren Citrix-Konten zu warnen, ohne dass störende Maßnahmen ergriffen werden. Administratoren können den E-Mail-Nachrichtentext und die Betreffzeile je nach Szenario anpassen.

Weitere Informationen finden Sie unter Endbenutzer benachrichtigen.

04. Mai 2023

Generierung von Testereignissen

Die Funktion zur **Generierung von Testereignissen** wurde entwickelt, um Kunden dabei zu helfen, ihre Citrix Analytics-SIEM-Pipeline schnell zu testen. Musste der Administrator diese Integration früher testen, musste er auf das Onboarding der Datenquelle und die Benutzeraktivität warten, um zu überprüfen, ob die Ereignisse von Citrix Analytics generiert und somit von der SIEM-Umgebung empfangen wurden. Das ist keine Notwendigkeit mehr. Man kann einfach auf die Schaltfläche **Testdaten senden** klicken, um ein Dummy-Ereignis an die SIEM-Umgebung zu senden, und anhand der bereitgestellten

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Abfrage überprüfen, ob die Citrix Analytics SIEM-Integration wie erwartet eingestellt ist. Dies kann auch für den Administrator funktionieren, der versucht, einen gestörten Datenfluss zu debuggen, da es dabei helfen kann, die Fehlerquelle zu isolieren.

Weitere Informationen finden Sie unter Generierung von Testereignissen.

Generierung von SIEM-E-Mail-Benachrichtigungen

Die Funktion zur Generierung von SIEM-E-Mail-Benachrichtigungen macht die Problembehebung von Datenexporten auf ein neues Niveau der Benutzerfreundlichkeit. Citrix Analytics sendet Systemwarnungen für Aktivitäten, die zu einer Unterbrechung des SIEM-Datenflusses führen oder darauf hinweisen können. Die E-Mail wird an Citrix Cloud-Administratoren, Security-Volladministratoren, schreibgeschützte Sicherheitsadministratoren und schreibgeschützte Sicherheits- und Performance-Administratoren verteilt. Im Folgenden sind die verschiedenen Arten von Benachrichtigungen aufgeführt, die gesendet werden:

1. **Warnung beim SIEM-Datenexport —Kennwort wurde zurückgesetzt**

   Diese E-Mail wird ausgelöst, wenn das Kontokennwort auf der Seite Datenexporte zurückgesetzt wird. Wenn dies nur auf der Benutzeroberfläche von Citrix Analytics for Security erfolgt, kann dies zu einer Unterbrechung des Datenflusses führen. Diese Warnung enthält den Zeitpunkt, zu dem das Kennwort zurückgesetzt wurde, und erleichtert somit die Rückkehr zu einem erfolgreichen Datenfluss erheblich.

2. **SIEM-Datenexport-Warnung —Datenfluss gestoppt**

Diese E-Mail wird immer dann ausgelöst, wenn der Kunde von einer Unterbrechung des Datenflusses betroffen ist

- **Mehr als 24 Stunden** —Kritische Zeit, um schnell zum erfolgreichen Datenfluss zurückzukehren. Verwenden Sie dazu die hilfreichen Tipps zur Fehlerbehebung in der Warnung oder verwenden Sie die Registerkarte **Datenexportübersicht** mit **Kurzanleitung**.
- **Mehr als 7 Tage** —Die Kakfa-Aufbewahrungsfrist für jedes Kundenthema beträgt sieben Tage, was bedeutet, dass die Möglichkeit besteht, dass einige sicherheitsrelevante Daten abgelaufen sind. Es ist unbedingt erforderlich, die Tools zur Fehlerbehebung zu verwenden, um den Datenfluss zu SIEM wiederherzustellen.
- **Mehr als 30 Tage** —Das bedeutet, dass der Kunde unter sicherheitsrelevanten Daten gelitten hat und sofort darauf achten muss, den Datenfluss von Citrix Analytics in die SIEM-Umgebung wiederherzustellen.

Weitere Informationen finden Sie unter Generierung von SIEM-E-Mail-Benachrichtigungen.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

13. April 2023

Problem behoben

Windows - Die Citrix Workspace-App sendet einen leeren Dateinamen, einen Pfad und eine Formateigenschaft ab der Citrix Workspace-App Version 2203 und späteren Versionen. Daher zeigt die Citrix Analytics for Security GUI NA-Werte für die Spalten Download-Dateiname, Download-Dateipfad und Download-Dateiformat an. Dieses Problem ist jetzt behoben. [CAS-73498]

31. März 2023

Sitzungsaufzeichnung von Ereignissen in Citrix Analytics aus Sicherheitsgründen

In Citrix Apps and Desktops wurden zwei neue Ereignistypen hinzugefügt, um Ereignisse zu identifizieren und zu bewerten, die auf Sitzungsaufzeichnungen basieren.

- Citrix.EventMonitor.RDPConnection
- Citrix.EventMonitor.UserAccountModification

Administratoren können potenzielle Sicherheitsrisiken jetzt einfach identifizieren und bewerten. Sie können diese Ereignisse nutzen, um Informationen über wichtige Daten wie Prozess-IDs, Ziel-IP-Adressen und Beschreibungen der Benutzerkontovorgänge zu sammeln. Darüber hinaus finden Sie diese Ereignisse auch auf der Seite **Benutzerdefinierte Risikoindikatoren** und der **Self-Service-Suchseite** .

- **Self-Service-Suche**: Sie können diese Ereignisse zusammen mit ihren Attributdetails einsehen.
- **Benutzerdefinierte Risikoindikatoren**: Mithilfe dieser Ereignistypen können Sie jeden benutzerdefinierten Indikator konfigurieren.
  Weitere Informationen finden Sie unter Ereignistypen und unterstützte Felder.

App Protection-Ereignisse in Self-Service-Suche

Ein neues Ereignis namens **AppProtection.ScreenCapture** wird ausgelöst, wenn Sie versuchen, einen Screenshot aufzunehmen, während Sie sich in einer geschützten Sitzung unter der Citrix Apps and Desktops-Datenquelle befinden. Die **AppProtection.ScreenCapture-Ereignisse** sind auch auf den Seiten **Self-Service Search** und **Data Exports** verfügbar.

- **Self-Service-Suche**: Sie können die **AppProtection.ScreenCapture-Ergebnisse** zusammen mit all ihren Attributdetails einsehen.
- **Datenexporte**: Sie können den Ereignistyp **AppProtection.ScreenCapture** im Abschnitt Datenexporte einsehen. Navigieren Sie zu **Einstellungen > Datenexporte > Konfiguration**

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Datenereignisse für den Export**. Wählen Sie **Apps und Desktops** aus der Kategorie "Datenquellenereignisse"(optional) aus.

Sie können sich auch ein neues Attribut namens **App Protection Policies** für das **Session.Logon-Ereignis** anzeigen lassen.

Weitere Informationen finden Sie unter Ereignistypen und unterstützte Felder.

30. März 2023

Unterstützung benutzerdefinierter Rollen

Ein Administrator kann für benutzerdefinierte Rollen mithilfe von Gruppen in Ihrem Active Directory oder Azure Active Directory oder durch die Einrichtung einer Okta-Integration für Citrix Analytics for Security hinzugefügt werden. Diese Integration ermöglicht einen optimierten Ansatz zur Verwaltung der Dienstzugriffsberechtigungen für alle Gruppenadministratoren.

Nachdem ein Administrator erfolgreich zu Active Directory oder Azure Active Directory hinzugefügt wurde, kann der Administrator Gruppen erstellen und einer bestimmten Gruppe eine benutzerdefinierte Rolle zuweisen. Einzelberechtigungen haben Vorrang vor Gruppenberechtigungen, wenn ein Administrator Mitglied von beiden ist.

Weitere Informationen finden Sie unter Unterstützung benutzerdefinierter Rollen.

Bedienfeld zur Fehlerbehebung für die SIEM-Benutzeroberfläche

Die Benutzeroberfläche für Datenexporte wurde um die folgenden Änderungen erweitert:

- **Registerkarte "Zusammenfassung"**: Auf der Registerkarte "Zusammenfassung"werden die SIEM-Ereignismetriken, der Onboarding-Status der Datenquelle und der Status des Datenverbrauchs im folgenden Szenario beschrieben:
  - **Verfügbare Daten in Citrix Analytics**: Stellt den Onboarding-Status für die verschiedenen Datenquellen bereit.
  - **Verfügbare Ereignisse für die SIEM-Nutzung**: Gibt die Anzahl der Erkenntnisse an, die an Ihre SIEM-Umgebung gesendet werden.
  - **Datenverbrauch durch SIEM**: Gibt den Status des Datenverbrauchs an.
- **Registerkarte "Konfiguration"**: Die Registerkarte **Konfiguration** enthält Informationen zur Einrichtung Ihres Kontos, zur Einrichtung der SIEM-Umgebung und zur Auswahl von Datenereignissen.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Kurzanleitung zum Datenexport**: Administratoren können jetzt die **Kurzanleitung**verwenden, die die Einrichtung und Wartung von SIEM-Integrationen vereinfacht. Auf den Link zur **Kurzanleitung zum Datenexport** kann sowohl über die Registerkarte **Zusammenfassung** als auch über die Registerkarte **Konfiguration** zugegriffen werden.

Weitere Informationen finden Sie unter Problembehandlung bei Datenexporten.

24. März 2023

Änderung der Benutzerprofilansicht

Benutzerprofildaten in Bezug auf Anwendungen, Standorte, Geräte und die Nutzung von ShareFile-Daten sind auf der Seite **Benutzerinformationen in der Benutzer-Timeline** nicht verfügbar. Die folgenden Benutzerinformationen aus Active Directory sind weiterhin verfügbar:

- Berufsbezeichnung
- Adresse
- E-Mail
- Telefon
- Standort
- Organisation

Es gibt keine Änderungen an den Benutzerprofildaten, die nach SIEM exportiert werden. Weitere Informationen finden Sie unter Benutzerprofil.

Entfernung dynamischer Autovorschläge aus allen Suchansichten

Die automatische Vorschlagsfunktion für Dimensionen, die auf den historischen Daten des Mandanten basieren, ist jetzt für die folgenden Seiten veraltet:

- Self-Service-Suche
- Benutzerdefinierter Risikoindikator

Statische Vorschläge für Dimensionen wie **Event-Type** und **Clipboard-Operations** sind jedoch weiterhin im Suchfeld verfügbar.

Weitere Informationen finden Sie unter So verwenden Sie die Self-Service-Suche.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

21. März 2023

Bereich “Empfehlungen”zur Unterstützung der On-Premise-StoreFront-Datenquelle

Auf der Seite **Datenquellen** wurde ein neuer Bereich mit **Empfehlungen** eingeführt. Im Bereich **Empfehlungen** auf der Seite **Datenquellen wird** der Benutzer darüber informiert, wie wichtig das Onboarding von On-Premises-StoreFront-Datenquellen ist. Es hilft dem Benutzer beim einfachen Onboarding der On-Premises-StoreFront-Datenquellen und bietet dem Benutzer auch die Möglichkeit, alle verfügbaren Datenquellen zu überprüfen und sicherzustellen.

Weitere Informationen finden Sie unter Verbindung mit einer StoreFront-Bereitstellungherstellen.

23. Februar 2023

Behobene Probleme

Die Aktionen schlagen für die lokalen Citrix Apps und Desktop-Bereitstellungen fehl, bei denen die Citrix Apps- und Desktop-Version > 1912 ist. Dieses Problem wurde sowohl bei manuellen als auch bei richtlinienbasierten Aktionen festgestellt. Dieses Problem ist jetzt behoben. [CAS-69098]

Auf der Seite Self-Service-Suche nach Apps und Desktops werden mehrere App-Start- und App-End-Ereignisse angezeigt, wenn virtuelle Apps nur einmal gestartet werden. Dieses Problem tritt in der Citrix Workspace-App für Linux-Clientversionen auf. Dieses Problem ist jetzt behoben. [CAS-36236]

Benutzerereignisse aus dem Secure Private Access-Dienst nach dem 4. April 2022 und bis Ende Mai 2022 sind möglicherweise nicht in Ihren Citrix Analytics-Mandanten verfügbar. Dieses Problem ist jetzt behoben. [CAS-66897]

22. Februar 2023

Verbesserung der wöchentlichen E-Mail-Benachrichtigungen

Citrix Analytics versendet wöchentliche E-Mail-Benachrichtigungen, mit denen Sie die Sicherheitsrisiken Ihres Unternehmens zusammenfassen können. Die wöchentliche E-Mail-Benachrichtigung wurde mit den folgenden Updates verbessert:

- Bietet einen Überblick über die Risikoverteilung der Benutzer —Gesamtzahl der erkannten Benutzer, Anzahl der riskanten und nicht riskanten Benutzer für eine Woche
- Gesamtzahl der bearbeiteten Ereignisse für eine Woche
- Gesamtzahl der für eine Woche ausgelösten Indikatoren
- Gesamtzahl der für eine Woche ausgeführten Aktionen
- Gesamtzahl der Datenquellen, die für die Datenverarbeitung aktiviert sind

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Weitere Informationen finden Sie unter Wöchentliche E-Mail-Benachrichtigung.

Das Feld “Dateiformat herunterladen”für den Ereignistyp App.SaaS.File.Download wurde hinzugefügt

Auf der Seite Self-Service Search für die Datenquelle Apps and Desktops wurde ein neues Feld für das **Download-Dateiformat** für den Ereignistyp App.SaaS.File.Download hinzugefügt. Mit dieser Änderung können Sie jetzt benutzerdefinierte Risikoindikatoren für das Feld **Download-Dateiformat** konfigurieren und das Feld auch als Teil des Exportformats in CSV-Format exportieren.

Weitere Informationen finden Sie unter Self-Service-Suche nach Apps und Desktops.

Änderung der vom Browser abgeleiteten Felder

Bisher enthielt die Self-Service-Suchseite die Felder **Browser**, **Browser-Hauptversion** und **Browser-Nebenversion** zur Darstellung der Browsernamen und -Versionen. Aus Gründen der Übersichtlichkeit und Genauigkeit sind diese drei Felder nun jedoch veraltet und wurden in der Self-Service-Suche, der benutzerdefinierten Indikatorvorlage und dem CSV-Download für die Datenquelle Apps and Desktops durch den **Browsernamenund die Browserversion** ersetzt.

Weitere Informationen finden Sie unter Self-Service-Suche nach Apps und Desktops.

16. Februar 2023

Problem behoben

Wöchentliche E-Mails sind für einige EU- und APS-Kunden betroffen, während für einen Mandanten der Status Username Masking abgerufen wird. Infolgedessen erhalten die Administratoren aufgrund der Ausnahme 10 identische wöchentliche E-Mails. Sobald die Ausnahme aufgetreten war, erhielten nachfolgende Mandanten die wöchentliche E-Mail nicht. Dieses Problem wurde jetzt behoben. [CAS-76138]

03. Februar 2023

Analytics-Unterstützung für den Citrix Secure Private Access-Dienst, verfügbar in der Europäischen Union und den Regionen Asien-Pazifik, Süd

Citrix Analytics for Security verarbeitet jetzt Benutzerereignisse von Citrix Secure Private Access, das in der Region Europäische Union und der Region Asien-Pazifik Süd verfügbar ist. Wenn Ihr Unternehmen aus der Region der Europäischen Union oder der Region Asien-Pazifik Süd in die Citrix

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Cloud eingebunden ist, können Sie die Risikoinformationen der Benutzer einsehen, die den Secure Private Access Service verwenden.

Weitere Informationen finden Sie unter Datenquellen.

11. Januar 2023

Entfernung der Webfilterfunktion aus Secure Private Access

Die Webfilterfunktion wurde aus der Kategorie Secure Private Access entfernt. Die folgenden Funktionen von Citrix Analytics for Security sind beeinträchtigt, da die kategoriebasierte Webfilterung durch Secure Private Access nicht mehr unterstützt wird:

1. Datenfelder wie Kategorie-Gruppe, Kategorie und Reputation von URLs sind im Dashboard von Citrix Analytics for Security nicht mehr verfügbar.
2. Der Indikator für riskante Website-Zugriffe, der auf denselben Daten basiert, ist ebenfalls veraltet und wird für Kunden nicht ausgelöst.
3. Alle vorhandenen benutzerdefinierten Risikoindikatoren, die die Datenfelder (Kategorie-Gruppe, Kategorie und Reputation von URLs) und die zugehörigen Richtlinien verwenden, werden nicht mehr ausgelöst.
4. Die Registerkarten **Benutzerzugriff** und **App-Zugriff**.
5. Die SIEM-Exporte haben noch einige Zeit die Attribute urlcategory, urlcategorygroup und urlcategoryreputation mit den folgenden Dummy-Werten:
    - 99999 für Kategorie und Kategoriegruppe
    - 0 für Reputation

Weitere Informationen finden Sie unter Self-Service-Suche für Secure Private Access.

27. Dezember 2022

Änderung der Dropdownliste für die Datenquellensuche für Self-Service Search

Die Datenquellenliste wurde so geändert, dass sie standardmäßig **Sessions** und nicht **Apps und Desktops** auf der Self-Service-Suchseite anzeigt. Außerdem wird der Abschnitt Leistung an den Anfang verschoben, gefolgt vom Abschnitt Sicherheit, da die Leistungsdatenquellen nicht sichtbar waren.

Weitere Informationen finden Sie unter Self-Service-Suche.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

13. Dezember 2022

Verbesserung des Benutzer-Dashboards

Das Benutzer-Dashboard wurde mit Zusammenfassungen und Diagrammen überarbeitet, um Administratoren dabei zu helfen, die Sicherheitslage des Unternehmens zu überwachen. Die Ansicht enthält nicht nur Details zu erkannten Benutzern, ausgelösten Risikoindikatoren und angewandten Aktionen, sondern bietet auch eine zeitbasierte Trendlinie kritischer Metriken zur besseren Bewertung der Risiken. Administratoren können Daten, die für Sie von Interesse sind, detailliert aufschlüsseln und zu relevanten Dashboards mit dem richtigen Kontext navigieren, um so eine schnellere Risikoanalyse zu ermöglichen.

Weitere Informationen finden Sie unter Benutzer-Dashboard.

05. Dezember 2022

Dashboard zur Zugriffssicherung —Logon Network

Der Abschnitt Anmeldenetzwerk wurde neu hinzugefügt und enthält die folgenden Benutzerdetails:

- Die Organisationen, die den IP-Adressen zugeordnet sind, von denen aus sich die Benutzer angemeldet haben.
- Das gesamte eindeutige öffentliche Subnetz und das private Subnetz, von dem aus sich die Benutzer angemeldet haben.
- Die Details, die sich der Benutzer mit Proxys und privaten VPN-Diensten angemeldet hat.

Mithilfe dieser zusätzlichen Details kann ein Administrator die Benutzeranmeldedaten überprüfen und sicherstellen, dass die Benutzeranmeldung den Sicherheitserwartungen des Unternehmens entspricht.

Weitere Informationen finden Sie unter Access Assurance Dashboard.

18. November 2022

Problem behoben

- Die Geofence-Indikatoren, die fälschlicherweise ausgelöst wurden, ohne dass es irgendwelche Quellereignisse gab, wurden behoben. [CAS-73222]

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

08. November 2022

Aktionen umbenennen

Einige der in Citrix Analytics for Security verwendeten Aktionen wurden umbenannt, um mehr Klarheit zu schaffen. Diese Aktionen sind:

- **Admins benachrichtigen** —Administrator (en) benachrichtigen
- **Benutzer sperren** —Benutzerkonto sperren
- **Benutzer abmelden** —Aktive Sitzungen abmelden
- **Benutzer entsperren** —Benutzerkonto entsperren
- **Benutzer deaktivieren** —Benutzerkonto deaktivieren

Weitere Informationen finden Sie unter Was sind die Aktionen?

Behobene Probleme

- Wenn Sie eine Option aus der Dropdownliste der Timeline-Aktionen auswählen, können Sie keine manuelle Aktion auslösen, da die Schaltflächen Löschen und Anwenden nicht sichtbar sind. Dieser Zustand tritt in der neuesten Firefox-Version auf. Dieses Problem ist jetzt behoben. [CAS-72051]
- Die Kategorien **Festplatte**, **Festplatte**und **Festplatte** werden zu einer einzigen Kategorie zusammengefasst und zwar als **Festplattenlaufwerk** für das Feld “Download-Gerätetyp”in der Self-Service-Suche nach der Datenquelle Apps und Desktops. [CAS-67188]
- Manchmal werden doppelte Benachrichtigungen von Microsoft Graph mit derselben Warnungs-ID empfangen, was zur Entstehung doppelter Risikoereignisse führt. In den Anwendungen ist ein Deduplizierungsmechanismus implementiert, um dieses Problem zu vermeiden. [CAS-66731]

19. Oktober 2022

Datum, Quelle, Ereignisse, Auswahl und Export

Sie können jetzt den neuen Workflow für den Export von Datenereignissen nutzen, um zusätzlich zu den durch maschinelles Lernen generierten Risikoeinblicken und zugehörigen Daten Datenquellenereignisse zu exportieren.

Dadurch können Administratoren von Security and Security Operations (SOC):

- Korrelieren Sie Daten aus Citrix Analytics mit anderen Datenquellenereignissen, die im Sicherheitsinformations- und Ereignismanagement (SIEMs) zusammengefasst sind

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Steuern Sie, welche Datenereignisse zu SIEMs fließen, um die Speicherkosten zu optimieren

Die Datenereignisse werden an Ihre vorhandenen SIEM-Integrationen und Datenkonnektoren übermittelt und entsprechen den Informationen, die in unserer Self-Service-Ereignissuchansicht verfügbar sind.

Weitere Informationen finden Sie unter Datenereignisse, die aus Citrix Analytics for Security in Ihren SIEM-Dienst exportiert wurden.

18. Oktober 2022

Administratoren erlauben, dynamische Sitzungsaufzeichnungsaktionen auf Citrix DaaS-Sites auszuführen

Administratoren können jetzt dynamische Sitzungsaufzeichnungsaktionen auf Citrix DaaS-Sites ausführen und die virtuellen Sitzungen der Benutzer dynamisch aufzeichnen. Sie können die Aktion mit einer Richtlinie konfigurieren, um automatisch die Aufzeichnung von Benutzersitzungen zu starten, falls eine riskante Aktivität eines bestimmten Benutzers von Citrix Analytics for Security erkannt wird.

Weitere Informationen finden Sie unter Was sind die Aktionen?

14. Oktober 2022

Feedback zu Indikatoren für Benutzerrisiken geben

Administratoren von Citrix Analytics for Security können Benutzerrisikoindikatoren jetzt als hilfreich oder nicht hilfreich melden, indem sie Feedback im Bereich mit den Indikatorendetails geben. Diese Funktion ermöglicht es Administratoren, falsch positive Ergebnisse zu melden, Störungen bei häufig ausgelösten Indikatoren zu reduzieren und zusätzlichen Kontext mit anderen Administratoren zu teilen. Als zusätzliches Ergebnis wird der Risikoindikator, der nicht hilfreich ist, aus der Zeitleiste des Benutzers ausgeblendet, und die Benutzerrisikobewertung wird neu kalibriert.

Weitere Informationen finden Sie unter Feedback zu Indikatoren für Benutzerrisiken.

26. September 2022

Zugriffsabsicherung zur Unterstützung der Geofence-Sperrliste

Die Registerkarten **sicherer** und **riskanter** Standort werden unter den Geofence-Einstellungen hinzugefügt.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Safe Location Geofencing hilft dabei, den Zugriff außerhalb eines definierten Geofencebereichs zu identifizieren und einzuschränken.
- Riskantes Standort-Geofencing hilft dabei, riskante Benutzerzugriffe entsprechend dem bekannten Verhalten des Unternehmens zu erkennen und einzugrenzen.

Sowohl sichere als auch riskante Geofencings werden durch ihre eigenen vorkonfigurierten benutzerdefinierten Risikoindikatoren unterstützt.

Weitere Informationen finden Sie unter Aktivieren von Geofencing.

Behobene Probleme

- Citrix Cloud-API zur Anzeige des **Kundennamens** im E-Mail-Text. Jetzt verwendet die E-Mail den Spitznamen, um den **Kundennamen** im E-Mail-Text anzuzeigen, der an die Administratoren gesendet wird. [CAS-65350]
- Die NetScaler Gateway-Datenquellenkarte ist in **Citrix Analytics for Security** und **Citrix Analytics for Performance** üblich. Die Datenverarbeitung rief ständig den Citrix Analytics for Security-Endpunkt auf und war für Kunden unterbrochen, die nur die Berechtigung **Citrix Analytics for Performance** hatten. [CAS-70817]
- Wenn mehrere Berechtigungsnachrichten gleichzeitig von Citrix Cloud empfangen werden, tritt beim Aktualisieren des Redis-Cache eine Wettlaufbedingung auf. In einem solchen Szenario wird eine Berechtigungsnachricht im Cache aktualisiert und die verbleibende Nachricht wird verloren. Dieses Problem wurde nun behoben, sodass alle Entitlement-Nachrichten im Cache aktualisiert wurden. [CAS-70823]

13. September 2022

Erweiterung des Sharelink-Dashboards

Das Sharelink-Dashboard wurde mit einer Zusammenfassung und einer Detailansicht überarbeitet. Die zusammenfassende Ansicht besteht aus den wichtigsten aktiven Freigaben und Freigaben mit dem höchsten Risiko. Die Detailansicht bietet dem Administrator weitere Informationen mit der Einführung von erstellten Attributen, Aktivitätsanzahl, Authentifizierungstyp, Berechtigung, Freigabetyp und Inhalt. Der Administrator kann bei Bedarf einen Drilldown durchführen und weiter filtern und den Zeitrahmen für die Anzeige der interessierenden Daten ändern/angeben.

Weitere Informationen finden Sie unter Dashboard für Freigabelinks.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

09. September 2022

Verbesserung bei den Risikoindikatoren für unmögliche Reisen

Die Risikoindikatoren für unmögliche Reisen wurden verbessert, um die registrierende Organisation und den Routing-Typ der Client-IP-Adressen anzuzeigen. Diese neuen Felder sind sowohl in den Detailansichten der Benutzerzeitleistenanzeige als auch in an SIEM gesendeten Indikatordetails verfügbar.

Weitere Informationen zu den Standardrichtlinien finden Sie in den folgenden Artikeln:

- Kontinuierliche Risikobewertung.
- Richtlinien und Maßnahmen

19. August 2022

VDA-Drucktelemetrie aktivieren

Ein Ereignis namens VDA.Print wird ausgelöst, wenn ein Druckauftrag in Citrix Apps and Desktops initiiert wird. Die VDA-Druckereignisse sind auch auf den Seiten **Self-Service-Suche** und **benutzerdefinierten Risikoindikatoren** verfügbar.

- **Self-Service-Suche**: Sie können die VDA.PRINT-Ergebnisse zusammen mit allen Attributdetails anzeigen.
- **Benutzerdefinierte Risikoindikatoren**: Neue Ereignisse werden für die VDA-Drucktelemetrie über EventHub bereitgestellt und sind auch innerhalb des benutzerdefinierten Indikators verfügbar. Sie können diese Ereignisschlüssel/Wert-Paare verwenden, um benutzerdefinierte Indikatorauslöser zu konfigurieren.

Um die Drucktelemetrie und die Übertragung von Druckprotokollen an Citrix Analytics for Security zu ermöglichen, müssen Sie Registrierungsschlüssel erstellen und Ihren VDA konfigurieren. Diese Druckprotokolle enthalten wichtige Informationen über Druckaktivitäten wie Druckernamen, Druckdateinamen und die Gesamtzahl der gedruckten Exemplare. Als Sicherheitsadministrator können Sie diese Protokolle verwenden, um das Risiko zu analysieren und Ihre Benutzer zu untersuchen.

Weitere Informationen finden Sie unter Aktivieren der Drucktelemetrie für Citrix DaaS.

18. August 2022

Problem behoben

- In der Self-Service-Suche nach Apps und Desktops und auf der Seite Benutzeranmeldungen unter dem Dashboard für den Speicherort der Zugriffsabsicherung wurde der Versionswert

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

der Workspace-App in der heruntergeladenen CSV-Datei als **N/A** (nicht verfügbar) aufgefüllt, während er in der Seitenansicht verfügbar war. Dieses Problem ist jetzt behoben. [CAS-70361]

17. August 2022

Anpassung der Endbenutzer-E-Mail pro Richtlinie

Sie können jetzt den Inhalt der an Endbenutzer gesendeten E-Mail gemäß Richtlinie anpassen. Insbesondere wenn Sie eine Richtlinie mit der Aktion Endbenutzer-Antwort anfordern oder eine störende Aktion für das Konto des Benutzers erstellen (z. B. Benutzer abmelden und Benutzer sperren), ist der E-Mail-Inhalt, der bei Anwendung der Richtlinie an Endbenutzer gesendet wird, anpassbar.

Weitere Informationen zum Anpassen der Endbenutzer-E-Mails pro Richtlinie finden Sie unter Richtlinien und Aktionen.

11. August 2022

Neue Fragen zur **Zugriffssicherung** —**Geolocation** wurden im **FAQ-Artikel** hinzugefügt. Weitere Informationen finden Sie unter Häufig gestellte Fragen.

Problem behoben

- Die Schaltfläche **Alle Benachrichtigungen** anzeigen leitete den Administrator zu einem wöchentlichen E-Mail-Link `https://citrix.cloud.com/notifications` weiter, der einen Tippfehler enthielt. [CAS-69236]

17. Juni 2022

Die Datenverarbeitung ist standardmäßig für neue bezahlte Ansprüche aktiviert

Bisher mussten Kunden mit einer neuen kostenpflichtigen Berechtigung für Citrix Analytics for Security die Datenverarbeitung in der Sitekarte bestimmter Datenquellen aktivieren, um mit der Verarbeitung von Daten für diese Datenquellen zu beginnen.

In dieser Version ist die Datenverarbeitung für die folgenden Citrix Cloud-Dienste standardmäßig aktiviert, wenn die neue kostenpflichtige Lizenz für Citrix Analytics for Security bereitgestellt wird:

- Citrix Secure Private Access
- Citrix Content Collaboration
- Citrix DaaS

Weitere Informationen finden Sie unter Erste Schritte.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

09. Juni 2022

Problem behoben

- Microsoft Graph-Risikoindikatoren, die von Azure AD Identitätsschutz und Microsoft Defender for Endpoint generiert wurden, können in Security Analytics mehrfach angezeigt werden. Dieses Problem ist jetzt behoben. [CAS-66593,CAS-66731]

02. Juni 2022

Behobene Probleme

- Bei der Self-Service-Suche nach Richtlinien wurde bei der Auswahl der Dimension **Policy-Name** in Ihrer Suchabfrage zum Filtern von Ereignissen eine Liste mit nicht gültigen Richtlinien zusammen mit den gültigen Richtlinien für Security Analytics vorgeschlagen. [CAS-66838]
- Die Downloaddateigröße von **File.Download-Ereignissen** von Windows Citrix Receiver wurde in der Self-Service-Suche falsch angezeigt. Dieses Problem trat auf, weil der tatsächliche Wert in KB lag und die Benutzeroberfläche den Wert als Byte behandelte, was dazu führte, dass den Benutzern falsche Werte angezeigt wurden. [CAS-67105]

24. Mai 2022

Einführung von Indikatoren für unmögliche Reiserisiken für Content Collaboration, Citrix DaaS und Citrix Virtual Apps and Desktops sowie Gateway-Datenquellen

Wenn sich der Benutzer an zwei Standorten anmeldet, die zu weit voneinander entfernt sind, um innerhalb der verstrichenen Zeit zu reisen, erkennt Citrix Analytics diese Aktivität als unmögliches Reiseszenario und löst den Indikator **Unmögliches Reiserisiko** aus. Weitere Informationen zu den Indikatoren für unmögliche Reiserisiken finden Sie in den folgenden Artikeln:

- Citrix Content Collaboration-Risikoindikatoren
- NetScaler Gateway-Risikoindikatoren
- Citrix Virtual Apps and Desktops und Citrix DaaS-Risikoindikatoren

17. Mai 2022

Virtual Apps and Desktops werden in Apps und Desktops umbenannt

In den Security Analytics-Dashboards und Berichten sowie in den Daten, die von Security Analytics an Ihren SIEM-Dienst gesendet werden, werden nun alle Kennungen für Virtual Apps and Desktops als

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Apps und Desktops aktualisiert, um sie an den umbenannten Produktnamen anzupassen.

Beispielsweise werden auf der Seite Datenquellen die Beschriftungen Virtual Apps and Desktops in Apps und Desktops umbenannt.

Das Label Apps and Desktops steht sowohl für Citrix on-premises Citrix Virtual Apps and Desktops als auch für Citrix DaaS (ehemals Citrix Virtual Apps and Desktops Service) in Ihrer Organisation.

Behobene Probleme

Citrix Analytics erkennt nicht automatisch die Citrix DaaS Cloud Monitor- oder Director-Sites, die Ihrem Citrix Cloud-Konto zugeordnet sind. [CAS-66801]

05. April 2022

Was ist neu

Secure Workspace Access wurde in Secure Private Access umbenannt

In den Analytics-Dashboards und -Berichten werden alle **Secure Workspace Access-Labels** jetzt als **Secure Private Access** aktualisiert, um sie an den umbenannten Produktnamen anzupassen.

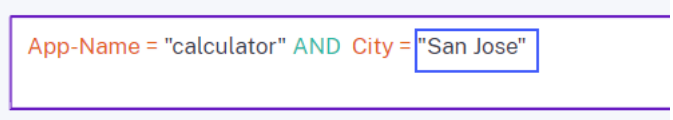
Beispielsweise werden auf der Seite **Datenquellen** und der **Self-Service-Suchseite** die **Secure Workspace Access-Labels** in **Secure Private Access** umbenannt.

21. März 2022

Problem behoben

- Auf der Seite **Risikoindikator erstellen** funktionieren automatische Vorschläge für Dimensionen und Operatoren nicht, wenn die vorherige Bedingung Ihrer Suchabfrage einen Dimensionswert enthält, der durch ein Leerzeichen getrennt ist.

  In der folgenden Abfrage funktionieren automatische Vorschläge beispielsweise nicht mehr, nachdem Sie die Stadt als ausgewählt haben `San Jose`. Dieses Problem ist jetzt behoben. [CAS-64126]

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

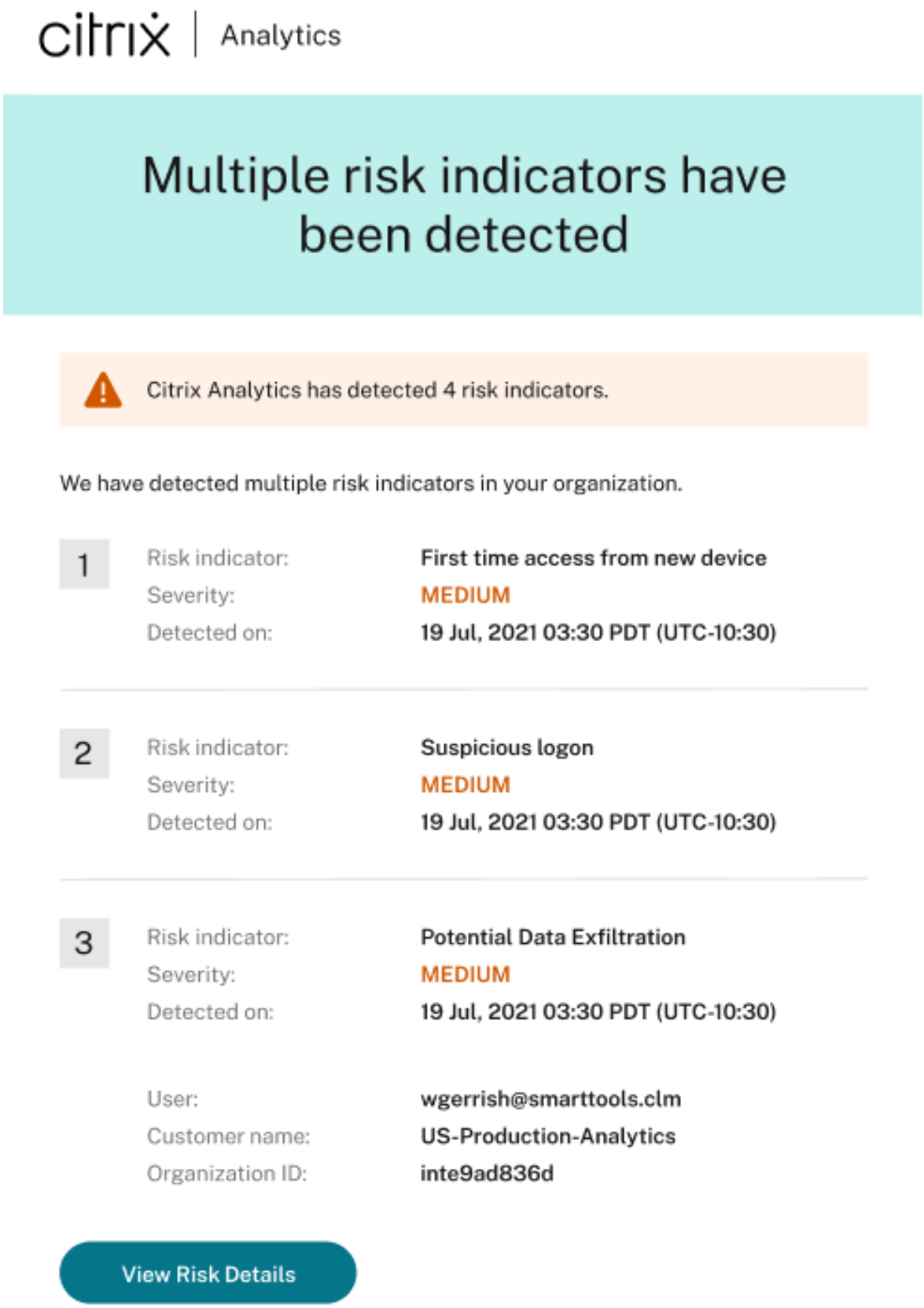
10. März 2022

Was ist neu

E-Mail-Erweiterungen des Administrators benachrichtigen

- Die E-Mail-Benachrichtigung für die Aktion **Administrator (e) benachrichtigen** enthält jetzt die Details der verschiedenen Risikoindikatoren, die mit einer ausgelösten Richtlinie verknüpft sind.
- Sie können den Namen, den Schweregrad und das Auslösedatum jedes mit der Richtlinie verknüpften Risikoindikators anzeigen.
- Klicken Sie auf **Risikodetails anzeigen**, um die Benutzer-Zeitleistenseite in Citrix Analytics zu öffnen und den neuesten Risikoindikator anzuzeigen, der die Richtlinie ausgelöst hat. Auf der Seite Benutzerzeitleiste können Sie auch alle für den Benutzer ausgelösten Risikoindikatoren anzeigen.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Weitere Informationen zur Aktion **Administrator (s) benachrichtigen** finden Sie unter Richtlinien und Aktionen.

Problem behoben

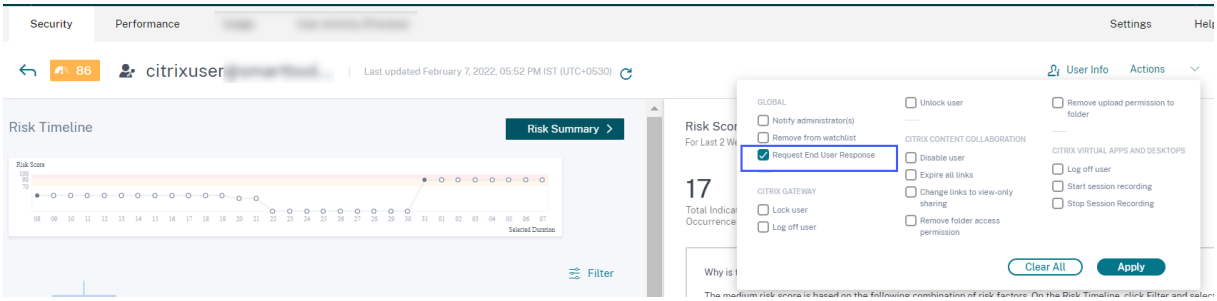
Citrix Analytics empfängt keine Benutzerereignisse von der Secure Workspace Access-Datenquelle. Daher sehen Sie die Benutzerereignisse nicht auf der entsprechenden Self-Service-Suchseite. Sie können auch keine benutzerdefinierten Risikoindikatoren für die Secure Workspace Access-Datenquelle erstellen. [CAS-64619]

03. März 2022

Was ist neu

Endbenutzerantwort manuell anwenden Bisher können Sie die Aktion **Endbenutzerantwort anfordern** nur auf ein Benutzerkonto anwenden, indem Sie eine Richtlinie erstellen.
In dieser Version können Sie die Aktion in der Liste **Aktionen** auf der Benutzerzeitleiste auswählen und diese Aktion manuell auf einen Risikoindikator anwenden.

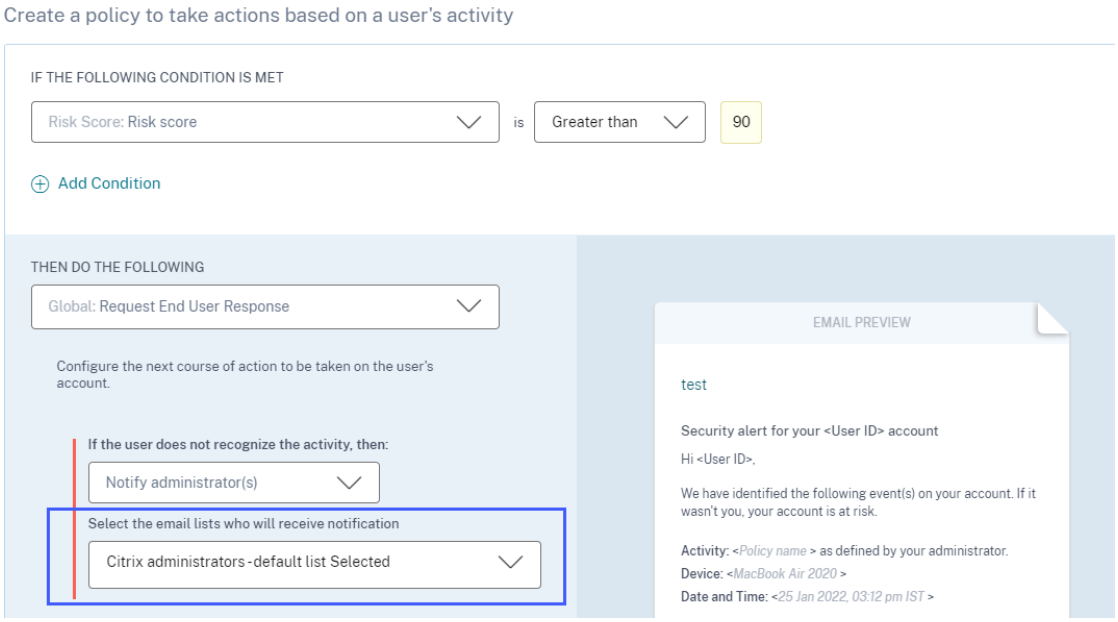
Weitere Informationen zur Aktion und zum manuellen Anwenden von Aktionen finden Sie unter Richtlinien und Aktionen.



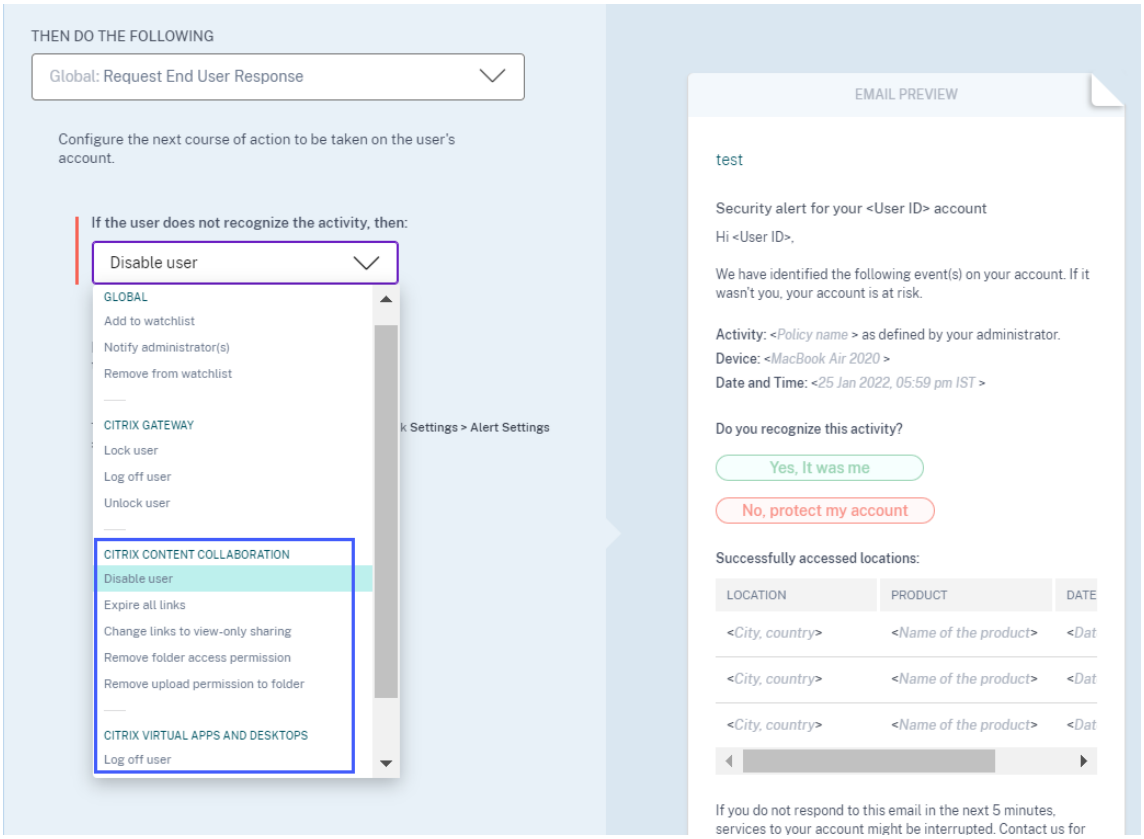
Anfordern von Erweiterungen der Endbenutzerantwort für die Richtlinie Wenn Sie eine Richtlinie mit der Aktion **Endbenutzer-Antwort anfordern** erstellen, werden die folgenden Verbesserungen angezeigt:

- Nachdem Sie als nächste Aktion **Administrator (e) benachrichtigen** ausgewählt haben, können Sie nun die Standard- und die erstellten E-Mail-Verteilerlisten anzeigen, aus denen Sie auswählen können.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



- Sie können jetzt eine der Aktionen aus Citrix Content Collaboration oder Citrix Virtual Apps and Desktops und Citrix DaaS als nächste Aktion auswählen. Zuvor können Sie nur eine der globalen Aktionen oder NetScaler Gateway-Aktionen auswählen.



Weitere Informationen über die Aktion finden Sie unter Richtlinien und Aktionen.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

23. Februar 2022

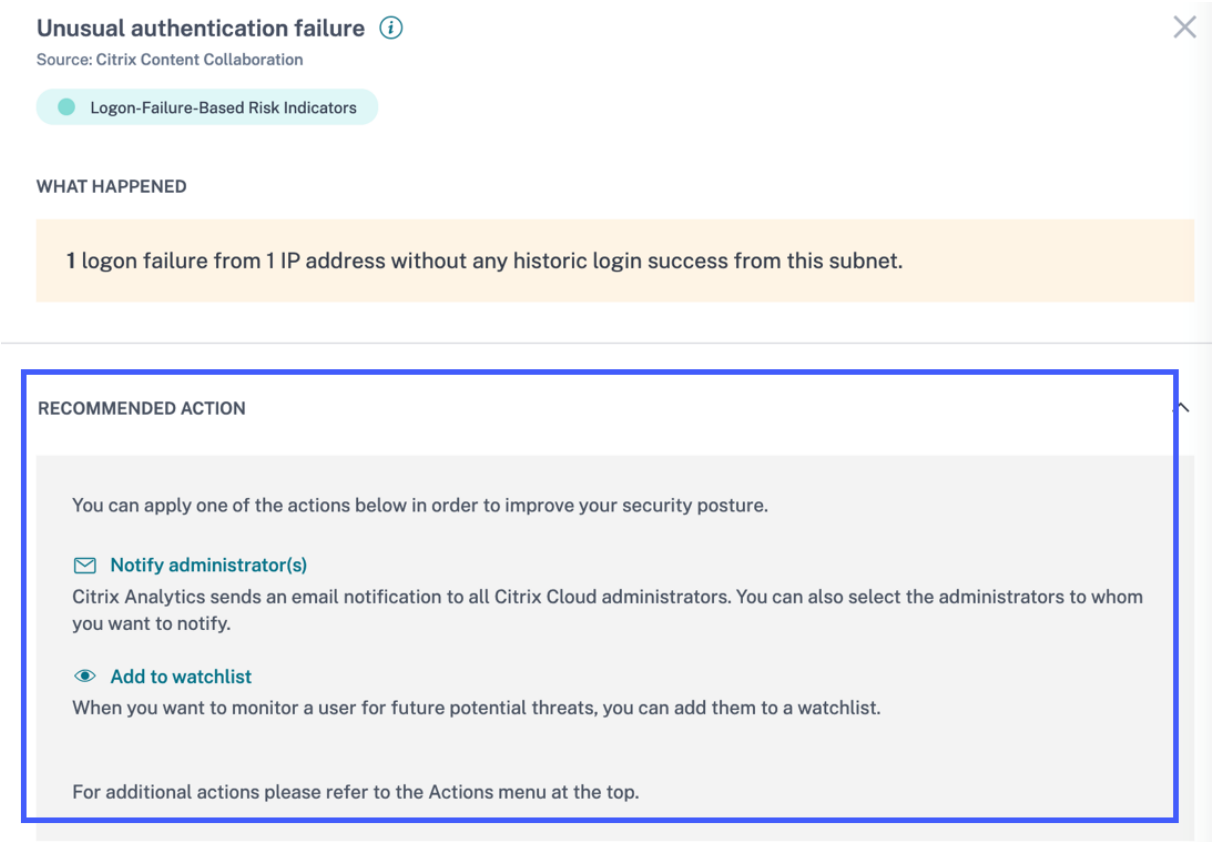
Was ist neu

Empfohlene Maßnahmen für einen Risikoindikator Citrix Analytics empfiehlt Ihnen, Aktionen wie **Administrator (e) benachrichtigen**, **Zur Watchlist hinzufügen**und **Richtlinie erstellen** anzuwenden, wenn die folgenden Risikoindikatoren für einen Benutzer ausgelöst werden:

- Ungewöhnlicher Authentifizierungsfehler (Content Collaboration-Datenquelle)
- Ungewöhnlicher Authentifizierungsfehler (Gateway Datenquelle)
- Verdächtige Anmeldung (Citrix Virtual Apps and Desktops und Citrix DaaS-Datenquelle)

Wenn Sie zur Benutzerzeitleiste gehen und den Risikoindikator auswählen, können Sie alle vorgeschlagenen Aktionen im Abschnitt **RECOMMENDED ACTION** anzeigen.

In der Risikoanzeige Ungewöhnlicher Authentifizierungsfehler können Sie beispielsweise die folgenden empfohlenen Aktionen anzeigen:



Diese Funktion bietet eine Anleitung zur Auswahl einer Aktion, die Sie je nach Schweregrad des vom Benutzer ausgehenden Risikos ergreifen können. Sie können jedoch auch eine geeignete Maßnahme ergreifen, die außerhalb der empfohlenen Liste liegt und von Ihrer Risikoanalyse abhängt.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Problem behoben

- Wenn Ihr Unternehmen in Citrix Cloud in der Heimatregion **Asien-Pazifik-Süd** eingebunden ist, empfängt Citrix Analytics möglicherweise keine Benutzerereignisse von der Authentifizierungsdatenquelle. Daher werden die Benutzerereignisse möglicherweise nicht auf der entsprechenden Self-Service-Suchseite angezeigt. Dieses Problem ist behoben. [CAS-62300]

17. Februar 2022

Was ist neu

Verbesserte Datenerfassung und Berichterstellung für die Citrix Virtual Apps and Desktops und die Citrix DaaS-Datenquelle Mit dieser Version sehen Sie die folgenden Änderungen:

- Verbesserungen bei der Datenerfassung, Korrelation und Berichterstellung von Ereignissen von Citrix Workspace-App-Clients und dem Citrix Monitor-Dienst.
- Verbesserung der Qualität von Ereignissen, die von Benutzern und Clientversionen empfangen wurden, die für die Self-Service-Suche, benutzerdefinierte Risikoindikatoren und die allgemeine Risikoerkennung verwendet werden können.

Unterstützung für kontextbezogene Vorlagen für die Sitzungsereignisse und die App-Ereignisse in Content Collaboration Auf der Self-Service-Suchseite können Sie jetzt nur die Details der relevanten Felder anzeigen, die mit den Datei-, Ordner-, Sitzungs-, Freigabe- und Benutzerereignissen verknüpft sind. Die nicht zutreffenden Felder für die Ereignisse werden entfernt.

Sie können beispielsweise die folgenden Details der `File.Copy`-Ereignisse anzeigen:

- Datei-ID
- Dateikopie-ID
- Datei-Pfad
- Zieldateipfad
- Stream-ID
- Zonen-ID

Diese Angaben helfen Ihnen bei der Risikountersuchung und Analyse eines Benutzerkontos, das mit einem riskanten Verhalten verbunden ist. Sie können die spezifischen Attribute eines Ereignisses aufschlüsseln, das riskant erscheint.

Weitere Informationen zu den Feldern finden Sie unter Self-Service-Suche für Content Collaboration.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

10. Februar 2022

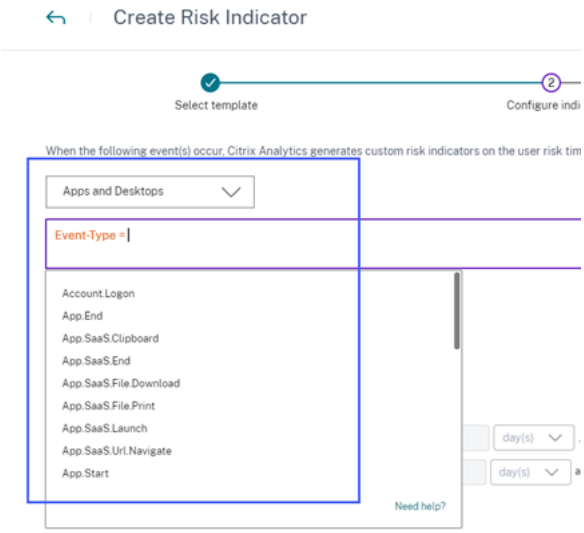
Was ist neu

Automatisch vorgeschlagene Werte für die Dimensionen im benutzerdefinierten Risikoindikator Wenn Sie auf der Seite "Benutzerdefinierter Risikoindikator"eine Dimension und einen gültigen Operator in der Bedingungsleiste auswählen, werden die Werte für die Dimension automatisch angezeigt. Wählen Sie einen Wert aus der Liste der automatischen Vorschläge aus oder geben Sie je nach Anwendungsfall manuell einen Wert ein. Wenn Sie einen Wert eingeben, werden die in den Datensätzen verfügbaren übereinstimmenden Werte automatisch vorgeschlagen.

Die für eine Dimension vorgeschlagene Werteliste ist entweder in der Datenbank vordefiniert (bekannte Werte) oder basiert auf historischen Ereignissen.

Wenn Sie beispielsweise die Dimension `Event-Type` und den Zuweisungsoperator auswählen, werden die bekannten Werte automatisch vorgeschlagen. Sie können je nach Anforderung einen Wert auswählen.

Weitere Informationen finden Sie unter Benutzerdefinierte Risikoindikatoren.



09. Februar 2022

Was ist neu

Neue benutzerdefinierte Rollen für die Administratoren Als Citrix Cloud-Administrator mit voller Zugriffsberechtigung können Sie andere Administratoren einladen, Security Analytics in Ihrer Organisation zu verwalten. Sie können den eingeladenen Administratoren jetzt die folgenden benutzerdefinierten Rollen zuweisen:

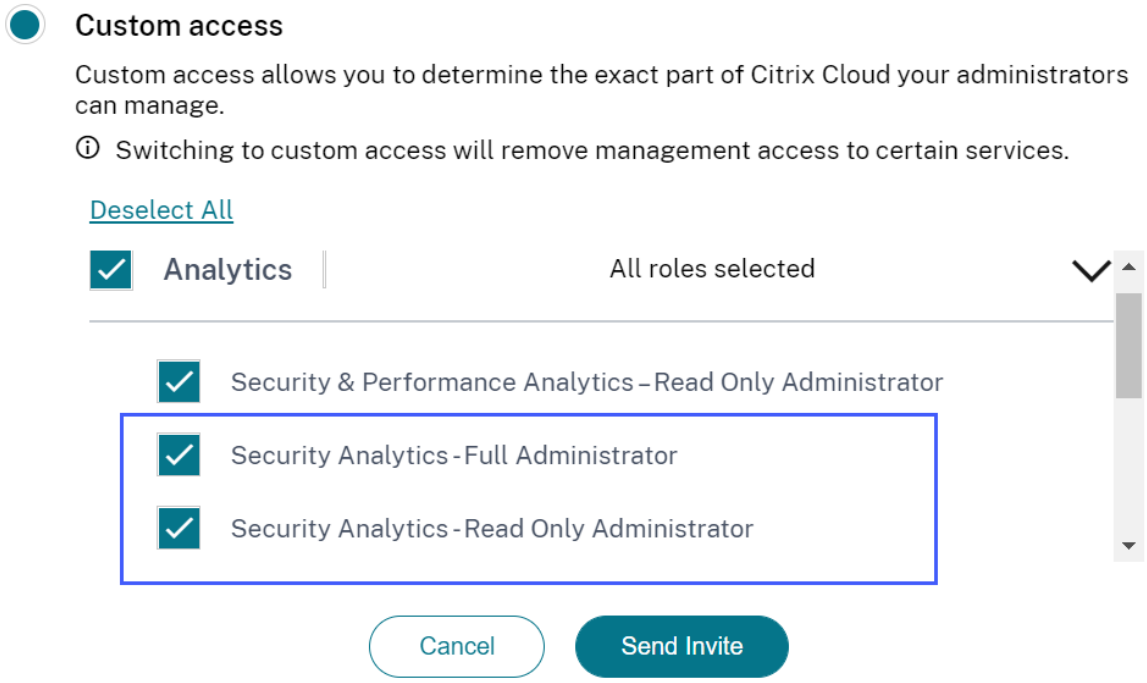
- Sicherheitsanalysen —Volladministrator

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Sicherheitsanalysen —Nur-Lese-Administrator

Mit der benutzerdefinierten Rolle können Sie Ihren Administratoren entweder Nur-Lese- oder Vollzugriffsberechtigungen erteilen und ihnen ermöglichen, die verschiedenen Funktionen von Security Analytics zu verwalten.

Weitere Informationen zu den Zugriffsberechtigungen für diese benutzerdefinierten Rollen finden Sie unter Verwalten von Administratorrollen für Security Analytics.



Unterstützung von E-Mail-Benachrichtigungen für Administratoren mit benutzerdefiniertem Zugriff Wenn Sie ein Citrix Cloud-Administrator mit benutzerdefinierten Zugriffsberechtigungen (schreibgeschützt oder Vollzugriff) zur Verwaltung von Security Analytics sind, erhalten Sie jetzt die folgenden Benachrichtigungen:

- Wöchentliche Benachrichtigungen über die in Ihrem Unternehmen entdeckten Sicherheitsrisiken. Weitere Informationen finden Sie unter Wöchentliche E-Mail-Benachrichtigung.
- Benachrichtigungen über die Risikoindikatoren, wenn die Aktion **Administrator (e) benachrichtigen** manuell angewendet oder durch eine Richtlinie ausgelöst wird. Weitere Informationen finden Sie unter Richtlinien und Maßnahmen.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

28. Januar 2022

Was ist neu

Einführung von Risikoindikatoren für verdächtige Anmeldungen für Content Collaboration und Gateway Citrix Analytics for Security erkennt jetzt verdächtige Benutzeranmeldungen basierend auf mehreren Kontextfaktoren wie:

- Der Standort wird in Bezug auf den Benutzer und die Organisationshistorie als ungewöhnlich angesehen
- Das Gerät wird in Bezug auf den Benutzer und die Organisationshistorie als ungewöhnlich angesehen
- Das Netzwerk wird in Bezug auf den Benutzer und die Organisationshistorie als ungewöhnlich angesehen.
- Die IP-Adresse wird basierend auf den Feeds der IP-Bedrohungsinformationen als verdächtig eingestuft

Wenn sich ein Benutzer aufgrund der Kombination dieser Faktoren aus einem verdächtigen Kontext anmeldet, wird der Risikoindikator ausgelöst.

Dieser Risikoindikator ersetzt den Risikoindikator Zugriff von einem ungewöhnlichen Standort, der mit den Datenquellen Citrix Content Collaboration und NetScaler Gateway verknüpft ist. Alle vorhandenen Richtlinien, die auf dem Risikoindikator Zugriff von einem ungewöhnlichen Standort aus basieren, werden automatisch mit dem neuen Risikoindikator - Verdächtige Anmeldung- verknüpft.

Weitere Informationen zu den Risikoindikatoren finden Sie unter Verdächtige Anmeldung —Content Collaboration und Suspicious Logon —Gateway.

Weitere Informationen zum Schema der Risikoindikatoren finden Sie unter Citrix Analytics-Datenformat für SIEM.

20. Januar 2022

Was ist neu

Microsoft Azure Active Directory-Integration Sie können jetzt Ihr Azure Active Directory mit Citrix Analytics for Security verbinden mit:

- Importieren Sie die Benutzerdetails und Benutzergruppen aus der Domäne Ihrer Organisation in Citrix Analytics for Security.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Bereichern Sie die Benutzerprofile mit zusätzlichen Details wie Berufsbezeichnung, Organisation, Bürostandort, E-Mail und Kontaktdaten, die Ihnen bei der Risikountersuchung und -analyse helfen.

Weitere Informationen finden Sie unter Azure Active Directory-Integration.

18. Januar 2022

Was ist neu

Unterstützung der Share-Link-Aktionen bei allen Risikoindikatoren für Content Collaboration Zuvor konnten Sie die Aktionen zum Teilen von Links anwenden: **Alle Links verfallen** und **Link zur Freigabe nur zum Anzeigen ändern für die folgenden Freigabelink-basierten** Risikoindikatoren, die mit dem Content Collaboration Service verknüpft sind:

- Anonymer Link zum sensiblen Teilen herunterladen
- Übermäßige Link-Downloads
- Übermäßige Dateifreigabe

Mit dieser Version können Sie nun die Freigabelinkaktionen auf die folgenden benutzerbasierten Risikoindikatoren anwenden, die mit dem Content Collaboration Service verknüpft sind:

- Zugang von einem ungewöhnlichen Ort
- Übermäßiger Zugriff auf vertrauliche Dateien
- Übermäßige Dateiuploads
- Übermäßige Dateidownloads
- Übermäßiges Löschen von Dateien oder Ordnern
- Malware-Dateien wurden erkannt
- Ransomware-Aktivität verdächtigt
- Ungewöhnliche Authentifizierungsfehler

Sie können die Freigabelinkaktionen auch auf die benutzerdefinierten Risikoindikatoren anwenden, die mit dem Content Collaboration Service verknüpft sind.

Weitere Informationen zu den Maßnahmen und Risikoindikatoren finden Sie in den folgenden Artikeln:

- Richtlinien und Maßnahmen
- Risikoindikatoren für die Content Collaboration
- Benutzerdefinierte Risikoindikatoren

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Die Integration mit SIEM ist jetzt allgemein verfügbar Sie können Citrix Analytics for Security in Ihre Security Information and Event Management (SIEM) -Dienste integrieren und die Benutzerdaten aus der Citrix IT-Umgebung in Ihr SIEM exportieren. Die Integration hilft Ihnen, die aus verschiedenen Quellen gesammelten Daten zu korrelieren und einen ganzheitlichen Überblick über die Sicherheit Ihres Unternehmens zu erhalten.

Derzeit können Sie Citrix Analytics for Security mit den folgenden Diensten integrieren:

- Splunk
- Sentinel
- Elastische Suche
- Andere SIEM-Dienste mithilfe eines Kafka- oder Logstash-basierten Datenkonnektors

Weitere Informationen finden Sie unter Integration von Sicherheitsinformationen und Ereignismanagement (SIEM).

23. Dezember 2021

Was ist neu

Verbesserungen der Risikoindikatoren für Freigabelinks Folgende Verbesserungen wurden vorgenommen:

- Sie können jetzt eine Richtlinie mit dem Risikoindikator für den **Download von anonymen vertraulichen Freigabelinks** erstellen.
- Der Risikoindikator für **anonyme sensible Freigaben** wurde in **anonyme sensible Freigabelink-Download** umbenannt, um ihn als Risikoindikator für Freigabelinks zu unterscheiden.
- Der Risikoindikator für **übermäßige Downloads** wird in **Exzessives Herunterladen von Freigabelinks** umbenannt, um ihn als Risikoindikator für Freigabelinks zu unterscheiden und ihn vom benutzerbasierten Risikoindikator für **übermäßige Dateidownloads** zu unterscheiden.

Weitere Informationen finden Sie unter Risikoindikatoren für Citrix Share-Links.

21. Dezember 2021

Was ist neu

Senden Sie Benachrichtigungen über Risikoindikatoren an Nicht-Citrix Cloud-Administratoren Sie können jetzt die Nicht-Citrix Cloud-Administratoren in Ihrer Organisation mit der Aktion **Adminis-**

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

trator (e) benachrichtigen .

Um diese Administratoren zu benachrichtigen, erstellen Sie eine E-Mail-Verteilerliste. Wählen Sie die Administratoren in der E-Mail-Verteilerliste entweder aus den externen Domänen aus, die mit Citrix Cloud verbunden sind, oder verwenden Sie ihre E-Mail-Adressen direkt. Wenn **Sie die Aktion Administrator (e) benachrichtigen** anwenden, wählen Sie die E-Mail-Verteilerliste aus, die Nicht-Citrix Cloud-Administratoren enthält.

Weitere Informationen finden Sie unter E-Mail-Verteiler.

20. Dezember 2021

Was ist neu

Senden Sie Benutzerantwort-Benachrichtigungen an Ihre Content Collaboration-Benutzer Zusätzlich zu Ihren Active Directory-Benutzern können Sie jetzt die Aktion **Endbenutzer-Antwort anfordern** auf Ihre Content Collaboration-Benutzer anwenden.

Diese Aktion sendet E-Mail-Benachrichtigungen an die Benutzer, wenn Citrix Analytics ungewöhnliche Aktivitäten in ihren Citrix Konten feststellt. Weitere Informationen zur Aktion **Endbenutzer-Antwort anfordern** finden Sie unter Richtlinien und Aktionen.

Access Control wurde in Secure Workspace Access umbenannt In den Dashboards und Berichten von **Security** Analytics werden alle Labels der **Zugriffssteuerung** jetzt als **Secure Workspace Access** aktualisiert, um sie an den umbenannten Produktnamen anzupassen.

Beispielsweise werden auf der Seite **Datenquellen**, der **Self-Service-Suchseite** und der Seite **Richtlinien** die Beschriftungen der Zugriffssteuerung in Secure Workspace Access umbenannt.

Problem behoben

- Wenn Sie für die Datenquelle Apps und Desktops den Suchbericht als CSV-Datei herunterladen, werden einige Feldwerte in der CSV-Datei als nicht verfügbar (Nicht verfügbar) angezeigt, obwohl ihre Werte verfügbar sind. Beispielsweise werden die Werte der Felder wie `Download File Name`, `Session Launch Type` und `Workspace App Version` auf der **Self-Service-Suchseite** angezeigt, aber in der heruntergeladenen CSV-Datei sehen Sie diese Werte als nicht verfügbar (Nicht zutreffend). Dieses Problem ist jetzt behoben. [CAS-62299]

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

09. Dezember 2021

Was ist neu

Erstellen Sie Ihre individuellen Risikoindikatoren ganz einfach mit Vorlagen Sie können jetzt eine Vorlage basierend auf Ihrem Anwendungsfall auswählen und einen benutzerdefinierten Risikoindikator erstellen. Die Vorlagen unterstützen Sie durch die Bereitstellung vordefinierter Abfragen und Parameter. Es erleichtert Ihnen die Erstellung eines benutzerdefinierten Risikoindikators.

Weitere Informationen finden Sie unter Benutzerdefinierte Risikoindikatoren.

07. Dezember 2021

Problem behoben

- In Citrix Analytics for Security erhalten Sie nicht die Ereignisse der Benutzer, die den Citrix Secure Browser verwenden, der im September 2021 veröffentlicht wurde. Das Problem tritt auf, weil die Richtlinie zur **Verfolgung von Hostnamen** in Citrix Secure Browser nach Version September 2021 nicht sichtbar ist und daher nicht für die Integration mit Citrix Analytics for Security aktiviert werden kann. Dieses Problem ist jetzt behoben. [CAS-62254]

02. Dezember 2021

Was ist neu

Risikoindikator für Malware-Dateien erkannt Sie können jetzt eine Warnung erhalten, wenn ein Benutzer eine infizierte Datei in Content Collaboration hochlädt.

Der Risikoindikator erkennt eine Datei, die mit einer Malware wie Trojanern, Viren oder anderen bösartigen Bedrohungen infiziert ist. Es bietet Einblick in die Details der schädlichen Datei wie den Eigentümer der Datei, den Virusnamen und den Speicherort der Datei.

Der mit dem Risikoindikator für **erkannte Malware-Dateien** verbundene Risikofaktor ist der dateibasierte Risikoindikator.

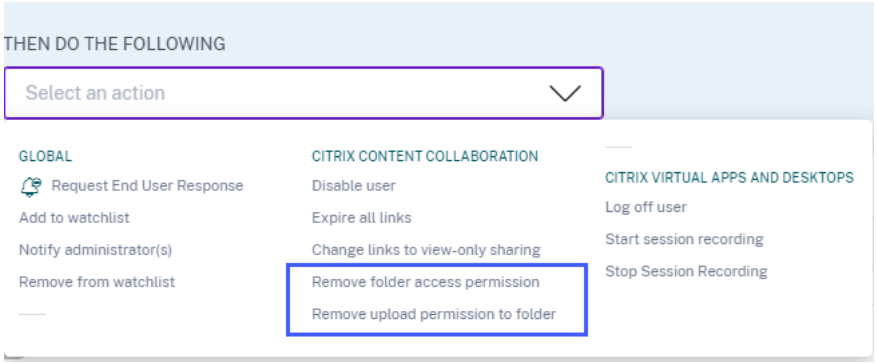
Weitere Informationen zum Risikoindikator und zu den Aktionen, die Sie anwenden können, finden Sie im Risikoindikator für erkannte Malware-Dateien.

Neue Aktionen für die Datenquelle Content Collaboration Sie können die folgenden Aktionen anwenden, wenn der Risikoindikator für **erkannte Malware-Dateien** für einen Benutzer ausgelöst wird:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Entfernen der Zugriffsberechtigung für Ordner**. Sie können die Zugriffsberechtigung des Benutzers sperren, der die infizierte Datei hochlädt. Der Benutzer kann nicht auf den Ordner zugreifen, in den die infizierte Datei hochgeladen wurde.
- **Entfernen Sie die Upload-Berechtigung für Ordner**. Sie können die Upload-Berechtigung des Benutzers blockieren, der die infizierte Datei hochlädt. Der Benutzer kann keine Datei in den Ordner hochladen, in den die infizierte Datei hochgeladen wurde.

Weitere Informationen zu den Aktionen für Content Collaboration finden Sie unter Richtlinien und Aktionen.



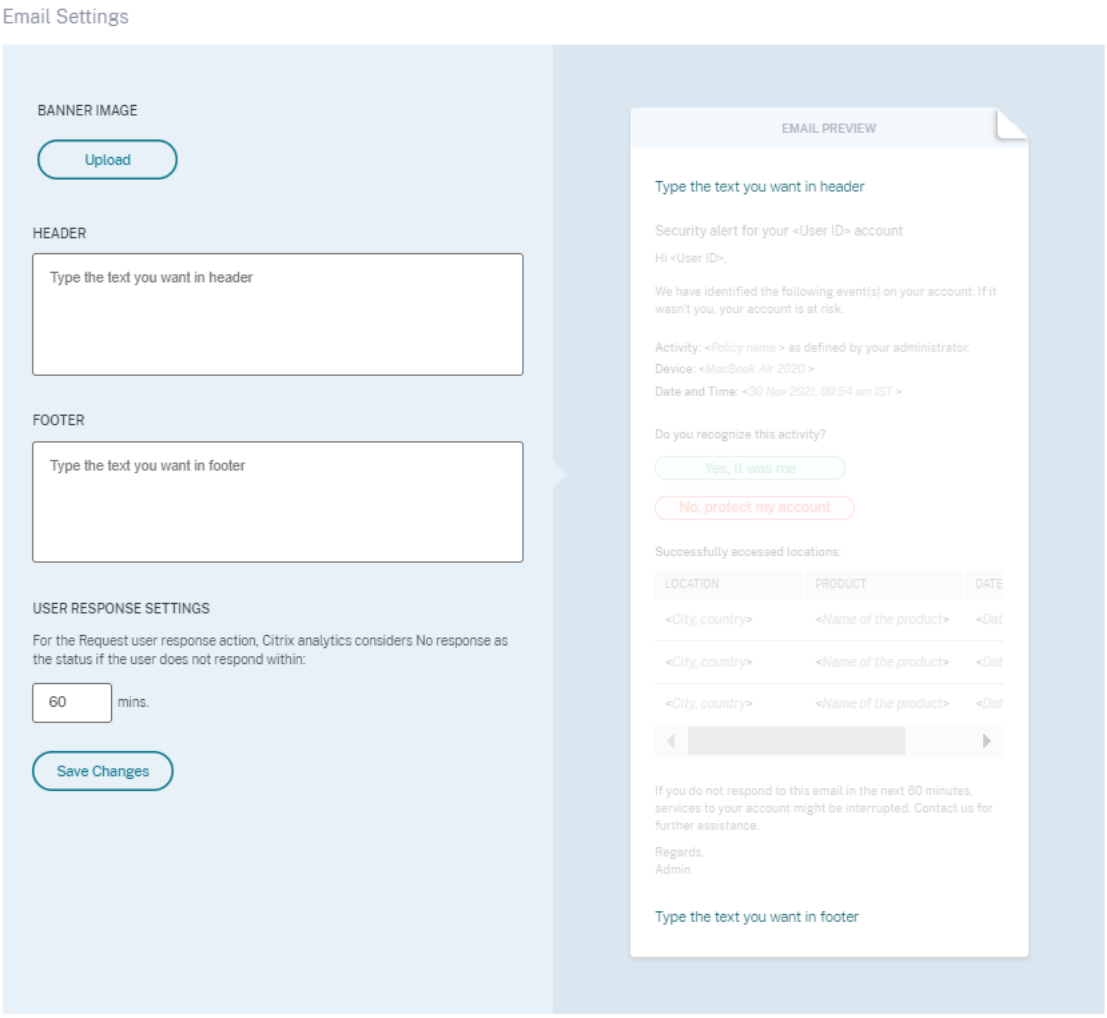
29. November 2021

Was ist neu

Verbesserungen der E-Mail-Einstellungen für Benutzerbenachrichtigungen Als Administrator können Sie jetzt Bannerbild, Kopf- und Fußzeilentext zur E-Mail-Vorlage für Benutzerantworten hinzufügen. Diese Felder erhöhen die Legitimität Ihrer E-Mail und erhöhen so die Aufmerksamkeit und Antworten der Benutzer auf Ihre E-Mail.

Weitere Informationen finden Sie unter E-Mail-Einstellungen für Endbenutzer.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

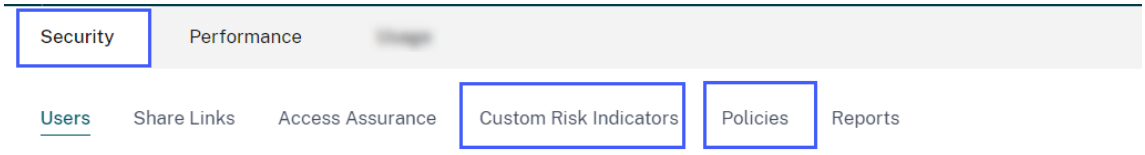


26. November 2021

Was ist neu

Menüänderungen für benutzerdefinierte Risikoindikatoren und Richtlinien Die Navigationslinks der folgenden Funktionen wurden aktualisiert:

- Benutzerdefinierte Risikoindikatoren: Verwenden Sie diese Funktion, indem Sie auf **Sicherheit > Benutzerdefinierte Risikoindikatoren**
- Richtlinien: Verwenden Sie diese Funktion, indem Sie auf **Sicherheit > Richtlinien**klicken.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

25. November 2021

Was ist neu

Verbesserungen bei der Integration von Sicherheitsinformationen und Ereignismanagement (SIEM)

> **Hinweis**
>
> Diese Integration ist in der Vorschau.

Sie können jetzt Citrix Analytics for Security in die folgenden SIEM-Dienste integrieren:

- Sentinel
- Elasticsearch mit Visualisierungsdiensten wie Kibana und SIEM-Service wie LogRythm
- Alle anderen SIEM-Dienste, die die Logstash-Datenerfassungsmaschine verwenden

Importieren Sie je nach Ihren Geschäftsanforderungen die Daten der Benutzer aus Citrix Analytics for Security in Ihren SIEM-Dienst. Diese Integration ermöglicht es Ihren Security Operations-Teams, Daten aus unterschiedlichen Protokollen innerhalb der SIEM-Dienste in Ihrem Unternehmen zu korrelieren, zu analysieren und zu durchsuchen, sodass sie die Sicherheitsrisiken identifizieren und schnell beheben können.

Weitere Informationen finden Sie unter Integration von Sicherheitsinformationen und Ereignismanagement (SIEM).

09. November 2021

Problem behoben

- Bei einigen Mandanten funktionieren die Benutzerrichtlinien nicht. Dieses Problem trat auf, wenn die Warnungen für die virtuellen Apps leere Zeichenfolgenwerte für die Domänen hatten. Dieses Problem ist jetzt behoben. [CAS-60920]

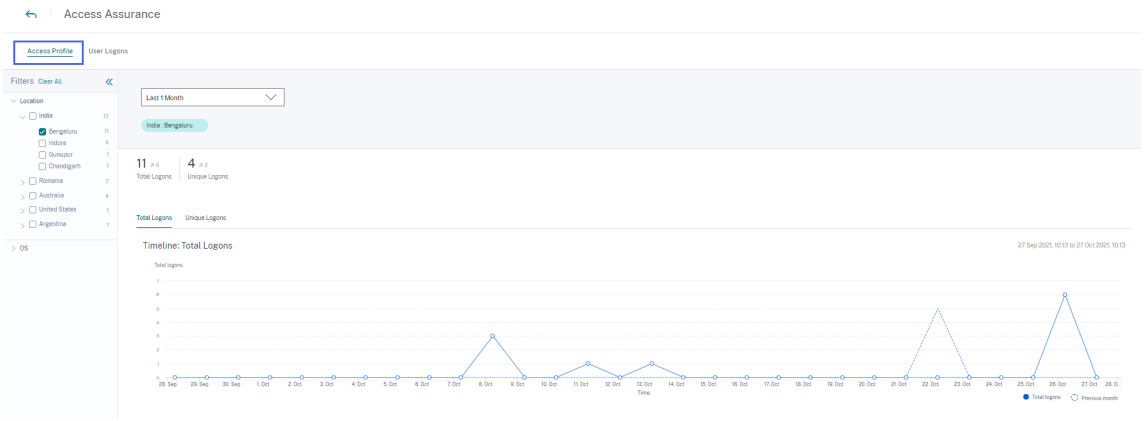
02. November 2021

Was ist neu

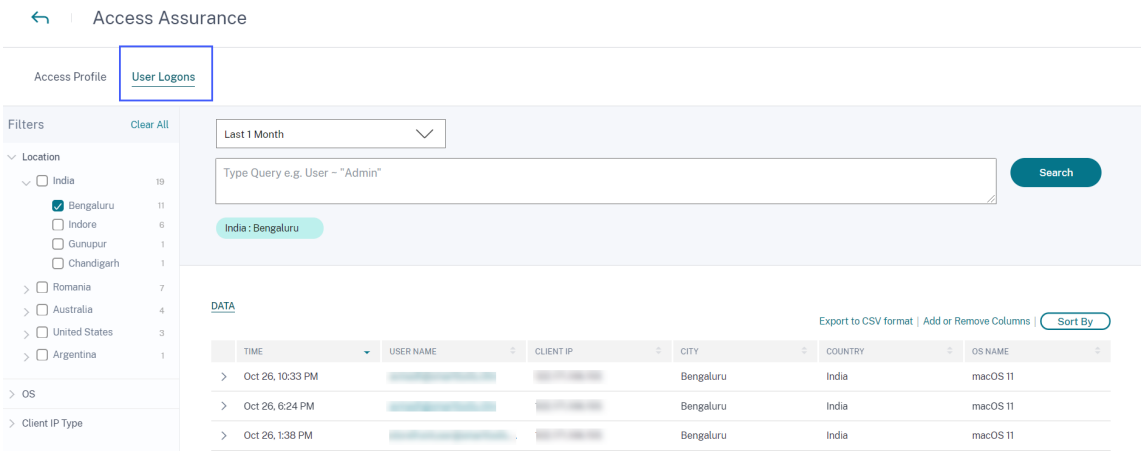
Zugriffsprofile und Anmeldedetails der Benutzer von Citrix Virtual Apps and Desktops und Citrix DaaS anzeigen Im **Access Assurance Location** Dashboard können Sie die Zugriffsprofile und die Anmeldedetails der Benutzer anzeigen, die sich bei virtuellen Apps und virtuellen Desktops angemeldet haben. Diese Informationen helfen Ihnen bei der Untersuchung und Analyse von Bedrohungen.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Auf der Seite **Zugriffsprofil** finden Sie eine Zusammenfassung der Benutzerzugriffe von den ausgewählten Speicherorten aus. Sie können die Trendanalyse und die Top-Zugriffsereignisse der gesamten Benutzer und die Anmeldungen der einzelnen Benutzer anzeigen.



- Auf der Seite **Benutzeranmeldungen** werden die Details der Benutzeranmeldungen an virtuellen Apps und virtuellen Desktops von den ausgewählten Speicherorten aus angezeigt.

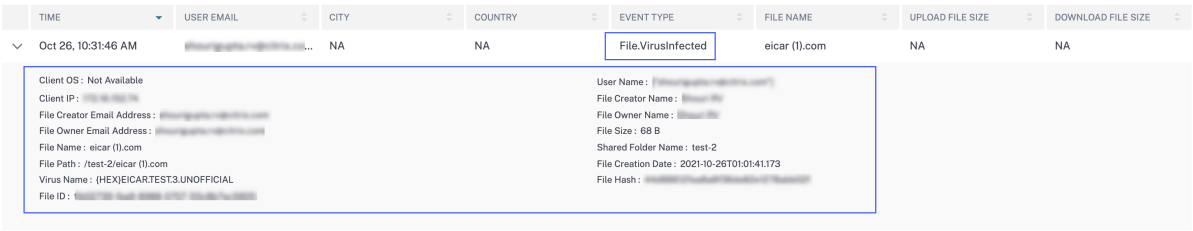


Weitere Informationen finden Sie im Dashboard für Zugriffssicherungsstandorte.

Malware-Protokolle auf der Self-Service-Suchseite für Content Collaboration anzeigen Auf der Self-Service-Seite für Content Collaboration können Sie jetzt das Malware-Ereignis `File.VirusInfected` und die zugehörigen Protokolle anzeigen. Dieses Ereignis wird ausgelöst, wenn ein Benutzer von Content Collaboration eine Datei hochlädt, die mit einer Malware infiziert ist.

Weitere Informationen finden Sie unter Self-Service-Suche nach Content Collaboration

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Problem behoben

- Einige Benutzer von Content Collaboration werden bei der Verarbeitung der Ereignisse in Citrix Analytics fälschlicherweise als Nicht-Mitarbeiter festgelegt. Daher werden die Benutzer nicht als entdeckte Benutzer identifiziert. Dieses Problem ist jetzt behoben. [CAS-59608]

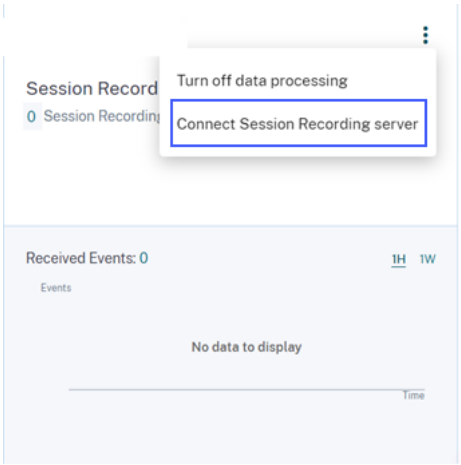
20. Oktober 2021

Was ist neu

Serverintegration für Sitzungsaufzeichnung Für Ihre Citrix Virtual Apps and Desktops und Citrix DaaS-Bereitstellung können Sie jetzt Ihre Sitzungsaufzeichnungsserver so konfigurieren, dass die Benutzerereignisse an Citrix Analytics for Security gesendet werden. Diese Benutzerereignisse werden verarbeitet, um umsetzbare Einblicke in das Verhalten der Benutzer zu erhalten.

Wechseln Sie auf der Seite **Datenquellen > Sicherheit** zur Sitekarte **Virtual Apps and Desktops** . Klicken Sie auf der Site-Karte **Sitzungsaufzeichnung** auf vertikale Ellipse (), und wählen Sie dann **Sitzungsaufzeichnungsserver verbinden**aus.

Weitere Informationen finden Sie unter Verbinden mit der Bereitstellung der Sitzungsaufzeichnung.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

19. Oktober 2021

Was ist neu

Verbesserungen der E-Mail-Vorlage für Administratoren benachrichtigen Die E-Mail-Benachrichtigung, die ein Administrator nach Anwendung der Aktion **Administrator (en) benachrichtigt** erhält, wurde verbessert, um bessere Einblicke in die riskanten Benutzerereignisse zu erhalten.

- Die Benachrichtigung enthält nun detaillierte Informationen über den ausgelösten Risikoindikator oder die angewandte Richtlinie. Sie können beispielsweise den Schweregrad und die ausgelöste Zeit der Standard- und benutzerdefinierten Risikoindikatoren anzeigen. Die Inhaltsstruktur wurde für eine bessere Lesbarkeit verbessert.
- Die Administratoren können jetzt direkt über die E-Mail-Benachrichtigung auf die Benutzerzeitleiste zugreifen und Details zu den riskanten Ereignissen anzeigen.
- Eine Feedback-Option wurde in der Benachrichtigung hinzugefügt. Diese Option hilft dabei, die Antworten der Administratoren zu sammeln und den Inhalt der Benachrichtigung basierend auf den Antworten kontinuierlich zu verbessern.

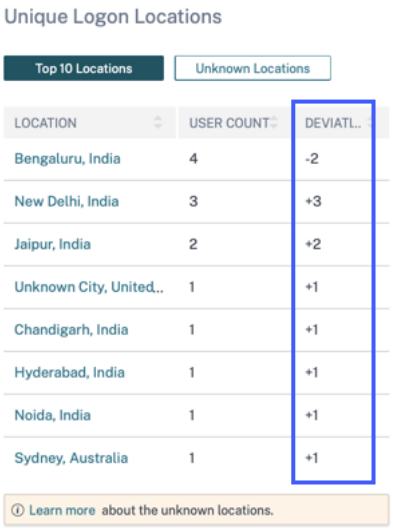
Weitere Informationen zur Aktion **Administrator (s) benachrichtigen** finden Sie unter Richtlinien und Aktionen.

Verbesserungen bei der Zusammenfassung der Benutzeranmeldung

- Sie können jetzt den Aufwärts- oder Abwärtstrend der Benutzeranmeldungen für die weltweite Gesamtzahl der Benutzeranmeldungen und weltweit eindeutigen Benutzeranmeldungen anzeigen.

- In der Spalte **DEVIATION** in der Tabelle **Unique Logon Locations** wird die Änderung der eindeutigen Benutzeranmeldungen für einen bestimmten Standort nach oben oder unten angezeigt.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Diese Metriken helfen Ihnen zu verstehen, wie sich die Benutzeranmeldungen (positiv oder negativ) gegenüber der Vorperiode geändert haben. Es bietet Einblick in die Benutzerinteraktionen mit Ihren Citrix Virtual Apps and Desktops und Citrix DaaS-Bereitstellungen.

Weitere Informationen finden Sie unter Standort-Dashboard für die Zugriffssicherung.

Problem behoben

- Auf dem Dashboard für **Zugriffssicherungsstandorte** zeigen die **Benutzeranmeldungszusammenfassungskarten** nicht die Benutzeranmeldungsmetriken an (weltweite Gesamtzahl der Benutzeranmeldungen, weltweit eindeutige Benutzeranmeldungen und Länder haben Benutzeranmeldungen), wenn sich keine Benutzer von außerhalb der Geofence-Bereiche anmelden. Dieses Problem ist jetzt behoben. [CAS-59595]

01. Oktober 2021

Was ist neu

Audit-Protokolle auf der Self-Service-Suche nach Content Collaboration Bei der Self-Service-Suche nach Content Collaboration können Sie jetzt die Überwachungsprotokolle anzeigen. Diese Protokolle bieten Einblicke in die Berechtigungen und Aktionen, die von den Content Collaboration Administratoren auf die Benutzerkonten angewendet werden. Mithilfe dieser Daten können Sie überprüfen, ob die Content Collaboration-Administratoren gültige Maßnahmen für ihre Benutzerkonten ergriffen haben. Als Sicherheitsadministrator hilft es Ihnen bei der Risikountersuchung und -analyse.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Weitere Informationen zu Überwachungsprotokollen finden Sie unter Self-Service-Suche nach Content Collaboration.

Problem behoben

Die Administratoren, die sich mit Azure AD bei Citrix Cloud anmelden, können nicht auf den Citrix Analytics Service zugreifen, wenn die vorherige abgelaufene Sitzungs-ID zusammen mit der neuen Sitzungs-ID geliefert wird. Dieses Problem ist jetzt behoben. [CAS-59385]

29. September 2021

Was ist neu

Das Standort-Dashboard zur Zugriffssicherung ist jetzt allgemein Das Dashboard bietet Einblick in die Speicherorte Ihrer Citrix Virtual Apps and Desktops und Citrix DaaS-Benutzer. Sie können die Benutzer identifizieren, deren Standorte ungewöhnlich sind, indem Sie Geofencing aktivieren und geeignete Maßnahmen ergreifen, um Bedrohungen zu verhindern.

Um das Dashboard anzuzeigen, klicken Sie auf **Sicherheit > Zugriffsversicherung**. Wählen Sie den Zeitraum aus, für den Sie die Standortdetails anzeigen möchten.

Weitere Informationen finden Sie unter Standort-Dashboard für die Zugriffssicherung.

15. September 2021

Was ist neu

Benutzerdefinierte Verbesserungen der Risikoindikatoren

- Wenn ein benutzerdefinierter Risikoindikator ausgelöst wird, wird er sofort in der Benutzerzeitleiste angezeigt. Die Risikoübersicht und die Risikobewertung des Benutzers werden jedoch nach einigen Minuten (ca. 15-20 Minuten) aktualisiert.
- Wenn Sie die Attribute wie Zustand, Risikokategorie, Schweregrad und Name eines vorhandenen benutzerdefinierten Risikoindikators auf der Benutzerzeitleiste ändern, können Sie weiterhin die vorherigen Vorkommen des benutzerdefinierten Risikoindikators (mit den alten Attributen) anzeigen, die für den Benutzer ausgelöst wurden.
- Wenn Sie einen benutzerdefinierten Risikoindikator löschen, können Sie auf der Benutzerzeitleiste weiterhin die vorherigen Vorkommen des benutzerdefinierten Risikoindikators anzeigen, die für den Benutzer ausgelöst wurden.

Weitere Informationen finden Sie unter Benutzerdefinierte Risikoindikatoren.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

14. September 2021

Was ist neu

Einführung des Risikoindikators für verdächtige Anmeldung Citrix Analytics for Security erkennt jetzt verdächtige Benutzeranmeldungen basierend auf mehreren Kontextfaktoren wie:

- Der Standort wird in Bezug auf den Benutzer und die Organisationshistorie als ungewöhnlich angesehen
- Das Gerät wird in Bezug auf den Benutzer und die Organisationshistorie als ungewöhnlich angesehen
- Das Netzwerk wird in Bezug auf den Benutzer und die Organisationshistorie als ungewöhnlich angesehen.
- Die IP-Adresse wird basierend auf den Feeds der IP-Bedrohungsinformationen als verdächtig eingestuft

Wenn sich ein Benutzer von Citrix Virtual Apps and Desktops und Citrix DaaS aufgrund der Kombination dieser Faktoren aus einem verdächtigen Kontext anmeldet, wird der Risikoindikator ausgelöst.

Dieser Risikoindikator ersetzt den Indikator **Zugriff von einem ungewöhnlichen Standortrisikoindikator**, der mit der Datenquelle Citrix Virtual Apps and Desktops verknüpft ist. Alle vorhandenen Richtlinien, die auf dem Risikoindikator **Zugriff von einem ungewöhnlichen Standort** aus basieren, werden automatisch mit dem neuen Risikoindikator - **Verdächtige Anmeldung**-verknüpft.

Weitere Informationen zum Risikoindikator finden Sie unter Citrix Virtual Apps and Desktops und Citrix DaaS-Risikoindikatoren.

Verbesserung der SIEM-Nachrichten Citrix Analytics for Security sendet jetzt die Schemadetails des Indikators für **verdächtige Anmelderisiken an** Ihren SIEM-Dienst. Sie können das Schema der Indikatorzusammenfassung und die Ereignisdetails des Indikators für **verdächtige Anmelderisiken** anzeigen. Weitere Informationen finden Sie unter Citrix Analytics-Datenformat für SIEM.

Problem behoben

- Bei der Self-Service-Suche für Apps und Desktops fehlt der Client-IP-Wert in der heruntergeladenen CSV-Datei. Dieses Problem ist jetzt behoben. [CAS-58426]

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

19. August 2021

Was ist neu

Einführung der Citrix Analytics App für Splunk

> **Hinweis**
>
> Die App befindet sich in der Vorschau.

Mit Citrix Analytics App für Splunk können Sie die von Citrix Analytics for Security gesammelten Daten in Form von aufschlussreichen Dashboards auf Ihrem Splunk anzeigen. Die Dashboards geben Einblicke in die riskanten Ereignisse Ihrer Benutzer. Sie können die Citrix Analytics-Daten auch mit Protokollen korrelieren, die aus verschiedenen anderen Datenquellen gesammelt wurden. Die Korrelation hilft Ihnen, Beziehungen zwischen Ereignissen zu finden und rechtzeitig Maßnahmen zum Schutz Ihrer IT-Umgebung zu ergreifen.

Um die App herunterzuladen, gehe zu Splunkbase. Installieren Sie die App auf Ihrem Splunk-Suchkopf.

Weitere Informationen finden Sie unter Citrix Analytics App für Splunk.

Benutzerdefiniertes Risikoindikatorschema für SIEM In Ihrem SIEM-Dienst können Sie jetzt das Schema der benutzerdefinierten Risikoindikatoren anzeigen, die für Citrix Virtual Apps and Desktops und Citrix DaaS erstellt wurden. Diese Daten helfen Ihnen, einen Einblick in die Haltung Ihres Unternehmens im Sicherheitsrisiko zu erhalten.

Weitere Informationen zum benutzerdefinierten Risikoindikatorschema finden Sie unter Citrix Analytics data format for SIEM.

Unterstützung für Citrix Director als Datenquelle Sie können jetzt Ihre on-premises Sites in Citrix Director so konfigurieren, dass Ereignisse an Security Analytics gesendet werden. Diese Ereignisse werden verwendet, um die mit Security Analytics verbundenen Benutzer zu ermitteln und die Versionen der Workspace-App zu ermitteln, die auf den Geräten der Benutzer installiert sind.

Standardmäßig ist die Datenverarbeitung nach der Entdeckung der Websites aktiviert. Auf der **Überwachungskarte** können Sie alle verbundenen Sites anzeigen.

Weitere Informationen zum Konfigurieren Ihrer Sites im Director finden Sie unter Citrix Virtual Apps and Desktops und Citrix DaaS-Datenquelle.

Unterstützung für Geofence im Dashboard für den Standort der Zugriffssicherung Sie können jetzt die **Geofence-Einstellungen** im Dashboard verwenden, um die Geofence-Bereiche auszuwählen und zu aktivieren. Nach dem Aktivieren des Geofence zeigt die Karte die Geofence-Gebiete (Länder)

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

an und der Benutzer meldet sich von außerhalb und innerhalb des Geofence an. Diese Funktion verwendet die **außerhalb des Geofence-Risikoindikators gestartete CVAD-Sitzung**, um die Benutzeranmeldungen zu überwachen.

Weitere Informationen finden Sie unter Standort-Dashboard für die Zugriffssicherung.

Status der Workspace-App auf der Seite Benutzer Auf der Seite **Benutzer** können Sie jetzt den Status der Citrix Workspace-App-Clients anzeigen, die von Citrix Analytics unterstützt werden. Die Seite zeigt den folgenden Status:

- Unterstützt
- Teilweise unterstützt
- Nicht unterstützt
- Nicht verfügbar
- Inaktiv

Der Status hilft Ihnen, nicht unterstützte Clientversionen zu identifizieren, die von den Benutzern verwendet werden, und empfiehlt den Benutzern, ihre Clients auf eine unterstützte Version zu aktualisieren. Eine unterstützte Clientversion sendet die Benutzerereignisse an Citrix Analytics.

> **Hinweis**
>
> Um den Status der Citrix Workspace-App anzuzeigen, müssen Sie Ihre Citrix Director-Datenquelle einbeziehen. Andernfalls wird der Status für alle Citrix Virtual Apps and Desktops und Citrix DaaS-Benutzer als **Inaktiv**angezeigt.

Weitere Informationen finden Sie im Benutzer-Dashboard.

Unterstützung für den Operator IS EMPTY Beim Erstellen eines benutzerdefinierten Risikoindikators können Sie jetzt den Operator **IS EMPTY** in Ihrem Zustand verwenden, um nach Null- oder Leerdimension zu suchen.

> **Hinweis**
>
> Der Operator funktioniert nur für stringartige Dimensionen wie App-Name, Browser und Country.

Weitere Informationen finden Sie unter Benutzerdefinierte Risikoindikatoren.

Verbessertes Risiko-Scoring Auf der Timeline des Benutzers können Sie jetzt die Risikoübersicht eines Benutzers anzeigen. Die Risikoübersicht enthält Informationen über die mit Benutzerereignissen verbundenen Risikofaktoren. Der Risikofaktor hilft Ihnen, die Art der Anomalien in den Benutzerereignissen zu identifizieren und bestimmt auch den Risiko-Score. Das Folgende sind die Risikofaktoren:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Gerätebasierte Risikoindikatoren
- Standortbasierte Risikoindikatoren
- IP-basierte Risikoindikatoren
- Auf Anmeldeausfällen basierende Risikoindikatoren
- Datenbasierte Risikoindikatoren
- Dateibasierte Risikoindikatoren
- Benutzerdefinierte Risikoindikatoren
- Andere Risikoindikatoren

Auf der Zeitleiste des Benutzers können Sie jetzt den Filter anwenden, um die Benutzerereignisse basierend auf den Risikofaktoren anzuzeigen.

Weitere Informationen finden Sie in den folgenden Artikeln:

- Citrix Benutzerrisikoindikatoren
- Zeitleiste und Profil des Benutzerrisikos

29. Juli 2021

Veraltete Funktion

Veraltete Aktionen im Zusammenhang mit Citrix Endpoint Management Die folgenden Aktionen werden aus der Citrix Endpoint Management-Datenquelle entfernt. Mit diesen Aktionen können Sie diese Aktionen nicht mehr auf die Risikoindikatoren anwenden oder Richtlinien erstellen.

- Gerät sperren
- Endpoint Management-Admin benachrichtigen
- Benutzer benachrichtigen
- Gerät widerrufen
- Wipe device

Wenn diese Aktionen in Ihren bestehenden Richtlinien bereits verwendet werden, werden sie automatisch durch die Aktion **Zur Watchlist hinzufügen** ersetzt. Und Sie können solche Benutzer von der Watchlist aus überwachen.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

14. Juli 2021

Was ist neu

Unterstützung für den Operator IST NICHT LEER Beim Erstellen eines benutzerdefinierten Risikoindikators können Sie jetzt den Operator **IST NICHT LEER** in Ihrem Zustand verwenden, um zu überprüfen, ob die Dimension nicht leer (nicht leer) ist.

> **Hinweis**
>
> Der Operator funktioniert nur für stringartige Dimensionen wie App-Name, Browser und Country.

Beispielsweise erkennt die folgende Bedingung Benutzeranmeldeereignisse aus jedem Land, in dem der Länderwert nicht Null ist. Mit anderen Worten, der Ländername wird angegeben.

```
Event-Type = "Session.logon" AND Country IS NOT EMPTY
```

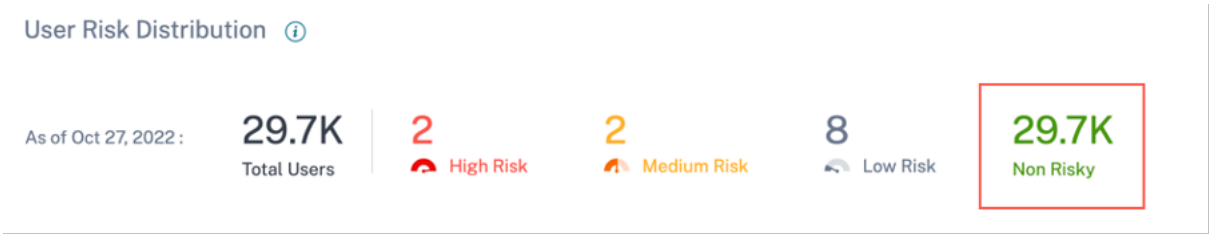
Weitere Informationen finden Sie unter Benutzerdefinierte Risikoindikatoren.

06. Juli 2021

Was ist neu

Zeigen Sie nicht riskante Benutzer im Benutzer-Dashboard an Im **Benutzer-Dashboard** können Sie jetzt die Anzahl der nicht riskanten Benutzer für den ausgewählten Zeitraum anzeigen. Diese entdeckten Benutzer werden basierend auf dem Null-Risiko-Score für den ausgewählten Zeitraum als nicht riskant identifiziert. Klicken Sie auf die Karte "**Nicht riskante Benutzer**", um alle Benutzer anzuzeigen, die einen Risikowert von Null haben.

Weitere Informationen finden Sie unter Benutzer-Dashboard.



01. Juli 2021

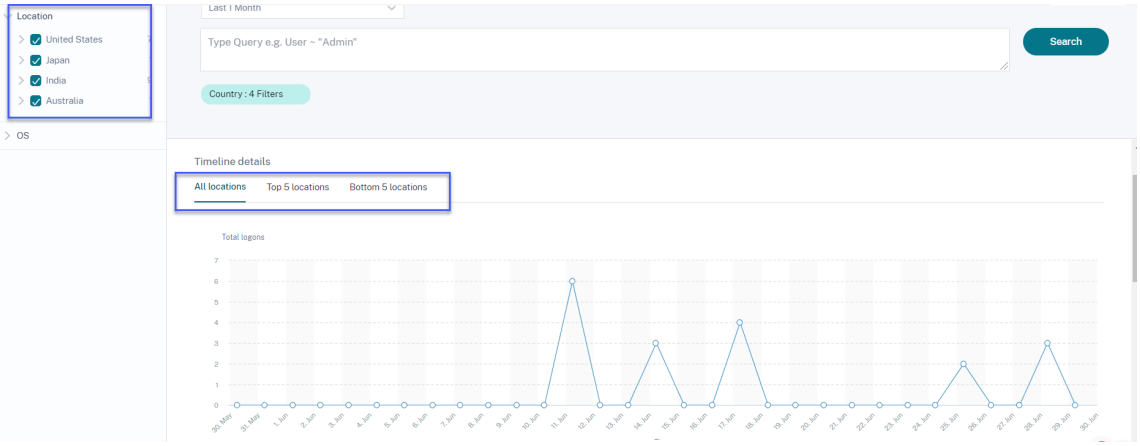
Was ist neu

Verbesserungen des Standort-Dashboards für Zugriffsversicherungen

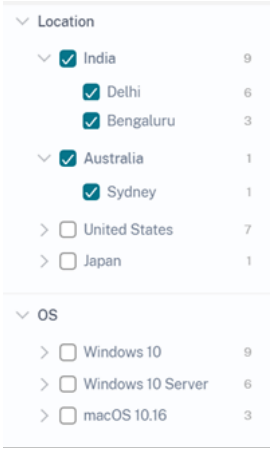
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- In der Tabelle **Top 10 Unique Logon Locations** können Sie die Anzahl der eindeutigen Benutzeranmeldungen von unbekannten Orten aus anzeigen. Diese Liste ist eine Teilmenge der 10 besten eindeutigen Anmeldeorte. Sie können auch die Gründe finden, warum die Standorte unbekannt sind, und die Möglichkeiten, die Standorte der Benutzer zu ermitteln.

- Wenn Sie auf der Seite **Zugriffsort** mehrere Standorte auswählen, können Sie die Timeline-Details der Benutzeranmeldungen von allen Standorten, den fünf besten Standorten und den fünf unteren Standorten aus anzeigen und vergleichen.



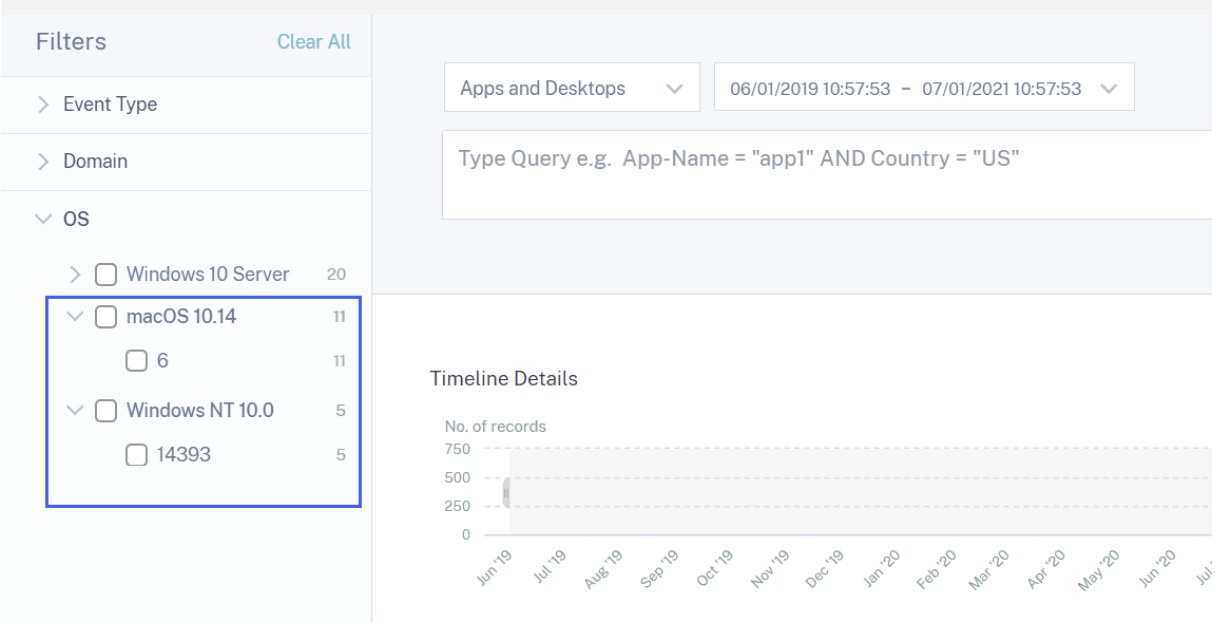
- Auf der Seite **Zugriffsort** können Sie die verschachtelten Facetten wie Land und ihre Städte, Betriebssysteme - Haupt- und Nebenversionen - verwenden. Diese Facetten ermöglichen es Ihnen, die Ereignisse auf granulare Weise zu filtern.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Weitere Informationen finden Sie unter Standort der Zugriffssicherung.

Die Betriebssystem-Facette bei der Self-Service-Suche nach Virtual Apps and Desktops wurde aktualisiert Sie können jetzt die Apps- und Desktops-Ereignisse mithilfe der verschachtelten Betriebssystemfacette filtern. Wählen Sie die Hauptversion und die einem Betriebssystem zugeordnete Nebenversion aus und filtern Sie die Ereignisse auf granulare Weise. Weitere Informationen finden Sie unter Self-Service-Suche nach Apps und Desktops.



30. Juni 2021

Was ist neu

Workspace-App-Version in benutzerdefinierter Risikoindikatorbedingung für Apps und Desktops hinzugefügt Für die Datenquelle **Apps und Desktops** können Sie jetzt die Dimension **Workspace-App-Version** verwenden, um Ihre Bedingung zu definieren und gleichzeitig einen benutzerdefinierten Risikoindikator zu erstellen. Weitere Informationen zur Dimension finden Sie unter Self-Service-Suche nach Apps und Desktops.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

23. Juni 2021

Was ist neu

Verbesserungen bei SIEM-Nachrichten Die folgenden Felder werden nun zum Schema der Risikoindikatoren hinzugefügt:

- `indicator_vector_name`- Zeigt den mit einem Risikoindikator verbundenen Risikovektor an. Die Risikovektoren sind gerätebasierte Risikoindikatoren, standortbasierte Risikoindikatoren, Anmeldeausfallbasierte Risikoindikatoren, IP-basierte Risikoindikatoren, datenbasierte Risikoindikatoren, dateibasierte Risikoindikatoren und andere Risikoindikatoren.
- `indicator_vector_id`- Die mit einem Risikovektor verknüpfte ID. ID 1 = Gerätebasierte Risikoindikatoren, ID 2 = Standortbasierte Risikoindikatoren, ID 3 = Risikoindikatoren auf Anmeldeausfällen, ID 4 = IP-basierte Risikoindikatoren, ID 5 = IP-basierte Risikoindikatoren, ID 6 = Datenbasierte Risikoindikatoren, ID 7 = Andere Risikoindikatoren und ID 999 = Nicht verfügbar.

Weitere Informationen finden Sie unter Citrix Analytics-Datenformat für SIEM.

7. Juni 2021

Was ist neu

Verbesserungen der Aktion Administrator (s) benachrichtigen Wenn Sie die Aktion **Administrator (e) benachrichtigen** auf einen Risikoindikator anwenden oder eine Richtlinie mit der Aktion erstellen, können Sie jetzt die Administratoren auswählen, die eine Benachrichtigung über das riskante Verhalten des Benutzers erhalten. Weitere Informationen zur Aktion finden Sie unter Richtlinien und Aktionen.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Unterstützung für die schreibgeschützte Freigabeaktion hinzugefügt Wenn ein Benutzer Dateien übermäßig freigibt, löst Citrix Analytics den Risikoindikator für **übermäßige Dateifreigabe** aus. Aus der Risikozeitleiste des Benutzers können Sie die Aktion **Links auf schreibgeschützte Freigabe ändern auf** den Risikoindikator für **übermäßige Dateifreigabe** anwenden. Sie können die Aktion auch auf einen bestimmten Freigabe-Link auf der Freigabe-Link-Risikozeitleiste anwenden. Diese Aktion verhindert, dass andere Benutzer die mit den Freigabe-Links verknüpften Dateien herunterladen, kopieren oder drucken. Weitere Informationen über die Aktion finden Sie unter Richtlinien und Aktionen.

18. Mai 2021

Was ist neu

Migration der Ausfallrisikoindikatoren auf benutzerdefinierte Risikoindikatoren Die folgenden Standardrisikoindikatoren werden auf vorkonfigurierte benutzerdefinierte Risikoindikatoren migriert.

Indikator für Ausfallrisiko	Datenquelle	Vorkonfigurierter individueller Risikoindikator
Erster Zugriff von neuem Gerät	Citrix Virtual Apps and Desktops von Citrix und Citrix DaaS	CVAD-Erstzugriff von neuem Gerät
Erster Zugriff von neuer IP	Citrix Gateway	Gateway-Erstzugriff von neuer IP

Mit dieser Migration zu den benutzerdefinierten Risikoindikatoren sind die Ausfallrisikoindikatoren und die damit verbundenen Algorithmen für maschinelles Lernen veraltet.

Die entsprechenden benutzerdefinierten Risikoindikatoren werden basierend auf den folgenden vorkonfigurierten Bedingungen ausgelöst:

- Wenn ein Benutzer zum ersten Mal von einem neuen Gerät aus zugreift oder von einem vorhandenen Gerät, das seit mindestens 90 Tagen nicht benutzt wurde.
- Wenn sich ein Benutzer zum ersten Mal von einer neuen IP-Adresse oder einer vorhandenen IP-Adresse anmeldet, die seit mindestens 90 Tagen nicht verwendet wurde.

Zusammen mit den vorkonfigurierten Bedingungen können Sie jetzt Ihre eigenen Bedingungen für diese benutzerdefinierten Risikoindikatoren hinzufügen, um die Bedrohungen in Ihrer Citrix Umgebung zu identifizieren. Mit dieser Option können Sie den benutzerdefinierten Risikoindikator basierend auf Ihren Sicherheitsanforderungen konfigurieren. Sie können auch Richtlinien

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

erstellen, um Aktionen auf die riskanten Ereignisse anzuwenden, die von diesen benutzerdefinierten Risikoindikatoren erkannt werden.

In der Zeitlinie des Benutzers können Sie jedoch weiterhin die zuvor ausgelösten Standard-risikoindikatoren und ihre Ereignisse anzeigen.

Die mit diesen Ausfallrisikoindikatoren verknüpften Richtlinien werden automatisch mit den entsprechenden vorkonfigurierten benutzerdefinierten Risikoindikatoren verknüpft.

Weitere Informationen finden Sie unter Vorkonfigurierte benutzerdefinierte Risikoindikatoren und -richtlinien.

Verbesserungen bei der Self-Service-Suche nach Gateway

- Der **Ereignistypfilter** wird jetzt in **Datensatztyp**umbenannt. Wählen Sie einen der folgenden Datensatztypen aus, um Ihre Ereignisse zu filtern - VPN_AI, VPN_IF und VPN_ST.
- Erweitern Sie in der Tabelle **DATA** eine Zeile für ein Benutzerereignis, um den entsprechenden Ereignistyp anzuzeigen. Die Ereignistypen können eine der folgenden sein: Authentifizierung, ICA-Datei oder Sitzungsabmeldung.

In der folgenden Tabelle wird die Korrelation zwischen den Datensatztypen und den Ereignistypen beschrieben.

Datensatztyp	Ereignistyp
VPN_AI	Authentifizierung
VPN_IF	ICA-Datei
VPN_ST	Abmelden von Sitzungen

Weitere Informationen finden Sie unter Self-Service-Suche für Gateway.

Problem behoben

- Der benutzerdefinierte Risikoindikator wird basierend auf der Groß- und Kleinschreibung der bedingten Werte ausgelöst. In den Benutzerereignissen, die Geräte-IDs in der zulässigen Liste enthalten, sehen Sie beispielsweise das folgende Verhalten:
  - Wenn Sie den Wert der Dimension `Device-ID` in Kleinbuchstaben eingeben, wird der benutzerdefinierte Indikator ausgelöst.

    ```
    Event-Type = Session.Logon AND Device-ID NOTIN ("1621d2cb-f598-5ef7-a5bf-81747496ed2e")
    ```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Wenn Sie den Wert der Dimension `Device-ID` in Großbuchstaben für dasselbe Gerät eingeben, wird der benutzerdefinierte Indikator nicht ausgelöst.

  ```
  Event-Type = Session.Logon AND Device-ID NOTIN ("1621D2CB-F598-5EF7-A5BF-81747496ED2E")
  ```

Dieses Problem ist jetzt behoben und der benutzerdefinierte Risikoindikator wird unabhängig von der Groß- und Kleinschreibung der bedingten Werte ausgelöst.

[CAS-50153]

29. April 2021

Was ist neu

Ereignisdetails für einen benutzerdefinierten Risikoindikator Auf der Risikozeitleiste des Benutzers können Sie jetzt die Ereignisse anzeigen, die einen benutzerdefinierten Risikoindikator ausgelöst haben. Zuvor konnten Sie nur die definierten Bedingungen, die Beschreibung und die Triggerfrequenz für einen benutzerdefinierten Risikoindikator anzeigen. Klicken Sie auf **Ereignissuche**, um die Details der mit dem Benutzer verbundenen Ereignisse und den Risikoindikator anzuzeigen. Weitere Informationen finden Sie unter Benutzerdefinierte Risikoindikatoren.

Problem behoben

- Ein Administrator kann keine benutzerdefinierten Risikoindikatoren erstellen, selbst nachdem seine Zugriffsberechtigung vom schreibgeschützten Admin auf den vollständigen Administrator geändert wurde. [CAS-49628]

16. April 2021

Was ist neu

Verbesserungen bei SIEM-Nachrichten Sie können die folgenden Verbesserungen im Risikoindikator-Schemaformat anzeigen:

- Die Client-IP-Adresse ist jetzt im Schema für alle Chargenrisikoindikatoren verfügbar. Zuvor war die Client-IP-Adresse nur für einige Chargenrisikoindikatoren verfügbar:
  - EPA-Scanfehler
  - Übermäßige Authentifizierungsfehler
  - Anmeldung von verdächtiger IP
  - Zugang von einem ungewöhnlichen Ort

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

  - Ungewöhnlicher Authentifizierungsfehler
  - Anonymer Download von vertraulicher Freigabe
  - Potenzielle Datenexfiltration

- Wenn ein Feldwert für ganzzahlige Datentypen nicht verfügbar ist, ist der zugewiesene Wert **-999**. Beispiel: `"latitide"= -999`.
- Wenn ein Feldwert des Zeichenfolgendatentyps nicht verfügbar ist, ist der zugewiesene Wert **NA**. Beispiel: `"city"= "NA"`.

Weitere Informationen finden Sie unter Citrix Analytics-Datenformat für SIEM.

26. März 2021

Was ist neu

Einschränkung der SIEM-Nachrichten Citrix Analytics sendet maximal 1000 Ereignisdetails für jedes Auftreten von Risikoindikatoren an Ihren SIEM-Dienst. Diese Ereignisse werden in einer chronologischen Reihenfolge des Auftretens gesendet. Weitere Informationen finden Sie unter Citrix Analytics-Datenformat für SIEM.

Die Datenquellen-ID und die Indikator-Kategorie-ID-Felder in den SIEM-Nachrichten hinzugefügt Folgende Felder werden im Zusammenfassungsschema des Indikators und im Detailschema für Indikatorereignisse hinzugefügt.

Feld	Beschreibung
`data_source_id`	Die mit einer Datenquelle verknüpfte ID. ID 0 = Citrix Content Collaboration, ID 1 = NetScaler Gateway, ID 2 = Citrix Endpoint Management, ID 3 = Citrix Virtual Apps and Desktops, ID 4 = Citrix Access Control
`indicator_category_id`	Die ID, die mit einer Risikoindikatorkategorie verknüpft ist. ID 1 = Datenexfiltration, ID 2 = Insider-Bedrohungen, ID 3 = Kompromittierte Benutzer

Weitere Informationen finden Sie unter Citrix Analytics-Datenformat für SIEM.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

18. März 2021

Was ist neu

Zugriff auf das Dashboard für die Sicherung

> **Hinweis**
>
> Die Funktion befindet sich in der Vorschau.

Das **Access Assurance Location** Dashboard bietet einen Überblick über die Standorte, von denen aus sich die Citrix Virtual Apps and Desktops und Citrix DaaS-Benutzer für einen ausgewählten Zeitraum angemeldet haben. Citrix Analytics empfängt diese Benutzeranmeldeereignisse von der Citrix Workspace-App, die auf den Geräten der Benutzer installiert ist.

Um das Dashboard anzuzeigen, klicken Sie auf **Sicherheit > Zugriffsversicherung**.

Sie können die folgenden Informationen für einen ausgewählten Zeitraum anzeigen:

- Gesamtzahl der Benutzeranmeldungen von einem bestimmten Ort und über die Standorte hinweg.
- Gesamtzahl der eindeutigen Benutzeranmeldungen an den Standorten.
- Gesamtzahl der Länder, aus denen sich die Benutzer angemeldet haben.
- Top 10 Standorte mit eindeutigen Benutzeranmeldungen.

Weitere Informationen finden Sie unter Standort der Zugriffssicherung.

Unterstützung für NOT LIKE (!~)-Operator Für die Self-Service-Suchanfrage und die benutzerdefinierte Risikoindikatorbedingung können Sie jetzt das NOT LIKE (! ~) Betreiber. Der

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Operator sucht nach den Benutzerereignissen nach dem von Ihnen angegebenen übereinstimmenden Muster. Es gibt die Ereignisse zurück, die das angegebene Muster nirgendwo in der Ereigniszeichenfolge enthalten.

Die Abfrage `User-Name !~ "John"` zeigt beispielsweise Ereignisse für Benutzer mit Ausnahme von John, John Smith oder solchen Benutzern an, die den übereinstimmenden Namen "John"enthalten.

Weitere Informationen finden Sie unter Self-Service-Suche.

Übersetzte Betriebssystemversion Für die Citrix Virtual Apps and Desktops und Citrix DaaS-Datenquelle wird die **Platform-Dimension** jetzt in die Dimensionen **OS-Major-Version**, **OS-Minor-Version**und **OS-Extra-Details** übersetzt. Basierend auf den Betriebssystemdetails eines Benutzers zeigt Citrix Analytics diese Dimensionen auf der Self-Service-Suchseite an.

Sie können diese Dimensionen verwenden, um Ihre Bedingungen für einen benutzerdefinierten Risikoindikator zu definieren.

Wenn Sie für die zuvor erstellten benutzerdefinierten Risikoindikatoren die **Platform-Dimension** als Bedingung verwendet haben, ersetzt Citrix Analytics die **Platform-Dimension** automatisch durch die **OS-Major-Version**, **OS-Minor-Version**und **OS-Extra-Details**. Dieses Update hat keinen Einfluss auf die Integrität Ihrer definierten Bedingung.

Weitere Informationen zu den neuen Dimensionen finden Sie unter Self-Service-Suche nach Virtual Apps and Desktops.

Die Datenfelder für Apps und Desktops wurden aktualisiert Zeigen Sie in der Self-Service-Suche nach Apps und Desktops die aktualisierten Datenfelder basierend auf der kontextbezogenen Vorlage an.

Weitere Informationen finden Sie unter Self-Service-Suche nach Apps und Desktops.

Veraltete Funktion

Die Ereignisse VPN_AF und VPN_SU wurden von der Self-Service-Suchseite entfernt Auf der Self-Service-Suchseite für die NetScaler Gateway-Datenquelle werden die folgenden Datensatztypen jetzt entfernt.

Datensatztyp	Datensatzname
VPN_SU	Sitzungsaktualisierungsdatensatz
VPN_AF	Anwendungsstartfehlerdatensatz

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Sie können Ihre Ereignisse also nicht basierend auf diesen Datensatztypen filtern und anzeigen. Alle benutzerdefinierten Risikoindikatoren, die auf diesen Datensatztypen basieren, funktionieren nicht mehr.

Weitere Informationen finden Sie unter Self-Service-Suche für Gateway.

11. März 2021

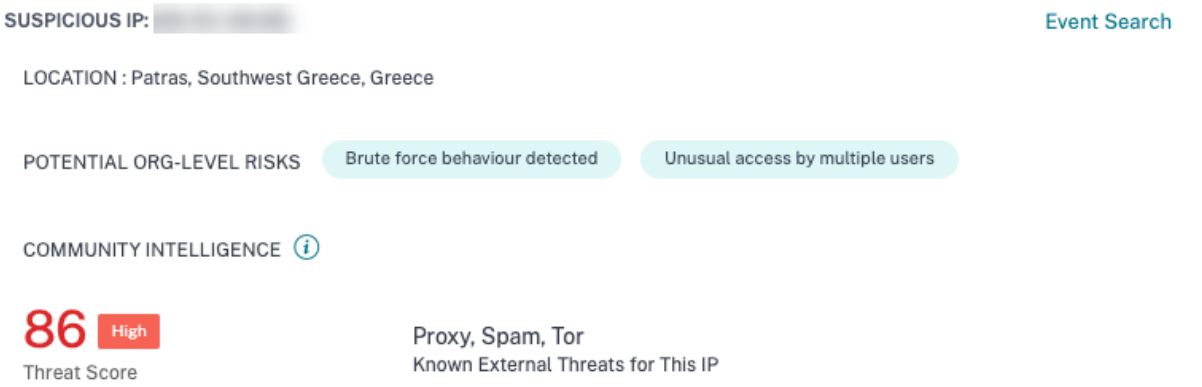
Was ist neu

Aktueller Zeitstempel für das Benutzerrisiko-Score-Schema Im Schemaformat für Benutzerrisiko-Score `last_update_timestamp` wird ein neues Feld hinzugefügt. Dieses Feld gibt den Zeitpunkt an, zu dem der Risikowert zuletzt aktualisiert wurde. Weitere Informationen zum Schemaformat finden Sie unter Benutzerrisiko-Score-Schema.

3. März 2021

Was ist neu

Verbesserungen des Risikoindikators "Anmeldung von verdächtigen IP" Auf der Risikozeitleiste des Benutzers wird ein neuer Abschnitt **Verdächtige IP** für den Risikoindikator "**Anmeldung von verdächtigen IP** "angezeigt. Dieser Abschnitt enthält die folgenden Informationen:



- Die IP-Adresse, von der verdächtige Anmeldeaktivitäten erkannt werden.
- Der Standort des Benutzers.
- Alle Muster verdächtiger IP-Aktivitäten, die Citrix Analytics kürzlich in Ihrer Organisation entdeckt hat.
- Intelligence-Feed auf Community-Ebene über die IP-Adresse.

Weitere Informationen finden Sie im Indikator "Anmelden von verdächtigen IP-Risiken".

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Verbesserungen bei Zugriff von einem ungewöhnlichen Standortrisikoindikator

- Im Indikator Zugriff von einem ungewöhnlichen Standortrisiko für Citrix Content Collaboration wurde die Spalte **TOOL NAME** in der Ereignistabelle hinzugefügt. Die Spalte **DEVICE BROWSER** wurde aus der Ereignistabelle entfernt. Weitere Informationen finden Sie unter Risikoindikatoren für Citrix Content Collaboration.
- Im Risikoindikator Zugriff von einem ungewöhnlichen Standort aus für Citrix Virtual Apps and Desktops und Citrix DaaS wurden die Spalten **DEVICE ID** und **RECEIVER TYPE** in der Ereignistabelle hinzugefügt. Weitere Informationen finden Sie unter Risikoindikatoren für Citrix Virtual Apps and Desktops.

Citrix Analytics-Datenformat für SIEM Der Artikel beschreibt das Schema der verarbeiteten Daten, die von Citrix Analytics für Ihren SIEM-Dienst generiert wurden.

Problem behoben

- Wenn der Wert `Is Employee<!--NeedCopy-->` für einen Content Collaboration-Benutzer NULL ist, wird der Benutzer nicht in der Liste der erkannten Benutzer angezeigt. [CAS-47815]

18. Februar 2021

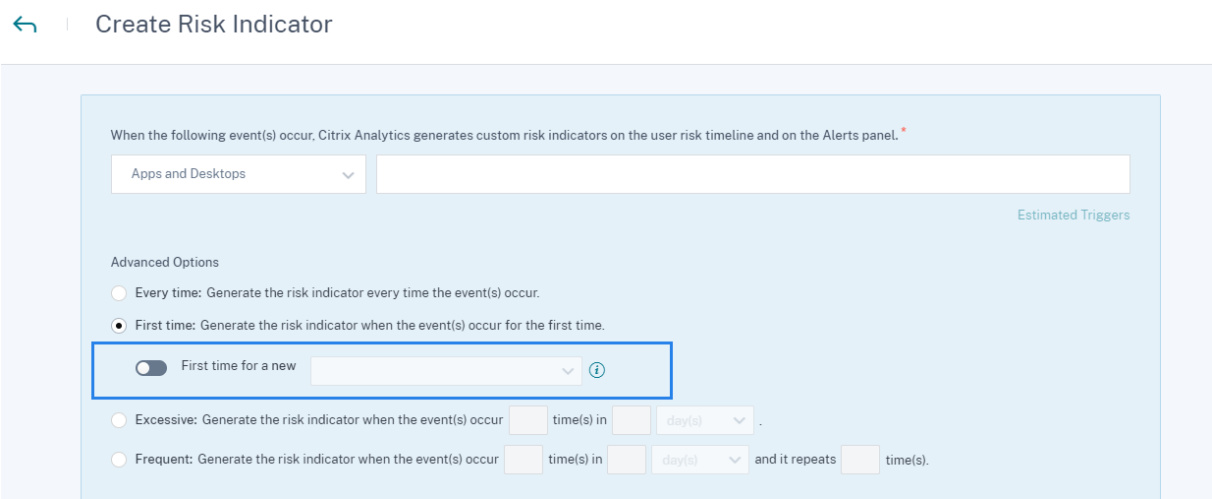
Was ist neu

Unterstützung für den ersten Zugriff von einer neuen Entität im benutzerdefinierten Risikoindikator Sie können jetzt einen Risikoindikator erstellen, der auslöst, wenn Citrix Analytics zum ersten Mal Ereignisse von einer neuen Entität empfängt. Einige Beispiele für Unternehmen sind Client IP, City und Country.

Klicken Sie auf der Seite **Indikator erstellen** auf die Option **Erstes Mal** . Aktivieren Sie das **erste Mal für eine neue** Schaltfläche und wählen Sie basierend auf der Datenquelle eine gültige Entität aus der Liste aus. Sie müssen der Entität keinen bestimmten Wert zuweisen. Wenn Sie beispielsweise **City** aus der Liste auswählen, löst Citrix Analytics einen Risikoindikator aus, wenn sich Benutzer zum ersten Mal von einer neuen Stadt aus anmelden.

Weitere Informationen finden Sie unter Erstellen eines benutzerdefinierten Risikoindikators.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



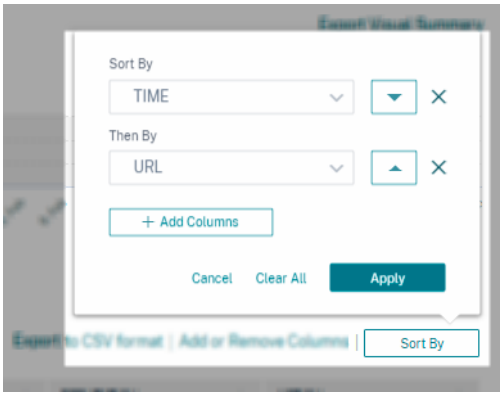
Maximalbegrenzung für die Erstellung eines benutzerdefinierten Risiko Sie können jetzt benutzerdefinierte Risikoindikatoren bis zu einer Höchstgrenze von 50 erstellen. Wenn Sie diese Höchstgrenze erreichen, müssen Sie alle vorhandenen benutzerdefinierten Risikoindikatoren löschen oder bearbeiten, um einen benutzerdefinierten Risikoindikator zu erstellen.

Weitere Informationen finden Sie unter Benutzerdefinierte Risikoindikatoren.

Standortdaten von Citrix Virtual Apps and Desktops und Citrix DaaS Auf der Seite **Benutzerinformationen** zeigt Citrix Analytics jetzt den Standort des Benutzers aus den Citrix Virtual Apps and Desktops und der Citrix DaaS-Datenquelle an.

Weitere Informationen zum Benutzerstandort finden Sie unter Benutzerprofil.

Mehrspaltige Sortierung Auf der Self-Service-Suchseite können Sie die Benutzerereignisse jetzt nach mehr als einer Spalte sortieren. Klicken Sie auf **Sortieren nach**, fügen Sie die Spalten und die Sortierreihenfolge hinzu. Klicken Sie auf **Übernehmen**, um die Benutzerereignisse zu Sie können bis zu sechs Spalten hinzufügen, um eine mehrspaltige Sortierung durchzuführen.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Weitere Informationen finden Sie unter Self-Service-Suche.

Veraltete Features

Risikoindikator für übermäßigen Autorisierungsausfall veraltet Der NetScaler Gateway-Risikoindikator - **Übermäßiger Autorisierungsfehler** wurde veraltet. Sie können nur historische Daten zu diesem Indikator anzeigen.

Die folgenden Änderungen gelten als Teil dieser Abwertung:

- Citrix Analytics generiert diese Risikoindikatoren nicht mehr.
- Citrix Analytics generiert keine Richtlinien mehr mit diesen Risikoindikatoren als Bedingungen.
- Standardrichtlinien mit diesen Risikoindikatoren, da die Bedingungen nicht mehr wirksam werden.

Weitere Informationen finden Sie unter NetScaler Gateway-Risikoindikatoren.

27. Januar 2021

Was ist neu

Verbesserungen des Zugriffs von einem ungewöhnlichen Standortrisikoindikator Für Citrix Content Collaboration, NetScaler Gateway und Citrix Virtual Apps and Desktops wird der **Zugriff von einem ungewöhnlichen Standortrisikoindikator** jetzt ausgelöst, wenn sich der Benutzer von einer IP-Adresse aus anmeldet, die einem neuen Land oder einer neuen Stadt zugeordnet ist, die ungewöhnlich weit von einer vorherigen Anmeldung entfernt ist Standort. Weitere Faktoren sind das allgemeine Mobilitätsniveau des Benutzers und die relative Häufigkeit von Anmeldungen aus der Stadt für alle Benutzer in Ihrem Unternehmen. In allen Fällen basiert der Standortverlauf des Benutzers auf den letzten 30 Tagen der Anmeldeaktivität.

Weitere Informationen zum Risikoindikator finden Sie in den folgenden Artikeln:

- Citrix Content Collaboration-Risikoindikatoren
- NetScaler Gateway-Risikoindikatoren
- Citrix Virtual Apps and Desktops und Citrix DaaS-Risikoindikatoren

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

20. Januar 2021

Problem behoben

- Für die Apps- und Desktops-Datenquelle mit lokalem StoreFront schlägt die Datenverarbeitung fehl, obwohl die StoreFront-Bereitstellung erfolgreich verbunden wurde.

  [CAS-46656]

19. Januar 2021

Problem behoben

- Auf der Seite mit dem benutzerdefinierten Risikoindikator reagiert der Link **Estimate Trigger** nicht, nachdem eine ungültige Bedingung im Suchfeld korrigiert wurde.

  Beispielsweise geben Sie eine ungültige Bedingung ein *Client-IP = 10.10.10.10*. Nachdem Sie diese Bedingung korrigiert und als *Client-IP = ‘‘10.10.10.10’’*eingegeben haben, antwortet der Link **Estimate Trigger** nicht.

  Problemumgehung: Aktualisieren Sie die Seite mit den benutzerdefinierten Indikatoren und erstellen Sie dann den benutzerdefinierten Indikator mit einer gültigen Bedingung.

  [CAS-46316]

13. Januar 2021

Was ist neu

Neue Version des Citrix Analytics Add-ons für Splunk ist verfügbar Citrix Analytics Add-on Version 2.1.0 für Splunk ist jetzt verfügbar. Gehen Sie zur Download-Seite, um die Datei herunterzuladen.

Unterstützung für Splunk Cloud Inputs Data Manager (IDM) und Splunk 8.1 64-Bit hinzugefügt Sie können jetzt Citrix Analytics for Security in Splunk Cloud IDM und Splunk 8.1 64-Bit integrieren. Weitere Informationen finden Sie unter Splunk-Integration.

Unterstützung läuft aus

Unterstützung für Splunk 7.1 64-Bit entfernt Sie können Citrix Analytics for Security nicht mehr in Splunk 7.1 64-Bit integrieren. Informationen zu unterstützten Splunk-Versionen finden Sie unter Splunk-Integration.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

11. Januar 2021

Problem behoben

- Auf der Sitekarte für Virtual Apps and Desktops wird die Bezeichnung **Unterstützte Clientbenutzer** in **Empfangene Ereignisse von Benutzern**umbenannt. Die Bezeichnung **Nicht unterstützte Clientbenutzer** wird in **Ereignisse von Benutzern nicht empfangen**umbenannt.

  [CAS-44773]

17. Dezember 2020

Was ist neu

Verwenden Sie vorkonfigurierte benutzerdefinierte Risikoindikatoren und eine Richtlinie, um den Zugriff von ungewöhnlichen Standorten aus zu blockieren (Geofencing) Citrix bietet eine Liste vorkonfigurierter benutzerdefinierter Risikoindikatoren und eine Richtlinie, mit denen Sie die Sicherheit Ihrer Citrix Infrastruktur überwachen können. Mit diesen Indikatoren und einer Richtlinie können Sie den Benutzerzugriff aus Ländern blockieren, die sich außerhalb ihres üblichen Betriebslandes befinden. Standardmäßig ist das Land auf "USA"eingestellt. Sie können Ihr erforderliches Land für Geofencing festlegen.

Im Folgenden sind die vorkonfigurierten benutzerdefinierten Risikoindikatoren und eine Richtlinie aufgeführt:

- CVAD-Sitzung begann außerhalb von Geofence
- GW-Geofence-Überfahrt
- CCC-Geofence-Überqueren
- Sitzungsstart außerhalb von Geofence

Weitere Informationen finden Sie unter Vorkonfigurierte benutzerdefinierte Risikoindikatoren und -richtlinien.

Anzeigen von aufgerufenen Standorten in der E-Mail zur Benutzer Anstelle der IP-Adresse eines Benutzergeräts zeigt die E-Mail mit der Benutzerantwort nun alle Standorte an, auf die der Benutzer in den letzten 15 Minuten zugegriffen hat. Der Ort wird im Format `<City>,<Country><!--NeedCopy-->` angezeigt. Wenn die Stadt oder das Land nicht verfügbar ist, wird der entsprechende Wert als "Unbekannt"angezeigt.

Weitere Informationen finden Sie unter Benutzerantwort anfordern.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Umbenannter Risikoindikator für Content Collaboration - Erstmaler Zugriff Der Citrix Content Collaboration Risikoindikator Der **erste Zugriff von einem neuen Standort** aus wird **von einem ungewöhnlichen Ort aus in Access**umbenannt.

Weitere Informationen finden Sie unter Zugriff von einem ungewöhnlichen Ortaus.

Veraltete Features

Risikoindikator-Feedback Der Rückkopplungsmechanismus für Risikoindikatoren wird entfernt. Wenn der Risikoindikator für Content Collaboration - Zugriff von einem ungewöhnlichen Ort aus falsch ausgelöst wird, können Sie ihn nicht mehr als falsch positiv melden und Feedback geben.

7. Dezember 2020

Was ist neu

Verbesserungen des Risikoindikators für potenzielle Datenexfiltration Die folgenden Verbesserungen wurden am Risikoindikator vorgenommen:

- Die Informationen im Abschnitt **WHAT HAPPENED**, werden aktualisiert. Das Zeitformat wird aktualisiert, um die Konsistenz zu gewährleisten.
- Die Standortinformationen des Geräts werden in der Ereignisliste angezeigt.

Weitere Informationen zum Risikoindikator finden Sie unter Mögliche Datenexfiltration.

Verbesserungen des Risikoindikators für Content Collaboration - Erstmaler Zugriff von einem neuen Standort Wählen Sie auf der Zeitleiste des Benutzerrisikos **Erstzugriff von einem neuen Standort aus**, um die folgenden Informationen anzuzeigen:

- **Anmeldeorte**: Zeigt eine geografische Kartenansicht der üblichen und ungewöhnlichen Orte an, von denen aus sich der Benutzer angemeldet hat.
- **Anzahl der Anmeldungen von üblichen Standorten - letzte 30 Tage**: Zeigt eine Tortendiagramm-Ansicht der 6 üblichen Orte an, von denen aus sich der Benutzer in den letzten 30 Tagen angemeldet hat. Es zeigt auch die Anzahl der Anmeldeereignisse an diesen Orten an.
- **Ereignisdetails für ungewöhnlichen Ort**: Stellt die Liste der Anmeldeereignisse vom ungewöhnlichen Ort für den Benutzer bereit.

Weitere Informationen zum Risikoindikator finden Sie unter Erster Zugriff von einem neuen Standort aus.

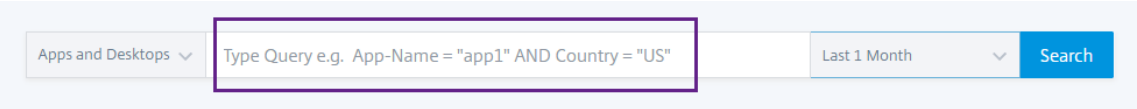
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

30. November 2020

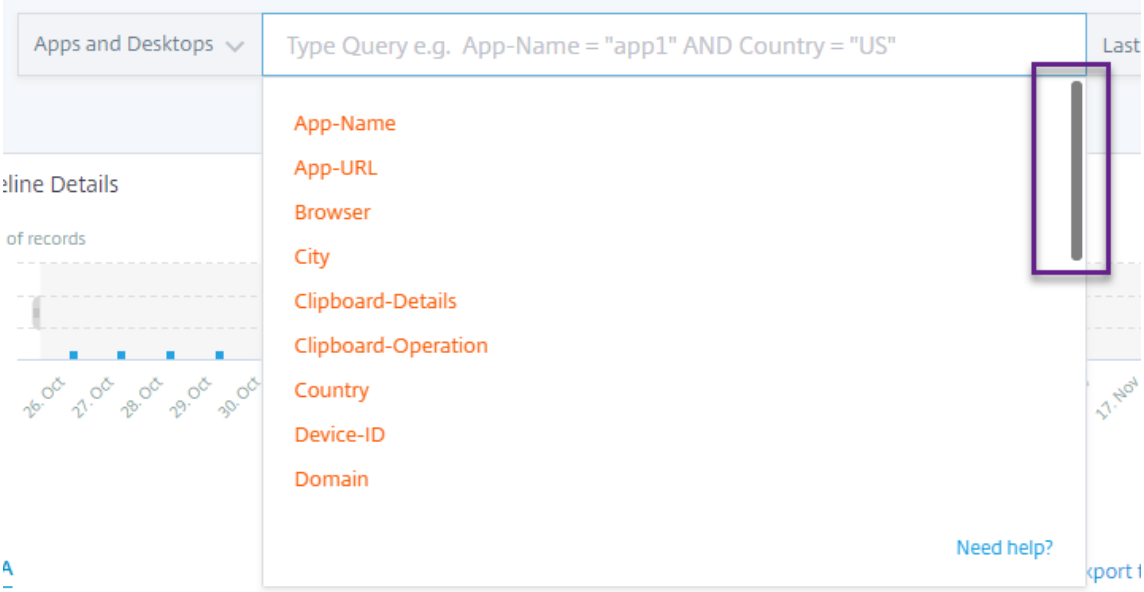
Was ist neu

Verbesserungen der Self-Service-Suchseite Folgende Verbesserungen wurden vorgenommen, um die Benutzerfreundlichkeit der Self-Service-Suchseite zu verbessern:

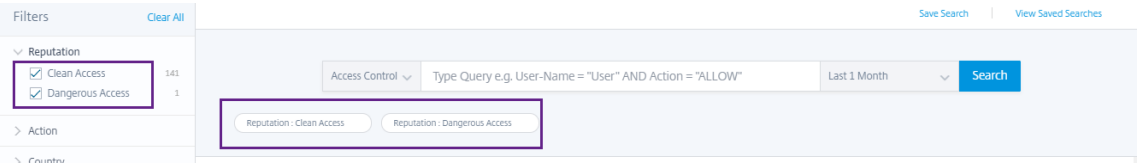
- Das Suchfeld zeigt ein Beispiel für eine Abfrage an, um anzugeben, wie Ihre eigene Abfrage eingegeben werden soll.



- In macOS wird jetzt standardmäßig die Bildlaufleiste in der Dimensionsliste angezeigt.

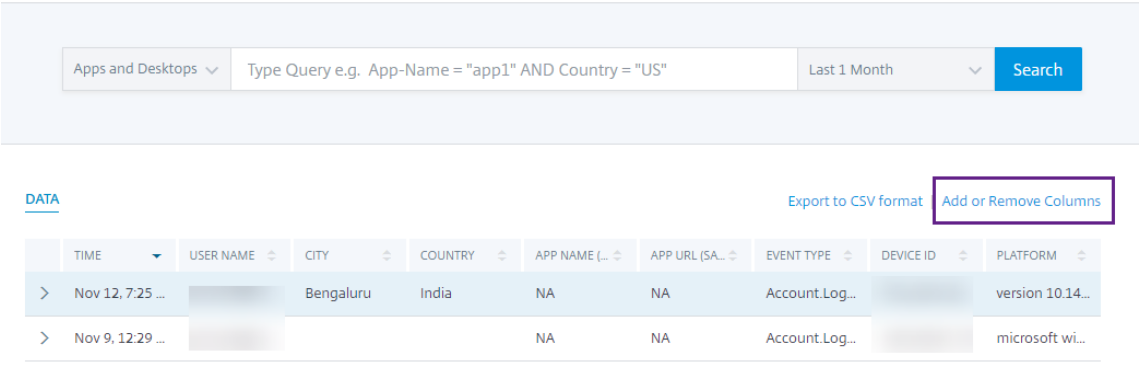


- Die angewendeten Filter erscheinen jetzt als Chips.



- Das Label **Spalten hinzufügen oder entfernen** ersetzt das **+-Symbol** .

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Weitere Informationen finden Sie unter Self-Service-Suche.

Politische Verbesserungen Auf der Seite **Richtlinien** werden jetzt die Richtlinien angezeigt, die mit den Datenquellen verknüpft sind, die erfolgreich erkannt und mit Citrix Analytics verbunden wurden. Auf dieser Seite werden die Richtlinien nicht angezeigt, für die eine Bedingung für die unentdeckten Datenquellen definiert ist. Das Deaktivieren der Datenverarbeitung für eine bereits verbundene Datenquelle hat keine Auswirkungen auf die vorhandenen Richtlinien auf der Seite **Richtlinien** .

Weitere Informationen finden Sie unter Konfigurieren von Richtlinien und Aktionen.

04. November 2020

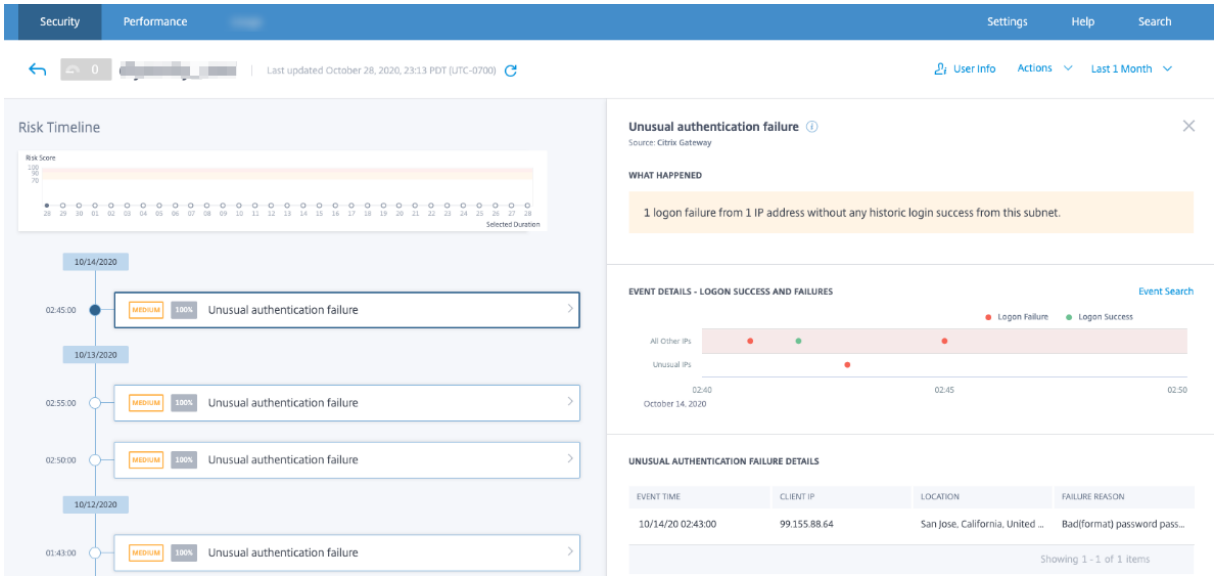
Was ist neu

Ungewöhnlicher Authentifizierungsfehler - NetScaler Gateway-Risiko Citrix Analytics erkennt zugriffsbasierte Bedrohungen, wenn ein Benutzer Anmeldefehler aufgrund einer ungewöhnlichen IP-Adresse hat, und löst den Risikoindikator für **ungewöhnliche Authentifizierungsfehler** aus.

Dieser Risikoindikator wird ausgelöst, wenn ein Benutzer in Ihrer Organisation Anmeldefehler aufgrund einer ungewöhnlichen IP-Adresse hat, die seinem üblichen Verhalten widersprechen.

Weitere Informationen finden Sie unter NetScaler Gateway-Risikoindikatoren.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



20. Oktober 2020

Problem behoben

- Der Risikoindikator Der **erstmalige Zugriff von einem neuen Gerät** mit angewendeter **Benutzeraktion abmelden** funktioniert nicht wie erwartet.

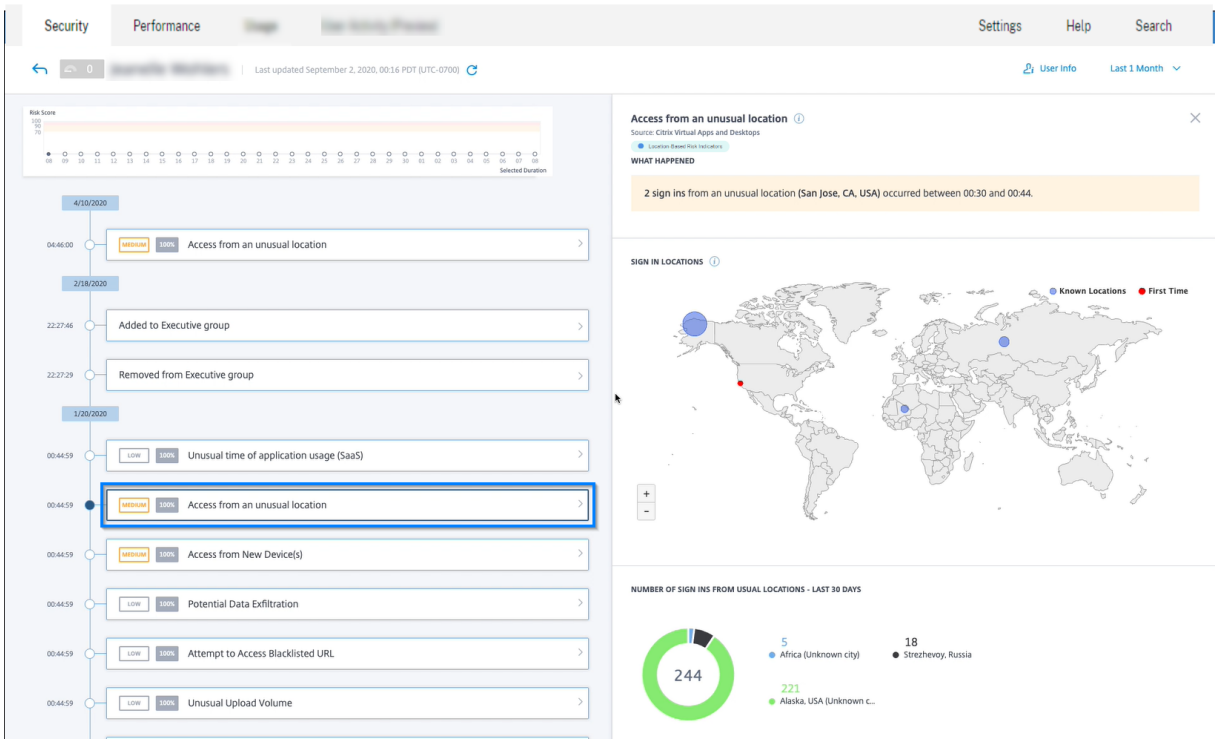
  [CAS-40743]

15. Oktober 2020

Neue Features

Zugriff von einem ungewöhnlichen Ort aus —Citrix Virtual Apps and Desktops und Citrix DaaS-Risikoindikator Citrix Analytics erkennt zugriffsbasierte Bedrohungen basierend auf ungewöhnlichen Anmeldungen von Citrix Workspace und löst den entsprechenden Risikoindikator aus.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Weitere Informationen finden Sie unter Citrix Virtual Apps and Desktops und Citrix DaaS-Risikoindikatoren.

Verbesserungen des Freigabe-Link-Dashboards

- Die Spalte SHARE URL wird jetzt durch die Spalte SHARE ID ersetzt. Jede Freigabe-URL wird jetzt mit einer Freigabe-ID identifiziert.
- Die Zeitauswahl auf dem Dashboard wird entfernt. Jetzt zeigt dieses Dashboard alle Freigabelinks vom aktiven Status bis zum abgelaufenen Status anstelle eines ausgewählten Zeitraums an.
- Alle Freigabelinks werden zuerst in der Reihenfolge der aktiven Links und dann der abgelaufenen Links sortiert. Standardmäßig wird der Freigabelink mit der höchsten Anzahl von Risikoindikatoren ganz oben auf der Liste angezeigt.
- Die riskanten Links zeigen jetzt die aktiven Links an, die ein riskantes Verhalten aufweisen. Die abgelaufenen Links werden nicht angezeigt. Standardmäßig wird der riskante Link mit der höchsten Anzahl von Risikoindikatoren ganz oben auf der Liste angezeigt.
- Die Trendansicht auf der Risky Share Links-Karte und der All Share Links-Karte wird entfernt.

Weitere Informationen finden Sie unter Dashboard für Freigabelinks.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Verbesserungen der Timeline für das Share-Link-Risiko In der Risikozeitleiste wird nun anstelle der Freigabe-URL die Freigabe-ID angezeigt. Weitere Informationen finden Sie unter Zeitplan für das Risiko von Freigabelinken.

Veraltete Features

Zugriff vom Gerät mit nicht unterstütztem Betriebssystem (OS) -Risikoindikator ist veraltet Der Risikoindikator für Citrix Virtual Apps and Desktops - **Zugriff von einem Gerät mit nicht unterstütztem Betriebssystem (OS)** wurde eingestellt. Sie können nur historische Daten zu diesem Indikator anzeigen.

Die folgenden Änderungen gelten als Teil dieser Abwertung:

- Analytics generiert diese Risikoindikatoren nicht mehr.
- Analytics generiert keine Richtlinien mehr mit diesen Risikoindikatoren als Bedingungen.
- Standardrichtlinien mit diesen Risikoindikatoren, da die Bedingungen nicht mehr wirksam werden.

Weitere Informationen finden Sie unter Citrix Virtual Apps and Desktops und Citrix DaaS-Risikoindikatoren.

10. September 2020

Neue Features

Checkliste für StoreFront Citrix Analytics zeigt jetzt eine Liste der Voraussetzungen an, die Sie erfüllen müssen, bevor Sie die StoreFront-Konfigurationsdatei herunterladen. Überprüfen Sie die Checkliste und stellen Sie sicher, dass alle Mindestanforderungen ausgewählt sind. Wenn die Mindestanforderungen nicht ausgewählt sind, können Sie die Konfigurationsdatei nicht herunterladen. Weitere Informationen finden Sie unter Citrix Virtual Apps and Desktops Datenquelle.

Self-Service-Suche - Unterstützung für NOT EQUAL (! =) Betreiber Du kannst jetzt das NOT EQUAL (! =) Operator in Ihrer Abfrage in den folgenden Funktionen:

- Benutzerdefinierte Risikoindikator
- Self-Service-Suche

Sie können diesen Operator für die folgenden Bedingungen verwenden:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Datenquelle	Dimensionen
Content Collaboration	Land, Stadt, Clientbetriebssystem
Zugriffssteuerung	Land, Stadt, Aktion, URL, URL Kategorie, Reputation, Browser, Betriebssystem, Gerät
Apps und Desktops	Land, Stadt, App-Name, Betrieb der Zwischenablage, Browser, Betriebssystem
Gateway	Phase der Authentifizierung, Client-IP

Erstellen Sie mit dem Operator einen benutzerdefinierten Indikatorausdruck mit einem einzigen Wert wie "Country! = XYZ"und sehen Sie sich die Benutzerliste an. Erstellen Sie dann eine Richtlinie, um Aktionen wie Zur Watchlist hinzufügen, Admin benachrichtigen oder Benutzer deaktivieren anzuwenden.
Sie können den Operator auch bei der Self-Service-Suche der angegebenen Datenquellen verwenden, um die Benutzerereignisse zu filtern.

Verwenden Sie bei der Eingabe der Werte für die Dimensionen in Ihrer Abfrage die genauen Werte, die auf der Self-Service-Suchseite für eine Datenquelle angezeigt werden. Bei den Dimensionswerten wird die Groß-/Kleinschreibung

08. September 2020

Neue Features

Benutzer-Korrelation Analytics korreliert jetzt die Benutzer, die aus verschiedenen Datenquellen entdeckt wurden. Dieser Mechanismus eliminiert die meisten doppelten Benutzer aus der Liste der erkannten Benutzer. Die entdeckten Benutzer in Analytics zeigen jetzt die Liste der eindeutigen Benutzer zusammen mit ihren Datenquellen und den Risikoindikatoren an.

Beispielsweise kann der Benutzer "Joe Smith"mehrere Benutzerkennungen haben —JosephSm joe.smith@citrix.com und joe.smith, basierend auf den Datenquellen. Analytics identifiziert diesen Benutzer jetzt mit einem eindeutigen Kennungsnamen. Alle anderen Benutzerkennungen sind korreliert und Ereignisse, die für Joe Smith aus verschiedenen Datenquellen empfangen wurden, sind mit diesem eindeutigen Namen verknüpft.
Weitere Informationen finden Sie unter Entdeckte Benutzer

Problem behoben

In der Liste **Aktionen** wird eine Fehlermeldung angezeigt, nachdem Sie die Aktionsoptionen ausgewählt und auf **Übernehmen**geklickt haben.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

[CAS-39914]

11. August 2020

Behobene Probleme

- Sie können Microsoft Graph Security nicht in Citrix Analytics integrieren. Dieses Problem trat auf, weil das Microsoft-Portal nicht zu Citrix Analytics umgeleitet werden konnte.

[CAS-38021]

31. Juli 2020

Behobene Probleme

- Die Option **Geschätzte Auslöser** im benutzerdefinierten Risikoindikator prognostiziert die benutzerdefinierten Risikoindikatorinstanzen für den letzten Tag nicht.

[CAS-38129]

09. Juli 2020

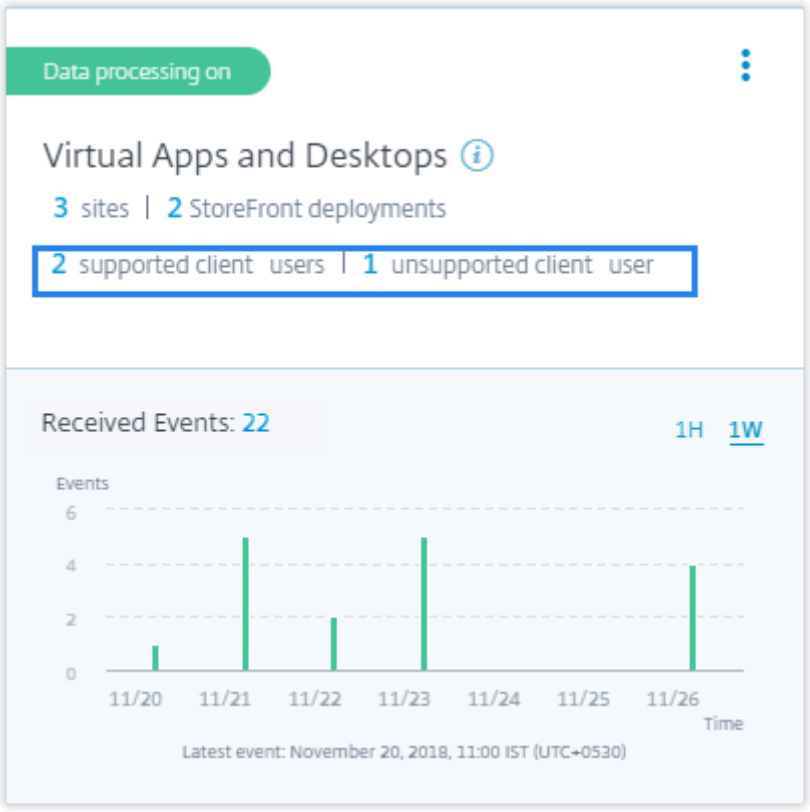
Neue Features

Die Sitekarte für Virtual Apps and Desktops zeigt Benutzer mit unterstützten und nicht unterstützten Clients an Auf der Sitekarte können Sie jetzt die Anzahl der Benutzer anzeigen, die unterstützte und nicht unterstützte Versionen der Citrix Workspace-App oder Citrix Receiver-Clients auf ihren Endpunkten verwenden.

- Klicken Sie auf die Benutzeranzahl für die unterstützten Clients, um die Seite **Benutzer** anzuzeigen, auf der alle erkannten Benutzer angezeigt werden.
- Klicken Sie auf die Benutzeranzahl, damit die nicht unterstützten Clients eine CSV-Datei herunterladen können. Die Datei listet die Benutzer und ihre nicht unterstützten Clientversionen auf. Analytics erhält keine Benutzerereignisse von den nicht unterstützten Clients und fügt daher die Benutzer nicht als erkannte Benutzer hinzu. Mithilfe der CSV-Datei identifizieren Sie die Benutzer, die ihre Clients auf eine unterstützte Version aktualisieren müssen, damit Analytics Sicherheitseinblicke in ihr Verhalten geben kann.

Informationen zum Anzeigen der Liste der unterstützten Clients finden Sie unter Citrix Virtual Apps and Desktops und Citrix DaaS-Datenquelle.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Zugriff von einem ungewöhnlichen Standortrisikoindik

- Der NetScaler Gateway-Risikoindikator Der **erste Zugriff von einem neuen Standort** aus wird **von einem ungewöhnlichen Ort aus in Access**umbenannt.
- Auf der Zeitleiste des Benutzerrisikos werden im Abschnitt "Ereignisdetails"eine geografische Karte und ein Kreisdiagramm eingeführt.
  - **Anmeldestandorte:** **In**diesem Abschnitt wird eine geografische Kartenansicht der üblichen und ungewöhnlichen Standorte des Benutzers angezeigt. Die üblichen und ungewöhnlichen Orte werden durch einen Farbcode oben rechts auf der Geokarte angezeigt. Sie können die Geokarte zoomen, um den Standort genauer zu betrachten.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

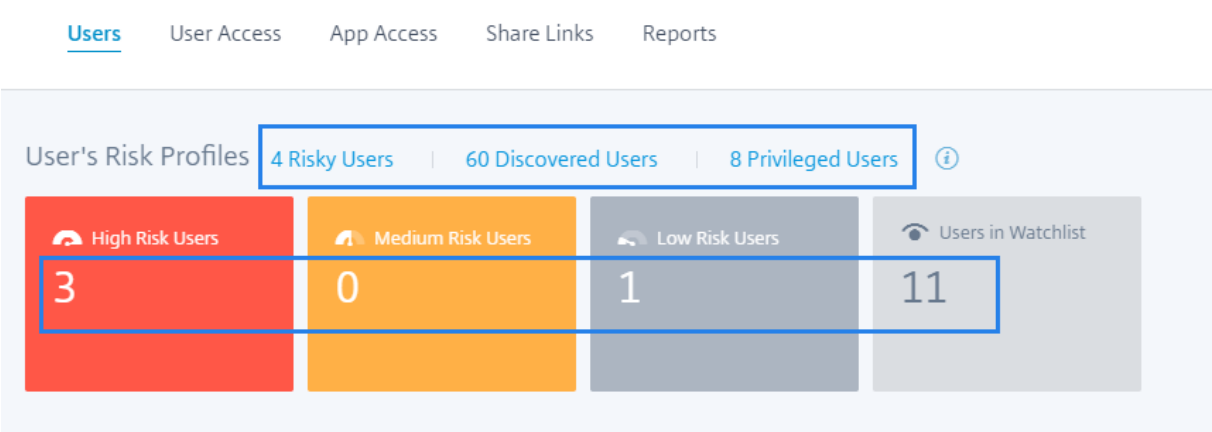
- **Übliche Standorte - letzte 30 Tage**: In diesem Abschnitt wird ein Tortendiagramm angezeigt, das einen Überblick über die 6 üblichen Standorte gibt, von denen aus sich der Benutzer angemeldet hat. Jeder Standort ist mit einem anderen Farbcode gekennzeichnet. Sie können den Abschnitt nach dem Ort sortieren, um eine detaillierte Ansicht des ausgewählten Standorts zu erhalten.

Weitere Informationen finden Sie unter Zugriff von einem ungewöhnlichen Ortaus.

Benutzer-Dashboard-Daten Die Anzahl der riskanten Benutzer, entdeckten Benutzer, privilegierten Benutzer und Benutzer in der Watchlist wird für die letzten 13 Monate angezeigt, unabhängig vom im **Benutzer-Dashboard** und auf der Seite **Benutzer** ausgewählten Zeitraum. Wenn Sie den Zeitraum auswählen, ändern sich die Vorkommnisse des Risikoindikators.

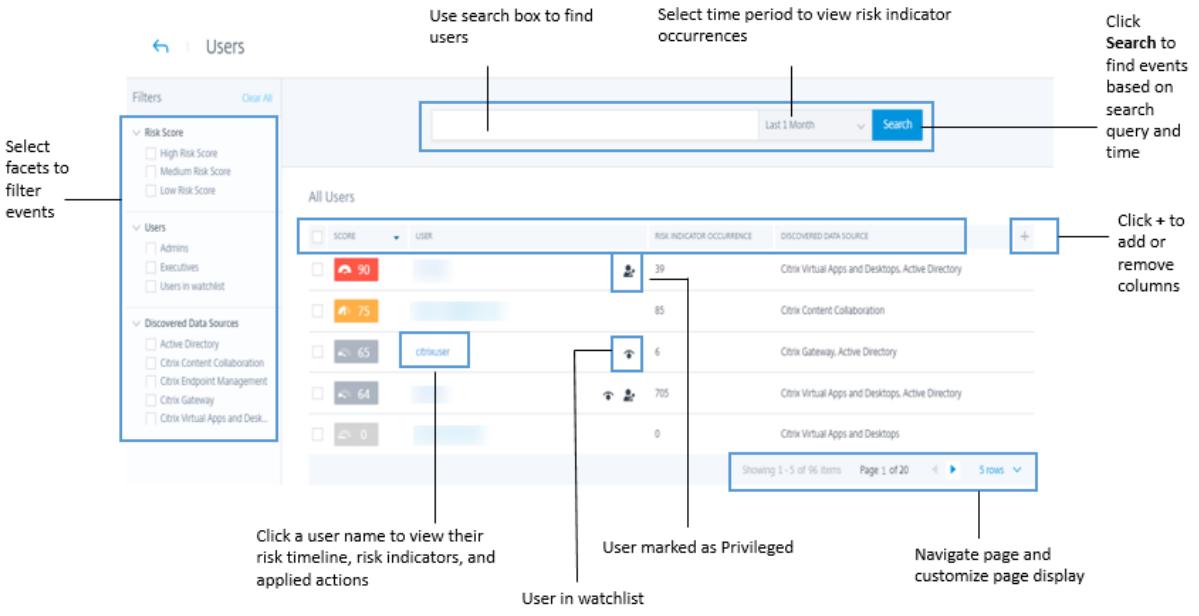
Weitere Informationen finden Sie unter Benutzer-Dashboard.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Benutzerseite neu gestaltet Die Seite **Benutzer** wurde für eine bessere Benutzererfahrung erweitert. Es bietet eine konsolidierte Zusammenfassung der Benutzerereignisse basierend auf den Benutzerrisikobewertungen, der Datenquelle und dem Benutzertyp.

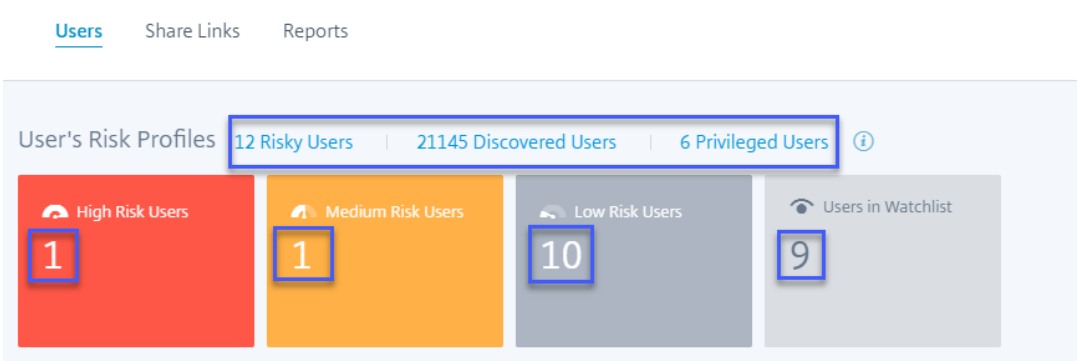
Um eine fokussiertere Suche zu unterstützen, enthält die Seite **Benutzer** den Abschnitt **Filter** im linken Bereich und die Suchleiste oben. Sie können nach Benutzerereignissen für eine voreingestellte Zeit oder einen benutzerdefinierten Zeitraum suchen.



So zeigen Sie die Seite "**Benutzer** "an:

- Gehen Sie zu **Sicherheit > Benutzer**, um das **Benutzer-Dashboard** anzuzeigen, und gehen Sie wie folgt vor:
  - Klicken Sie auf einen der folgenden Links oder die Karten.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



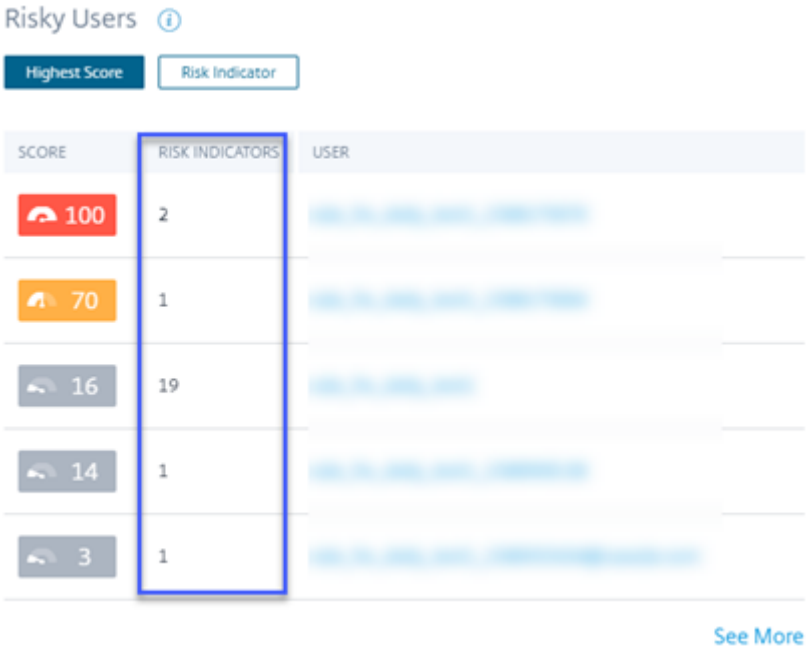
  - Klicken Sie im Bereich **Riskante Benutzer** auf **Mehr anzeigen**.
  - Klicken Sie im Bereich **Benutzer in Watchlist** auf **Mehr anzeigen**.
  - Klicken Sie im Bereich **Privilegierte Benutzer** auf **Mehr anzeigen**.

- Gehen Sie zu **Einstellungen > Datenquellen > Sicherheit**. Klicken Sie auf die Anzahl der Benutzer auf einer Datenquell-Site-Karte.

Weitere Informationen finden Sie unter Benutzer-Dashboard.

Verbesserungen des Bereichs "Riskante Benutzer" Die Spalte **Änderung** wird durch die Spalte **Risikoindikatoren** ersetzt. In der Spalte **Risikoindikatoren** werden die Gesamtrisikoindikatorvorkommen eines Benutzers für einen bestimmten Zeitraum angezeigt.

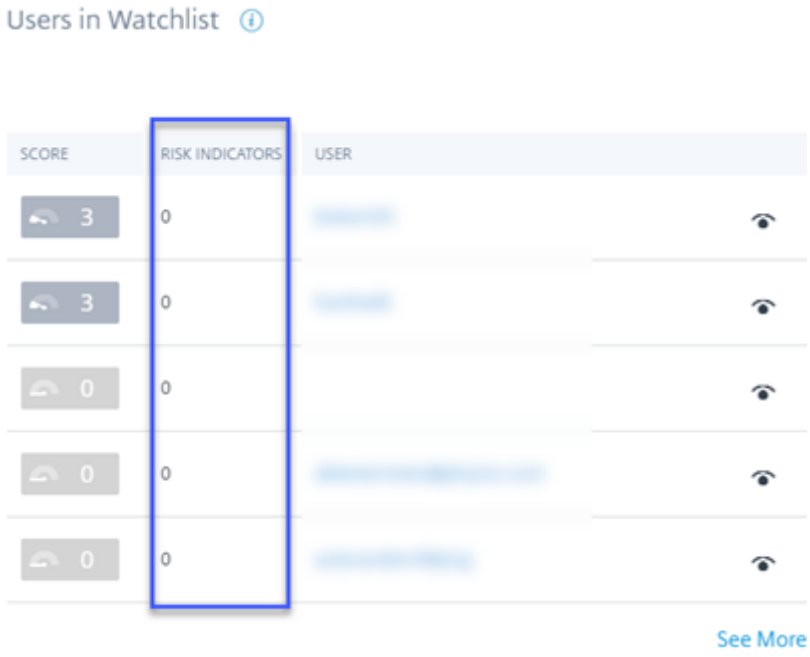
Weitere Informationen finden Sie unter Riskante Benutzer.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Verbesserungen des Bereichs Benutzer im Watchlist-Bereich Die Spalte **Änderung** wird durch die Spalte **Risikoindikatoren** ersetzt. In der Spalte **Risikoindikatoren** werden die Gesamtrisikoindikatorvorkommen eines Benutzers für einen bestimmten Zeitraum angezeigt.

Weitere Informationen finden Sie unter Benutzer in der Watchlist.

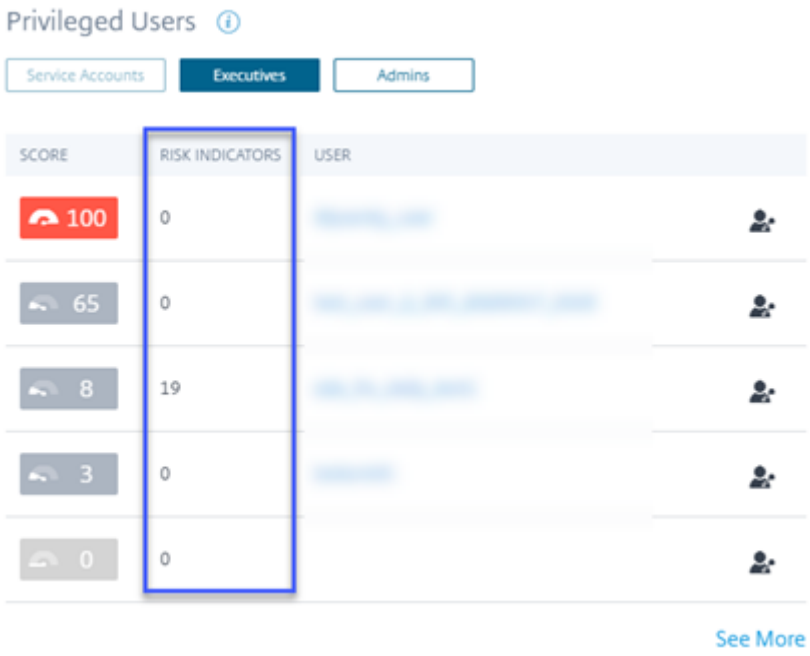


Erweiterungen des Bereichs Privilegierte Benutzer

- Die Spalte **Änderung** wird durch die Spalte **Risikoindikatoren** ersetzt. In der Spalte **Risikoindikatoren** werden die Gesamtrisikoindikatorvorkommen eines Benutzers für einen bestimmten Zeitraum angezeigt.
- Klicken Sie auf **Mehr** anzeigen, um die Seite "**Benutzer** "anzuzeigen. Die Seite **Benutzer**, auf der die Liste der privilegierten Admin- und Executive-Benutzer angezeigt wird. Auf dieser Seite können Sie einen Benutzer als privilegierten Benutzer hinzufügen oder entfernen.

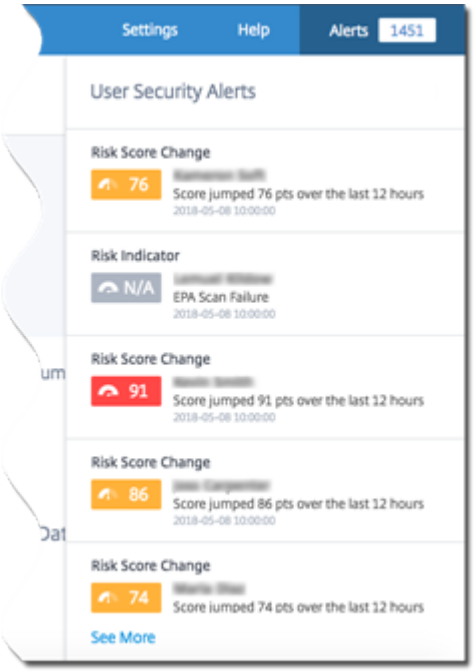
Weitere Informationen finden Sie unter Privilegierte Benutzer.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



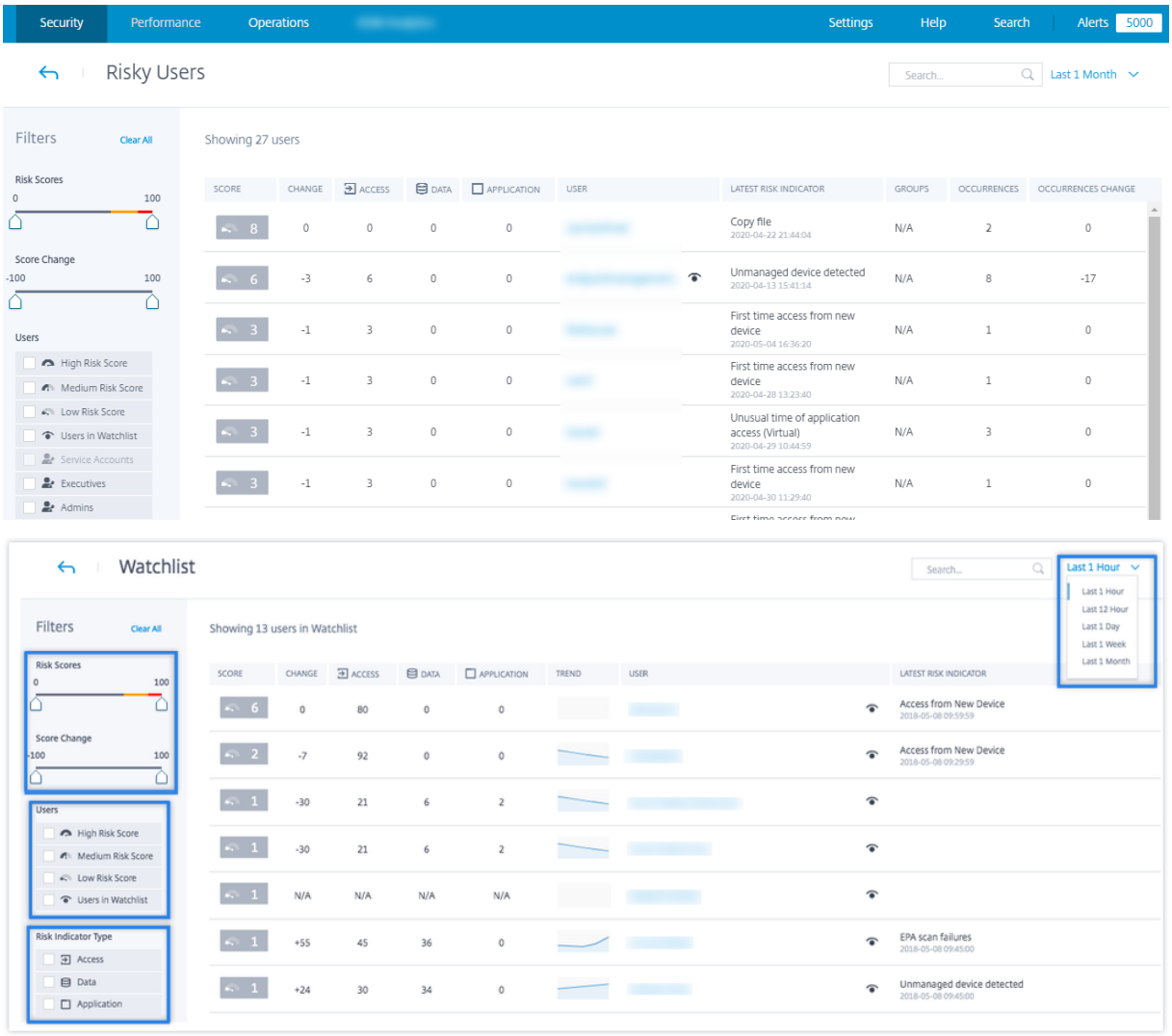
Veraltete Features

Warnungen Die Funktion "**Warnungen** "ist jetzt veraltet und auf der Analytics-Benutzeroberfläche nicht mehr verfügbar.



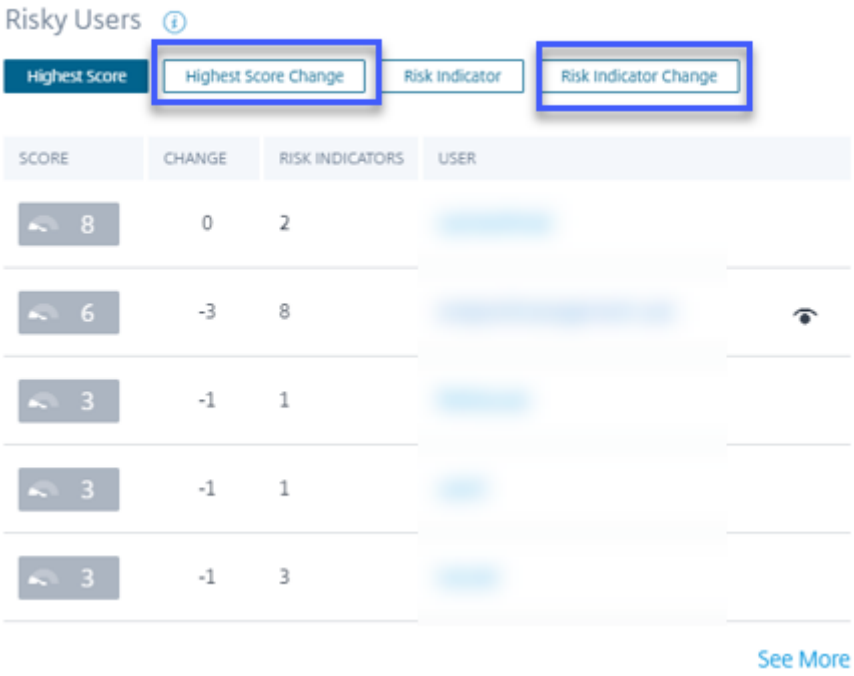
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Riskante Benutzer und Watchlist-Seite Die Seiten **Risky Users** und **Watchlist** sind veraltet. Sie werden durch die Seite **Benutzer** ersetzt, auf der alle riskanten Benutzerereignisse und die Benutzer in der Watchlist zusammengefasst sind.



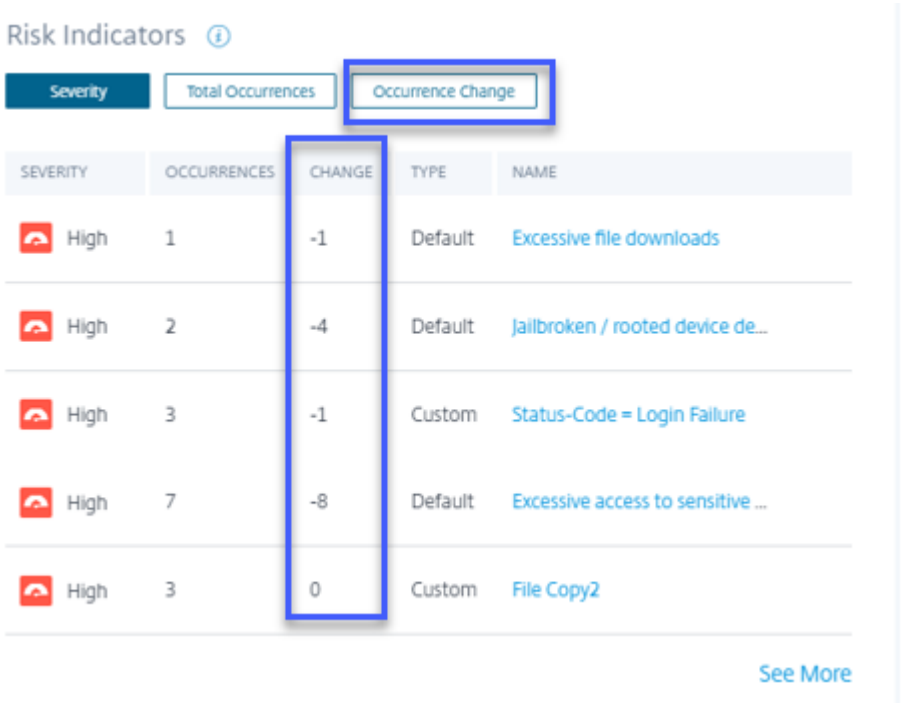
Bereich "Riskante Benutzer" Die Registerkarten **Änderung der höchsten Bewertung** und **Änderung des Risikoindikators** werden aus dem Bereich **Riskante Benutzer** entfernt.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Bereich Risikoindikator

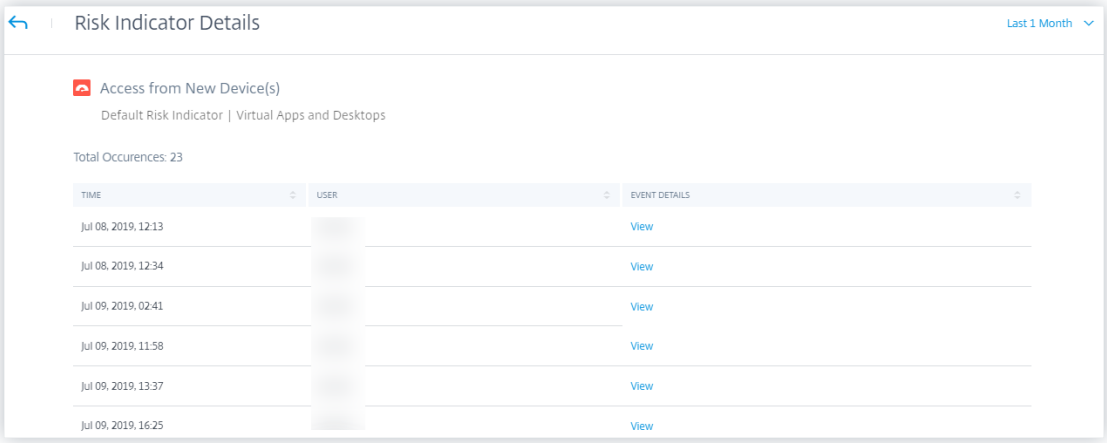
- Die Registerkarte "**Vorkommensänderung** "und die Spalte **ÄNDERN** werden entfernt.



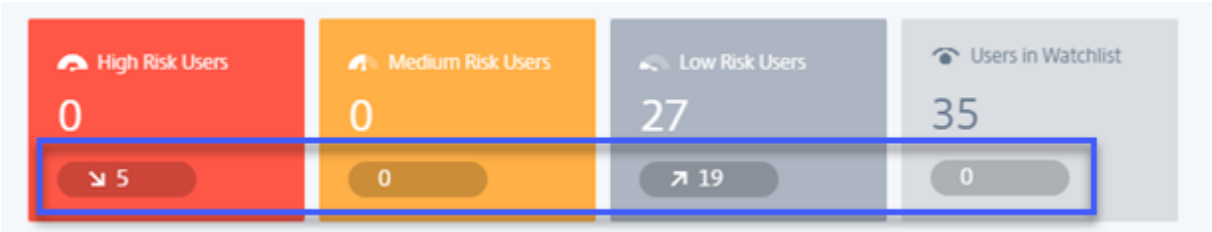
- Die Seite **Risikoindikator-Details** ist veraltet. Zuvor wurde diese Seite angezeigt, als im Bereich **Risikoindikatoren** oder auf der Seite **Risikoindikatorübersicht** einen Risikoindikator aus-

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

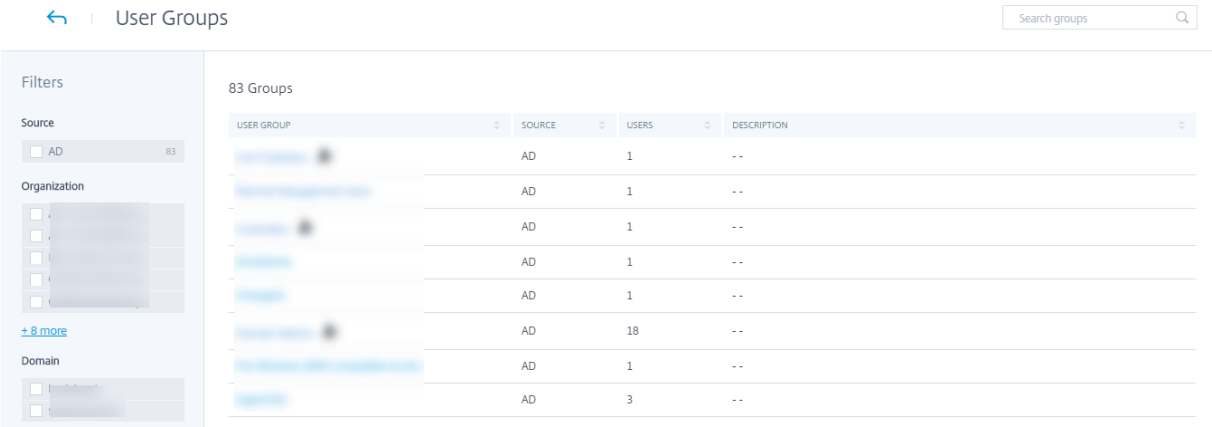
gewählt wurde.



Trendansicht Im **Benutzer**-Dashboard wird die Trendansicht der Benutzeranzahl von **Benutzer mit hohem Risiko**, **Benutzer mit mittlerem Risiko**, **Benutzer mit geringem Risiko** und **Benutzer in Watchlist**-Karten entfernt.



Seite "Benutzergruppen" Die Seite **Benutzergruppen** unter der Option **Einstellungen** ist veraltet. Sie können eine Benutzergruppe nicht mehr als privilegierte Gruppe hinzufügen oder entfernen. Sie können jedoch einzelne Benutzer als privilegierte Benutzer hinzufügen oder entfernen. Weitere Einzelheiten finden Sie unter Privilegierte Benutzer.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

26. Juni 2020

Veraltete Features

Ungewöhnliche Risikoindikatoren für den Anwendungszugriff (Virtual/SaaS) sind veraltet Die Risikoindikatoren für Citrix Virtual Apps and Desktops - **Ungewöhnliche Zeit des Anwendungszugriffs (virtuell)** und **ungewöhnliche Zeit des Anwendungszugriffs (SaaS)** wurden eingestellt. Sie können nur historische Daten zu diesen Indikatoren anzeigen.

Die folgenden Änderungen gelten als Teil dieser Abwertung:

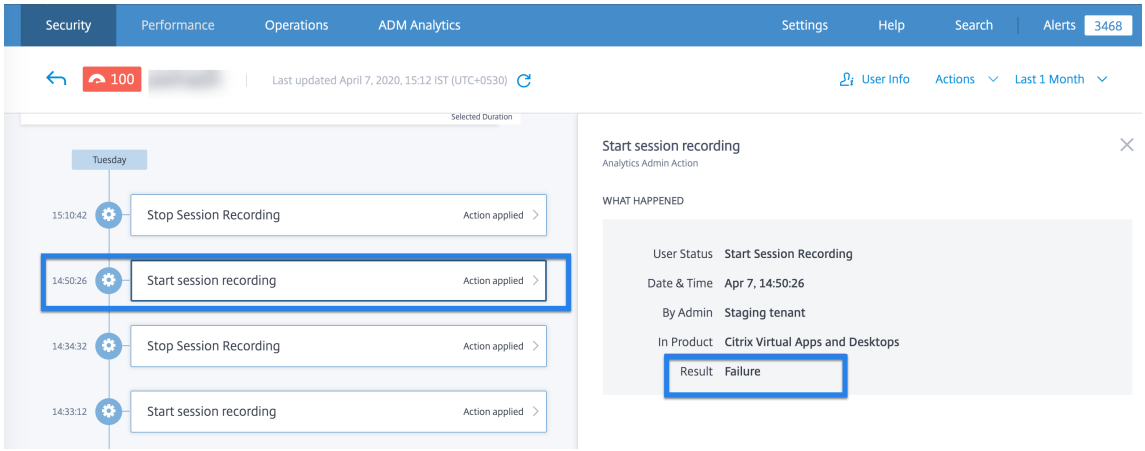
- Analytics generiert diese Risikoindikatoren nicht mehr.
- Analytics generiert keine Richtlinien mehr mit diesen Risikoindikatoren als Bedingungen.
- Standardrichtlinien mit diesen Risikoindikatoren, da die Bedingungen nicht mehr wirksam werden.

Weitere Informationen finden Sie unter Citrix Virtual Apps and Desktops und Citrix DaaS-Risikoindikatoren.

02. Juni 2020

Behobene Probleme

- Auf der Zeitleiste des Benutzerrisikos wird der Status der Aktionen für Virtual Apps and Desktops (richtlinienbasiert oder manuell angewendet) als “Fehler”angezeigt, obwohl die Aktionen erfolgreich auf das Benutzerkonto angewendet wurden. Beispielsweise wird die Aktion **Sitzungsaufzeichnung starten** erfolgreich auf das Benutzerkonto angewendet, das Ergebnis wird jedoch als “Fehler”angezeigt. [CAS-32773]



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

11. Mai 2020

Behobene Probleme

- Für einige Benutzer werden die richtlinienbasierten Aktionen nicht ausgelöst und der Modus zur Durchsetzung von Richtlinien kann nicht angewendet werden. Dieses Problem tritt auf, wenn die Kunden-IDs nicht in Kleinbuchstaben sind.

  [CAS-34209], [CAS-34141]

- Für einige Benutzer konnten keine benutzerdefinierten Risikoindikatoren erstellt werden. Dieses Problem tritt auf, wenn die Kunden-IDs nicht in Kleinbuchstaben sind.

  [CAS-34139]

29. April 2020

Behobene Probleme

- Aktionen, die auf Risikoindikatoren für Citrix Virtual Apps and Desktops angewendet werden, werden nicht wirksam, obwohl Analytics eine Meldung anzeigt, dass die Aktionen erfolgreich angewendet wurden. Dieses Problem wird in der Version Citrix Virtual Apps and Desktops 7 1912 beobachtet.

  [CAS-31544]

02. April 2020

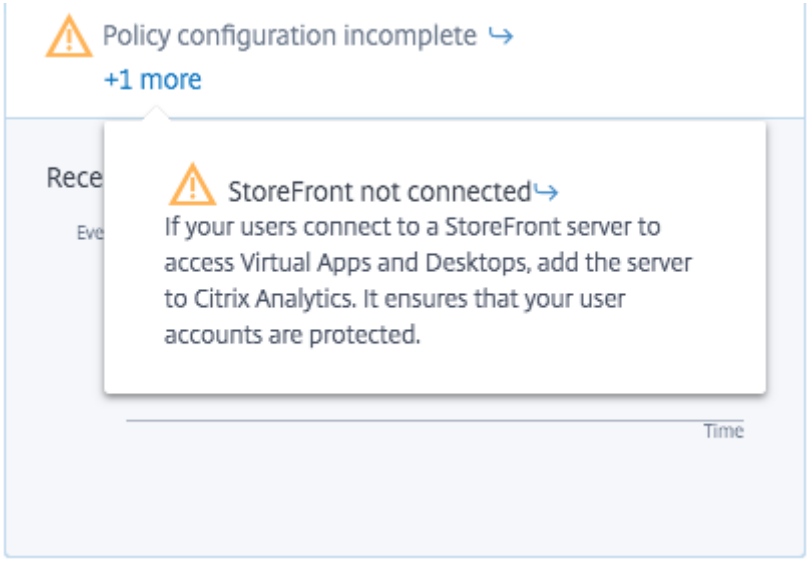
Neue Features

Deaktivieren Sie die Datenverarbeitung, wenn StoreFront nicht hinzugefügt wird Auf der Datenquellen-Sitekarte **Einstellungen** > **Datenquellen** > **Sicherheit** > Datenquellen-Sitekarte für **Virtual Apps and Desktops** wird die Schaltfläche **Datenverarbeitung einschalten** nicht aktiviert, wenn Sie StoreFront nicht integriert haben. Auf der Site-Karte wird die Warnmeldung **StoreFront nicht verbunden** angezeigt. Wenn Sie über eine aktive on-premises Site verfügen, von der Analytics Daten empfangen soll, müssen Sie sicherstellen, dass Sie StoreFront in Citrix Analytics integriert haben. Es stellt sicher, dass Ihre Benutzerkonten geschützt sind.

Wählen Sie auf der Sitekarte für **Virtual Apps and Desktops** die vertikalen Auslassungspunkte (⋮) aus und klicken Sie auf **StoreFront-Bereitstellung verbinden**. Folgen Sie auf dem angezeigten Bildschirm den Anweisungen und schließen Sie die StoreFront-Konfiguration ab.

Weitere Informationen finden Sie unter Onboarding von Citrix Virtual Apps and Desktops on-premises Sites mithilfe von StoreFront.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Behobene Probleme

- Für Benutzer von Citrix Content Collaboration werden richtlinienbasierte Aktionen unter den folgenden Bedingungen nicht wirksam:
  - Wenn benutzerdefinierte Risikoindikatorbedingungen definiert sind
  - Bis ein Risikoindikator für einen Benutzer generiert wird

  [CAS-29226]

04. März 2020

Behobene Probleme

- Wenn Gateway-Benutzer zum ersten Mal in Analytics einsteigen, sehen sie den Fehler **NetScaler ADC reagiert nicht oder die Anmeldeinformationen sind falsch**. Beim erneuten Versuch sehen sie, dass der Fehler **Gerät mit dieser IP-Adresse bereits vorhanden ist**.

[CAS-31180]

20. Februar 2020

Neue Features

Angebot von Citrix Analytics für Sicherheit Citrix Analytics for Security ist jetzt für ein Einzelabonnement verfügbar.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Sie können Citrix Analytics for Security abonnieren und Einblicke erhalten, die für dieses Angebot spezifisch sind. Weitere Informationen finden Sie unter Erste Schritte.

Risikokategorien Dashboard Citrix Analytics führt die Kategorisierung von Risikoindikatoren basierend auf Risiken ein, die ähnliche Auswirkungen auf den Sicherheitsaspekt des Unternehmens haben. Dieses Dashboard bietet einen umfassenden Überblick über die Risiken und kritischen Risiken, die sofortige Aufmerksamkeit erfordern. Für Standardrisikoindikatoren weist Analytics automatisch eine Risikokategorie basierend auf dem Risikorisiko zu. Für benutzerdefinierte Risikoindikatoren müssen Sie basierend auf dem Risikorisiko eine geeignete Risikokategorie auswählen.

Analytics unterstützt die folgenden Risikokategorien:

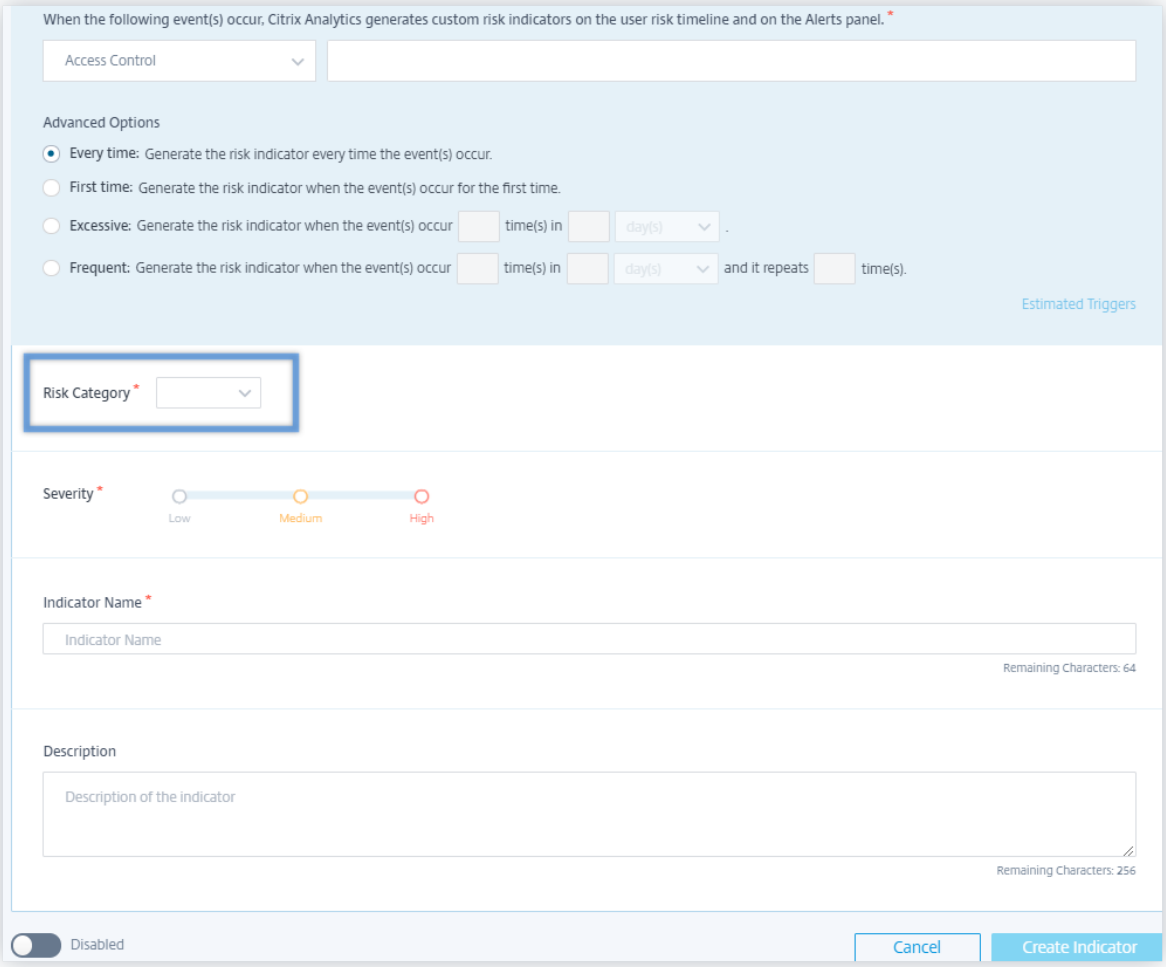
- Exfiltration von Daten
- Insider-Bedrohungen
- Kompromittierte Benutzer
- Kompromittierte Endpunkte

Weitere Informationen finden Sie unter Risikokategorien.

Spalte Risikokategorie auf der Seite Benutzerdefinierte Indikatoren Die Spalte **Risikokategorie** wird auf der Seite Benutzerdefinierter Risikoindikator eingeführt. Basierend auf der Art der Risikoexposition können Sie eine Risikokategorie für Ihren benutzerdefinierten Risikoindikator auswählen. Zuvor erstellte benutzerdefinierte Risikoindikatoren werden im Dashboard Risikokategorien angezeigt, wenn Sie sie durch Auswahl einer Risikokategorie ändern.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Weitere Informationen finden Sie unter Benutzerdefinierte Risikoindikatoren.



Änderung der Namen von Risikoindikatoren Die folgenden Namen von Risikoindikatoren wurden geändert:

Datenquelle	Alter Name	Neuer Name
Citrix Virtual Apps and Desktops von Citrix und Citrix DaaS	Ungewöhnliche Anwendungsnutzung (Virtual)	Ungewöhnliche Zeit des Anwendungszugriffs (virtuell)
Citrix Virtual Apps and Desktops von Citrix und Citrix DaaS	Ungewöhnliche Anwendungsnutzung (SaaS)	Ungewöhnliche Zeit des Anwendungszugriffs (SaaS)
Citrix Content Collaboration	Übermäßige Anmeldefehler	Übermäßige Authentifizierungsfehler

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Datenquelle	Alter Name	Neuer Name
Citrix Content Collaboration	Ungewöhnlicher Anmeldezugriff	Erster Zugriff von neuem Standort
Citrix Access Control	Ungewöhnliches Download-Volumen	Übermäßiger Datendownload
Citrix Gateway	Anmeldefehler	Übermäßige Authentifizierungsfehler
Citrix Gateway	Autorisierungsfehler	Übermäßige Autorisierungsfehler
Citrix Gateway	Ungewöhnlicher Anmeldezugriff	Erster Zugriff von neuem Standort

Weitere Informationen finden Sie unter Risikoindikatoren.

Behobene Probleme

- Für einige Benutzer kann Citrix Analytics keine Daten von Virtual Apps and Desktops empfangen, obwohl die Datenquelle erfolgreich integriert und StoreFront aktiviert ist. [CAS-24134]
- Citrix Analytics kann keine Download-Ereignisse von Citrix Content Collaboration empfangen. Daher werden die folgenden Risikoindikatoren nicht ausgelöst:
  - Anonymer Download von vertraulicher Freigabe
  - Übermäßige Link-Downloads
  - Übermäßiger Zugriff auf vertrauliche Dateien
  - Übermäßige Dateidownloads

  [CAS-29207]
- Für neu eingebundene Benutzer haben manuelle und richtlinienbasierte Aktionen, die auf NetScaler Gateway-Risikoindikatoren angewendet werden, keine Wirkung. [CAS-29029]
- Einige Benutzer können die Sitekarten auf der Seite Datenquellen nicht anzeigen. Dieses Problem wird durch Neu-Auffüllen des Caches behoben. [CAS-28781]

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

09. Januar 2020

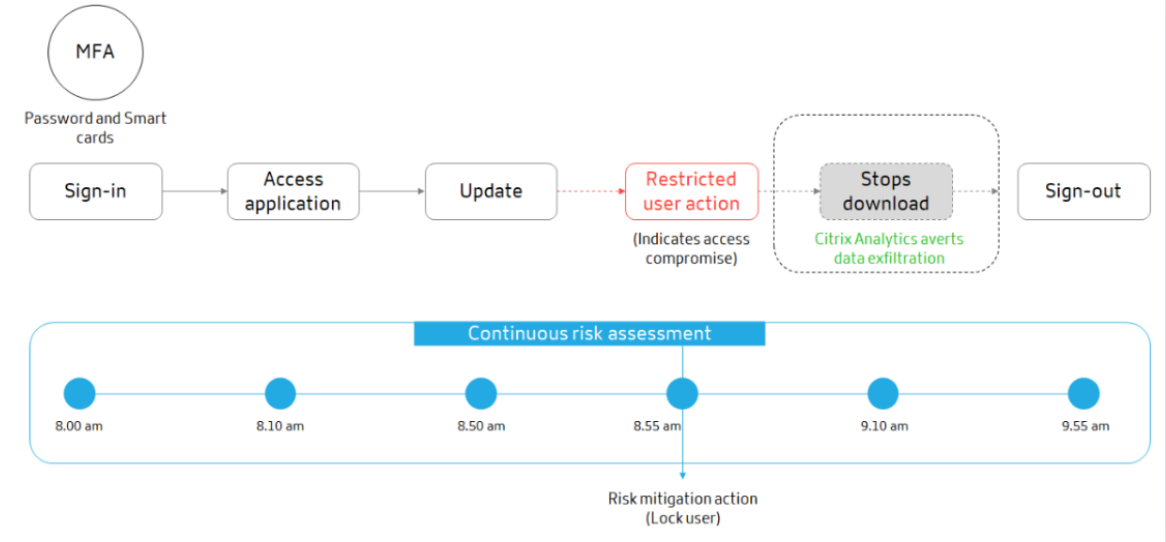
Neue Features

Kontinuierliche Risikobewertung Einige Herausforderungen für Citrix Workspace-Benutzer bestehen darin, dass der Fernzugriff sensible Daten durch cyberkriminelle Aktivitäten wie Datenexfiltration, Diebstahl, Vandalismus und Serviceunterbrechungen Sicherheitsrisiken aussetzt. Mitarbeiter innerhalb von Organisationen werden wahrscheinlich ebenfalls zu diesem Schaden beitragen.

Einige Möglichkeiten, diesen Risiken zu begegnen, sind die Implementierung einer Multifaktor-Authentifizierung, die Durchsetzung kurzer Anmelde-Timeouts usw. Obwohl diese Risikobewertungsmethoden ein höheres Sicherheitsniveau gewährleisten, bieten sie nach der ersten Validierung keine vollständige Sicherheit.

Um den Sicherheitsaspekt zu verbessern und eine bessere Benutzererfahrung zu gewährleisten, führt Citrix Analytics die Lösung einer kontinuierlichen Risikobewertung ein. Mit dieser Lösung können Sie Benutzerprofile kontinuierlich überwachen und verschiedene Maßnahmen ergreifen, wenn riskante Ereignisse erkannt werden.

Weitere Informationen finden Sie unter Kontinuierliche Risikobewertung.



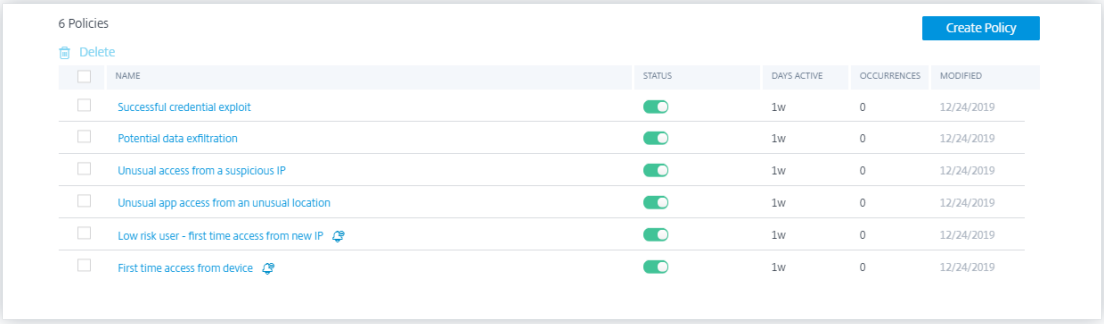
Konfiguration der Richtlinie Citrix Analytics hilft Ihnen, Richtlinienkonfigurationen effizienter zu verwalten. Sie können Benutzerkonten mithilfe der folgenden Funktionen vor böswilligen Angriffen schützen:

- **Standardrichtlinien**: Citrix Analytics unterstützt die folgenden Standardrichtlinien:
  - Erfolgreicher Berechtigungs-Exploit

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Potenzielle Datenexfiltration
- Ungewöhnlicher Zugriff von einer verdächtigen IP
- Ungewöhnlicher App-Zugriff von einem ungewöhnlichen Ort
- Benutzer mit geringem Risiko - Erstzugriff von neuer IP
- Erster Zugriff vom Gerät

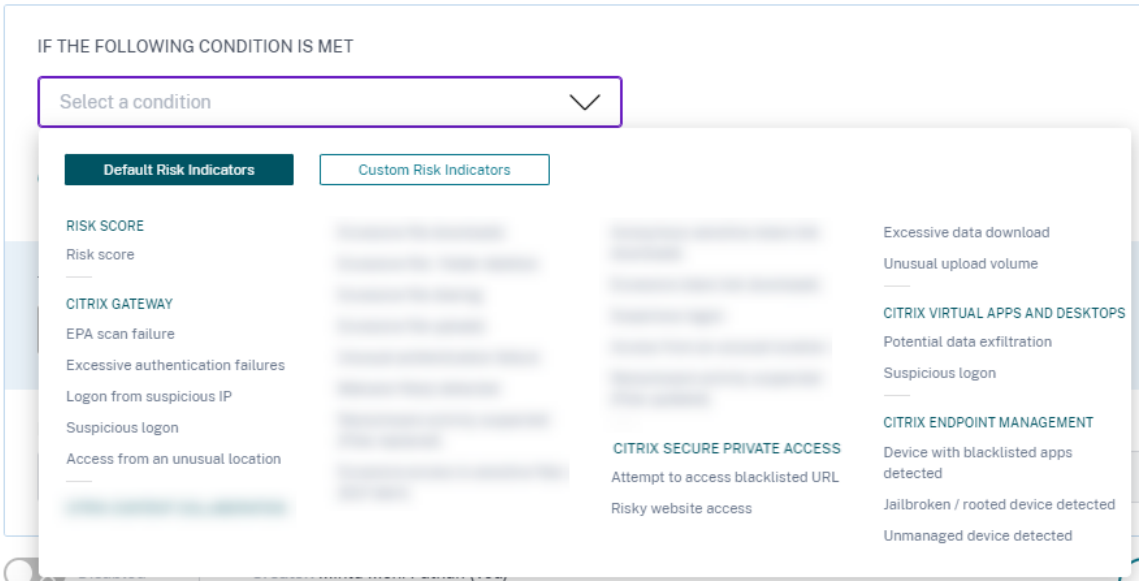
Sie können die Standardrichtlinien basierend auf Ihren Anforderungen ändern.



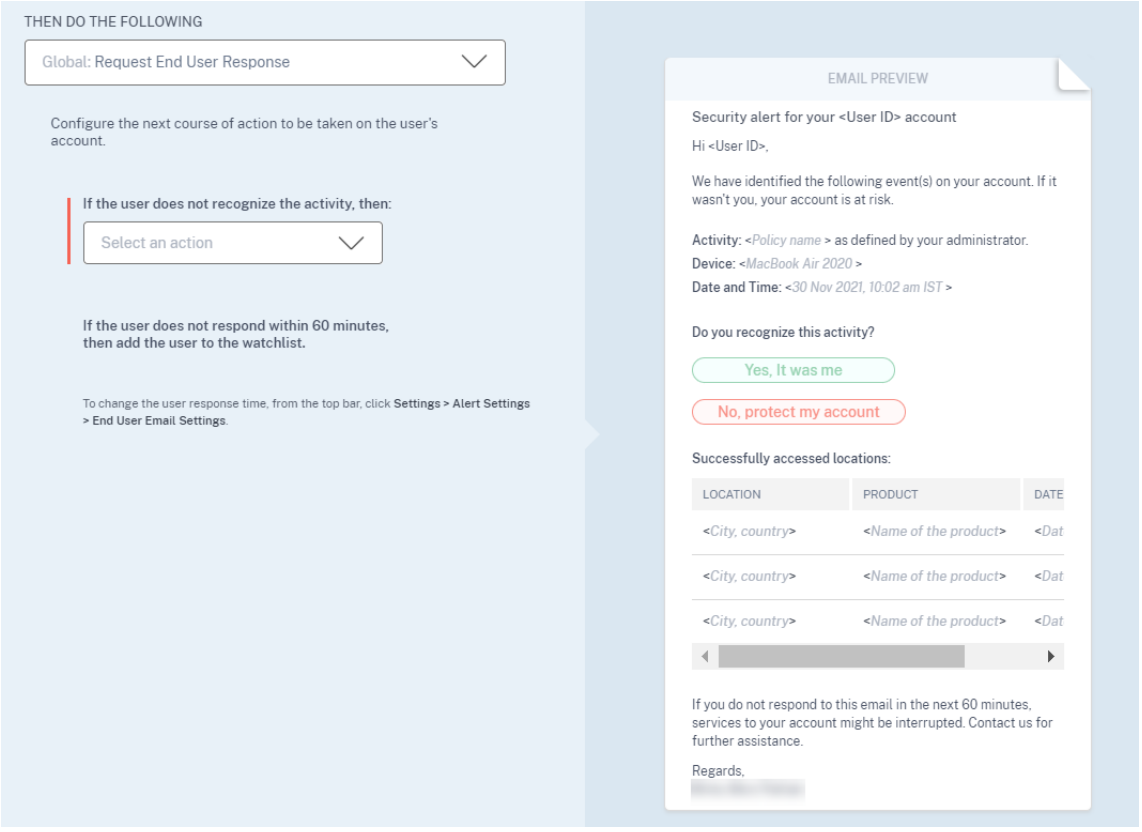
- **Mehrere Bedingungen**: Eine Richtlinie kann bis zu vier Bedingungen enthalten. Die Bedingungen können mit Kombinationen von Risikobewertungen und Risikoindikatoren oder beidem festgelegt werden.

- **Standard- und benutzerdefinierte Risikoindikatoren**: Das Konditionen Menü auf der Seite "**Richtlinie erstellen** "wird jetzt basierend auf Standard- und benutzerdefinierten Risikoindikatoren getrennt. Beim Erstellen einer Richtlinie können Sie zwischen den Registerkarten Standard- und benutzerdefinierte Risikoindikatoren wechseln und die Risikoindikatorbedingungen festlegen.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

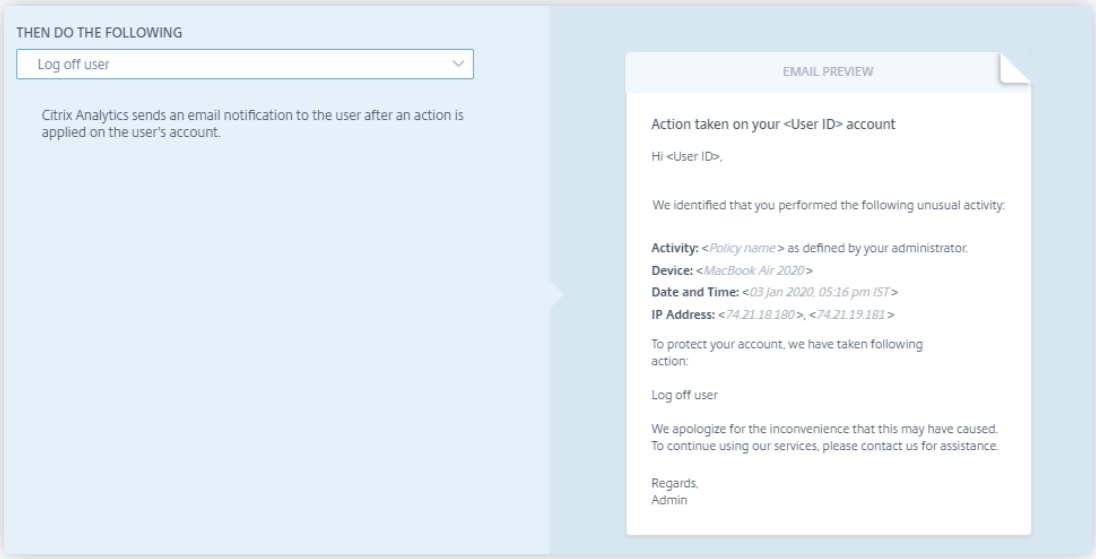


- **Endbenutzerantwort anfordern**: Citrix Analytics führt die Aktion **Endbenutzerantwort anfordern** ein. Mit dieser Aktion können Sie dem Benutzer eine E-Mail-Benachrichtigung bezüglich der erkannten riskanten Aktivität senden. Sobald der Benutzer auf die Aktivität reagiert, können Sie die nächste Vorgehensweise festlegen, die für sein Konto ergriffen werden soll. Sie können auch die Reaktionszeit des Benutzers einstellen. Wenn keine Antwort eingeht, betrachtet Citrix Analytics **Keine Antwort** als Status.

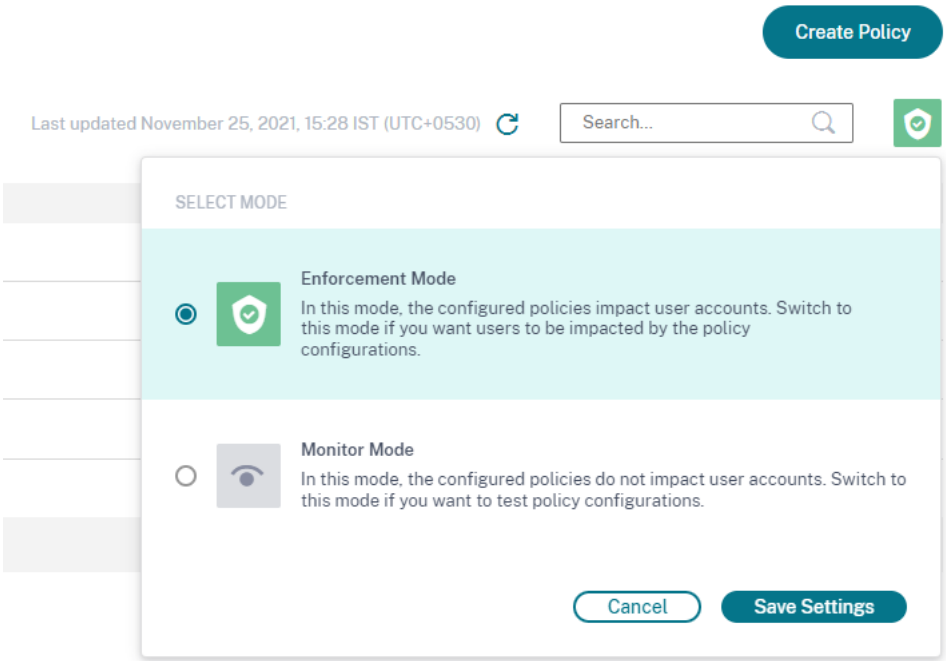


© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Unterbrechende Aktionen anwenden**: Sie können die Benutzer benachrichtigen, wenn eine störende Aktion wie **Benutzer abmelden** oder **Benutzer sperren**angewendet wird. Eine Benachrichtigung wird an den Benutzer mit Details der Aktivität und der angewendeten Aktion gesendet. Diese Aktion unterbricht vorübergehend Dienste für das Benutzerkonto, um weiteren Missbrauch zu verhindern. Um weiterhin auf das Konto zuzugreifen, muss der Benutzer den Administrator kontaktieren, um Hilfe zu erhalten.



- **Durchsetzungs- und Überwachungsmodi**: Sie können Durchsetzungs- oder Überwachungsmodi für Ihre Richtlinien festlegen.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

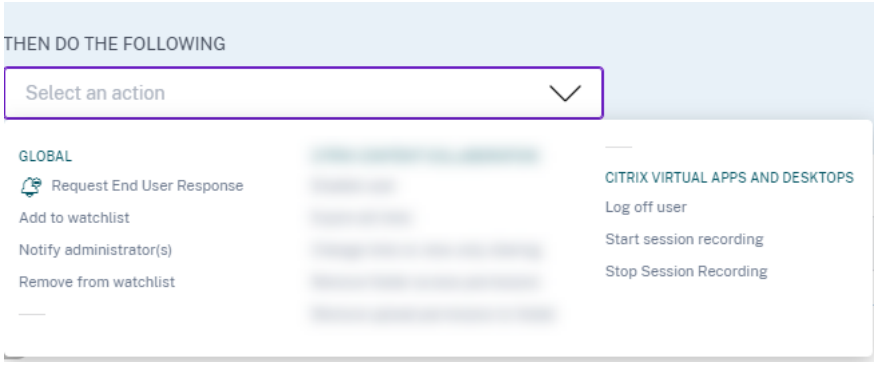
Weitere Informationen zu Richtlinienverbesserungen finden Sie unter Richtlinien und Aktionen.

Benutzer sperren und Benutzeraktionen entsperren Citrix Analytics führt die folgenden Gateway-Aktionen ein:

- Benutzer sperren
- Benutzer entsperren

Sie können diese Aktionen entweder manuell oder bei der Konfiguration von Richtlinien anwenden.

Weitere Informationen finden Sie unter Was sind Aktionen.



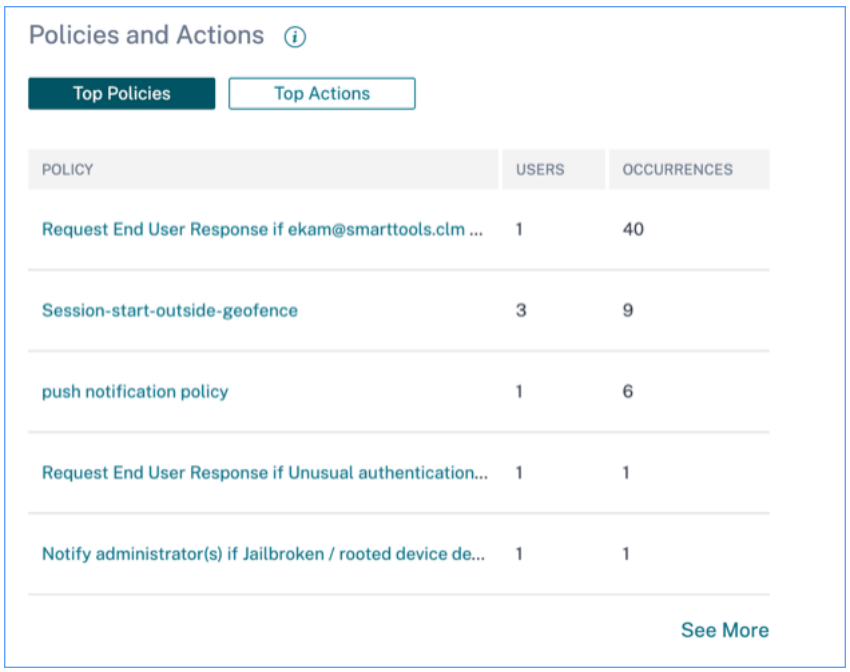
Zugriff auf das Zusammenfassungs-Dashboard Citrix Analytics führt den Bereich **Zugriffsübersicht** im **Benutzer-Dashboard** ein. Es fasst die Gesamtzahl der Versuche zusammen, die Benutzer unternommen haben, auf die Ressourcen innerhalb einer Organisation zuzugreifen.

Weitere Informationen finden Sie unter Access-Zusammenfassung.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Richtlinien- und Aktionen-Dashboard Citrix Analytics führt den Bereich **Richtlinien und Aktionen** im **Benutzer-Dashboard** ein. Es zeigt die fünf wichtigsten Richtlinien und Aktionen an, die auf Benutzerprofile angewendet werden. Sie können Daten basierend auf den Top-Richtlinien und den Top-Aktionen für einen ausgewählten Zeitraum sortieren.

Weitere Informationen finden Sie unter Richtlinien und Aktionen.



Self-Service-Suche für Richtlinien Verwenden Sie die Self-Service-Suche, um die Benutzerereignisse anzuzeigen, die Ihren definierten Richtlinien entsprechen. Sie können auch die Aktionen anzeigen, die Analytics für diese anomalen Ereignisse angewendet hat. Verwenden Sie die Facetten und das Suchfeld, um nach den erforderlichen Ereignissen zu suchen.

Um die Ereignisse anzuzeigen, wählen Sie im Suchfeld **Richtlinien** aus der Liste aus, wählen Sie den Zeitraum aus, und klicken Sie dann auf **Suchen**.

Weitere Informationen finden Sie unter Self-Service-Suche nach Richtlinien.

Veraltete Features

Richtlinienbasierte Änderung des Risiko-Scores wurde entfernt Wenn Sie Richtlinien konfigurieren, können Sie die richtlinienbasierte Bedingung für **Änderungen des Risiko-Scores** nicht mehr verwenden. Citrix Analytics unterstützt diese Bedingung nicht.

Weitere Informationen finden Sie unter Richtlinien und Aktionen.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Mehrere richtlinienbasierte Aktionen wurden entfernt Wenn Sie Richtlinien konfigurieren, können Sie nicht mehr mehrere Aktionen anwenden. Citrix Analytics unterstützt nur eine Aktion für jede Richtlinie.

Weitere Informationen finden Sie unter Richtlinien und Aktionen.

Behobene Probleme

- Delegierte schreibgeschützte Administratoren stoßen beim Zugriff auf die Dashboards **Benutzerzugriff** und **App-Zugriff** auf einen Fehler. [CAS-16297]

12. Dezember 2019

Neue Features

Unterstützung für Splunk-Versionen Citrix Analytics unterstützt die folgenden Versionen von Splunk:

- **Splunk 8.0 64-Bit**
- **Splunk 7.3 64-Bit**

Um die maximalen Sicherheitsvorteile der Splunk-Integration zu nutzen, aktualisieren Sie von der Download-Seite auf die neueste Version der Splunk-Add-On-App.

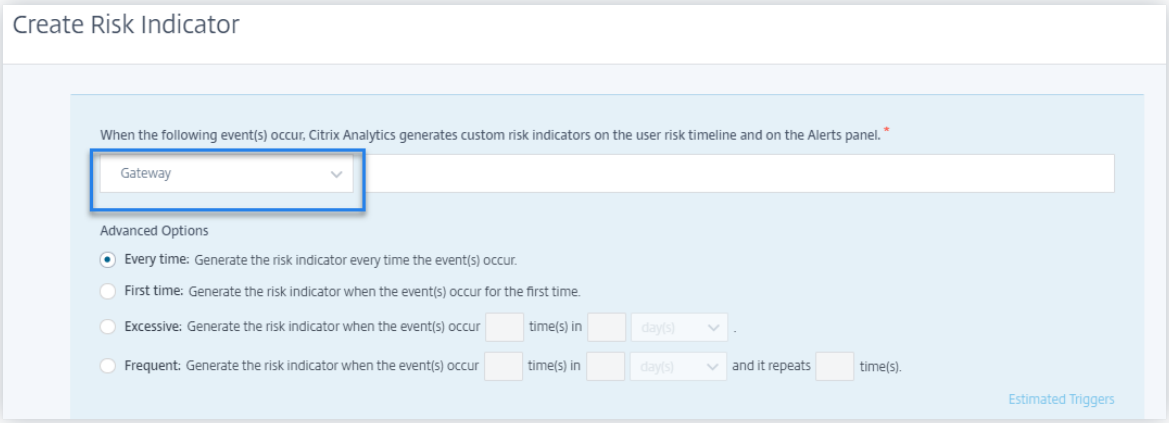
Weitere Informationen zu unterstützten Splunk-Versionen finden Sie unter Unterstützte Versionen.

04. Dezember 2019

Neue Features

Benutzerdefinierte Risikoindikator für NetScaler Gateway Mithilfe benutzerdefinierter Risikoindikatoren können Sie jetzt die Bedingungen und die Häufigkeit für das Auslösen von Risikoindikatoren für NetScaler Gateway-Ereignisse definieren. Wenn ein Benutzerereignis die Bedingungen erfüllt, löst Analytics die Risikoindikatoren aus. Weitere Informationen zum Erstellen eines benutzerdefinierten Risikoindikators finden Sie unter Benutzerdefinierte Risikoindikatoren.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

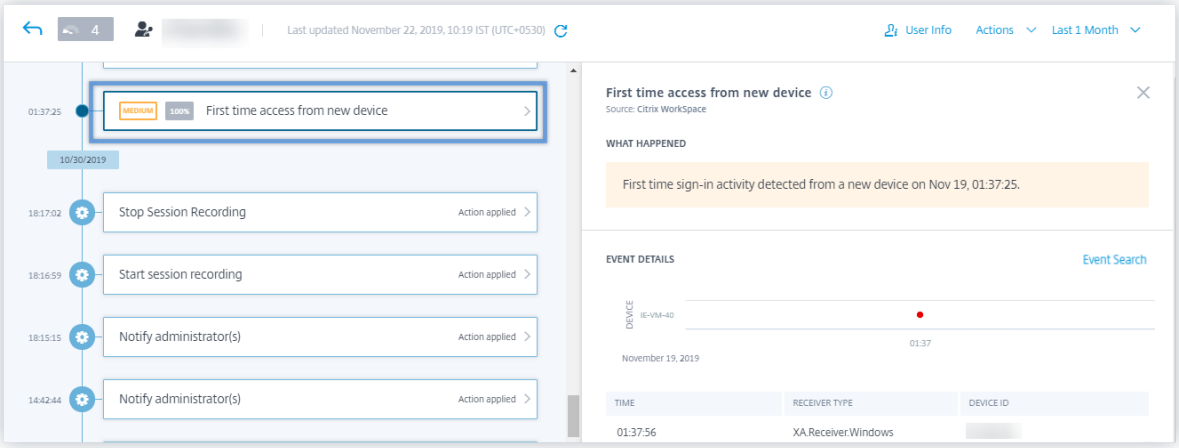


22. November 2019

Neue Features

Erster Zugriff von einem neuen Gerät aus —Citrix Virtual Apps and Desktops Risikoindikator Citrix Analytics erkennt Zugriffsbedrohungen basierend auf dem Zugriff von einem neuen Gerät und löst den entsprechenden Risikoindikator aus.

Der **erste Zugriff von einem neuen Gerät** aus wird ausgelöst, wenn sich ein Benutzer nach 90 Tagen von einem Gerät aus anmeldet. Dieses Ereignis wird ausgelöst, weil Citrix Receiver in den letzten 90 Tagen keine Anmeldedatensätze von diesem neuen oder unbekannten Gerät hat. Weitere Informationen finden Sie unter Citrix Virtual Apps and Desktops und Citrix DaaS-Risikoindikatoren.

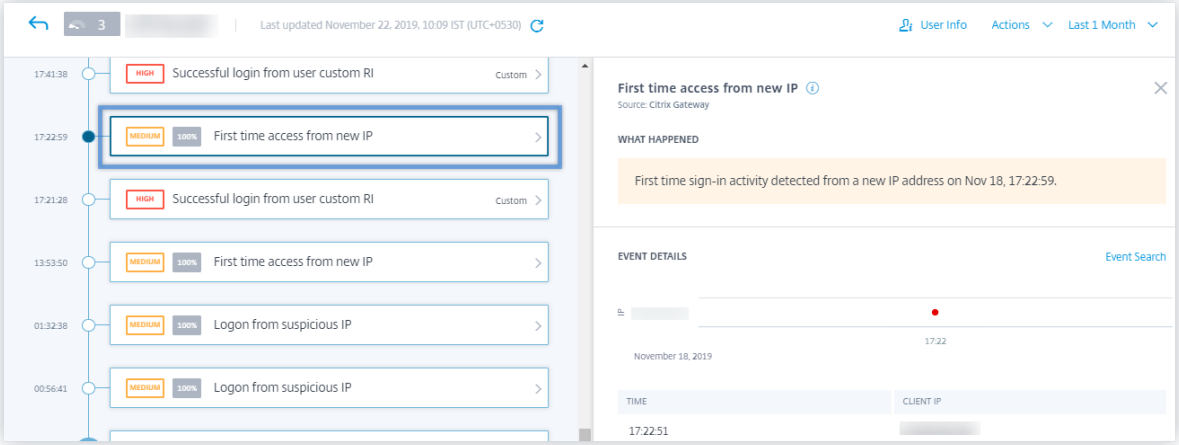


Erster Zugriff von neuer IP - NetScaler Gateway Risikoindikator Citrix Analytics erkennt Zugriffsbedrohungen basierend auf dem Zugriff von einer neuen IP-Adresse und löst den entsprechenden Risikoindikator aus.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Der **erste Zugriff von einem neuen IP-Risikoindikator** wird ausgelöst, wenn sich ein Benutzer nach 90 Tagen von einer IP-Adresse aus anmeldet. Dieses Ereignis wird ausgelöst, weil Citrix Receiver in den letzten 90 Tagen keine Anmeldedatensätze von der neuen oder unbekannten IP-Adresse hat.

Weitere Informationen finden Sie unter NetScaler Gateway-Risikoindikatoren.



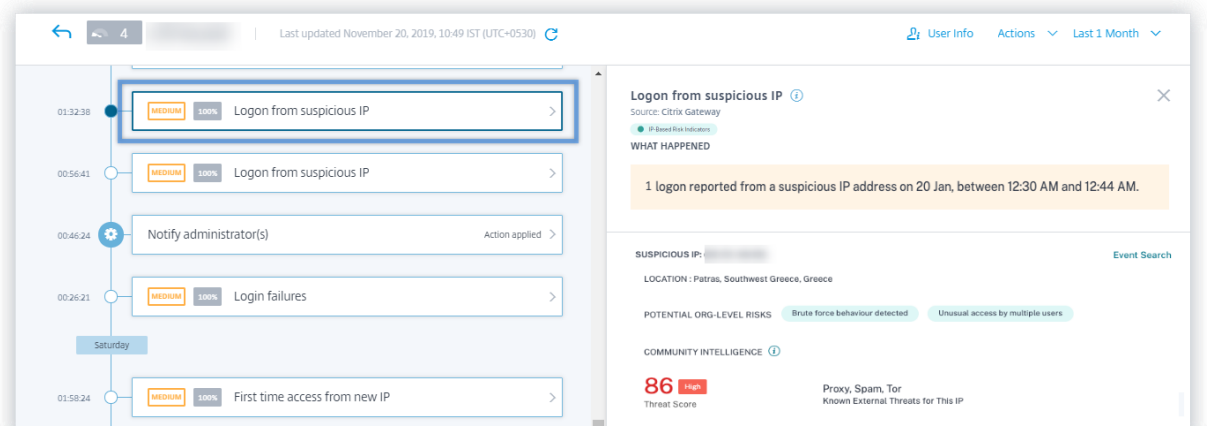
Anmeldung von verdächtiger IP - NetScaler Gateway Risikoindikator Citrix Analytics erkennt Benutzerzugriffsbedrohungen basierend auf der verdächtigen IP-Anmeldeaktivität und löst die **Anmeldung aufgrund eines verdächtigen IP-Risikoindikators aus** .

Dieser Risikoindikator wird ausgelöst, wenn ein Benutzer versucht, von einer verdächtigen IP-Adresse aus auf das Netzwerk zuzugreifen. Analytics betrachtet eine IP-Adresse aufgrund einer der folgenden Bedingungen als verdächtig:

- Ist im externen IP-Bedrohungsintelligence-Feed aufgeführt
- Verfügt über mehrere Benutzeranmeldedatensätze von einem ungewöhnlichen Ort
- Übermäßige fehlgeschlagene Anmeldeversuche, die auf einen Brute-Force-Angriff hinweisen könnten

Weitere Informationen finden Sie unter NetScaler Gateway-Risikoindikatoren.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Self-Service-Suche für NetScaler Gateway Ereignisse Verwenden Sie die Self-Service-Suchfunktion, um Einblick in Benutzerereignisse zu erhalten, die von der NetScaler Gateway-Datenquelle Citrix Analytics empfängt Ereignisse wie Authentifizierungsphase, Autorisierungstyp, VPN-Sitzungscode, VPN-Sitzungsstatus für NetScaler Gateway-Benutzer. Verwenden Sie die Facetten und das Suchfeld, um nach den erforderlichen Ereignissen zu suchen und die zugrunde liegenden Daten zu untersuchen.

Um die Ereignisse anzuzeigen, wählen Sie im Suchfeld **Gateway** aus der Liste aus, wählen Sie den Zeitraum aus, und klicken Sie dann auf **Suchen**.

Weitere Informationen finden Sie unter Self-Service-Suche für Gateway.

Self-Service-Suche für Citrix Remote Browser Isolationsereignisse Verwenden Sie die Self-Service-Suchfunktion, um einen Einblick in die vom Citrix Remote Browser Isolation Service empfangenen Browserereignisse zu erhalten. Citrix Analytics empfängt Ereignisse wie Sitzungsverbindung, Sitzungsstart, veröffentlichte Anwendungen, gelöschte Anwendungen für jede Benutzerverbindung. Verwenden Sie das Suchfeld, um nach den erforderlichen Ereignissen zu suchen und die zugrunde liegenden Daten zu untersuchen.

Um die Ereignisse anzuzeigen, wählen Sie im Suchfeld **Remote Browser Isolation** aus der Liste aus, wählen Sie den Zeitraum aus, und klicken Sie dann auf **Suchen**.

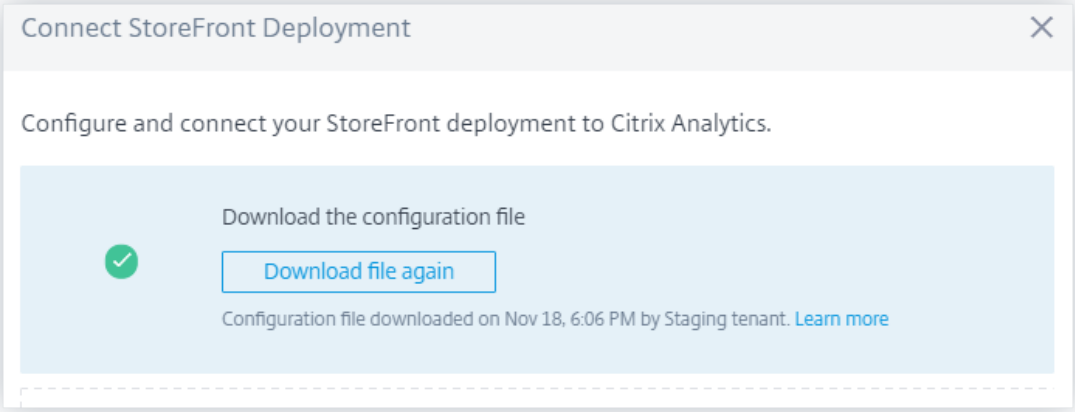
Weitere Informationen finden Sie unter Self-Service-Suche für Remote Browser Isolation.

Aktion "Aus Beobachtungsliste entfernen" Sie können einen Benutzer entweder durch Anwenden der manuellen Methode oder durch Anwenden einer richtlinienbasierten Methode aus der Watchlist entfernen. Weitere Informationen finden Sie unter Watchlist.

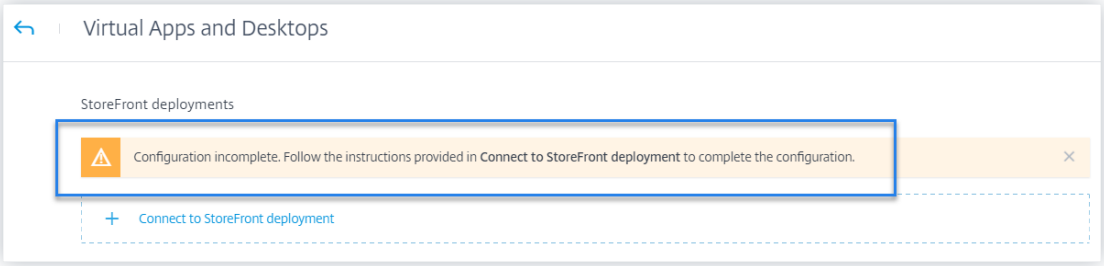
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Verbesserte Onboarding-Nachrichten bei der Konfiguration einer StoreFront-Bereitstellung
Citrix Analytics liefert jetzt die folgenden Meldungen, die Ihnen bei der Konfiguration Ihrer StoreFront-Bereitstellungen helfen:

- Nach dem Herunterladen der Konfigurationsdatei wird eine Meldung angezeigt, die das Datum und die Uhrzeit des Downloads sowie den Benutzernamen angibt. Wenn Sie diese Seite aktualisieren, ändert sich die Schaltfläche **Datei herunterladen** in **Datei neu herunterladen**.



- Wenn Ihre StoreFront-Konfiguration unvollständig ist, wird eine Warnmeldung angezeigt, die Sie anweist, den Konfigurationsschritten zu folgen und Ihre StoreFront-Bereitstellung mit Analytics zu verbinden.



Weitere Informationen zum Konfigurieren Ihrer StoreFront-Bereitstellung finden Sie unter Integrieren von on-premises Citrix Virtual Apps and Desktops mit StoreFront.

Veraltete Features

Risikoindikator - Zugriff von neuem Gerät entfernen Citrix Analytics löst den Risikoindikator **"Zugriff über ein neues Gerät"nicht mehr aus** . Auf dem Benutzer-Dashboard, der Benutzerzeitleiste und dem Richtlinien-Dashboard können Sie jedoch historische Daten zu diesem Risikoindikator anzeigen.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Für zuvor erstellte Richtlinien, die auf **Zugriff von einem neuen Gerät** basieren, müssen Sie entweder die Richtlinie ändern oder eine Richtlinie mit dem neuen Risikoindikator erstellen **Erstzugriff von einem neuen Gerät aus**.

Behobene Probleme

- Bei der Self-Service-Suche nach Authentifizierung werden die Ereignisse nicht angezeigt. [CAS-24959]

08. November 2019

Behobene Probleme

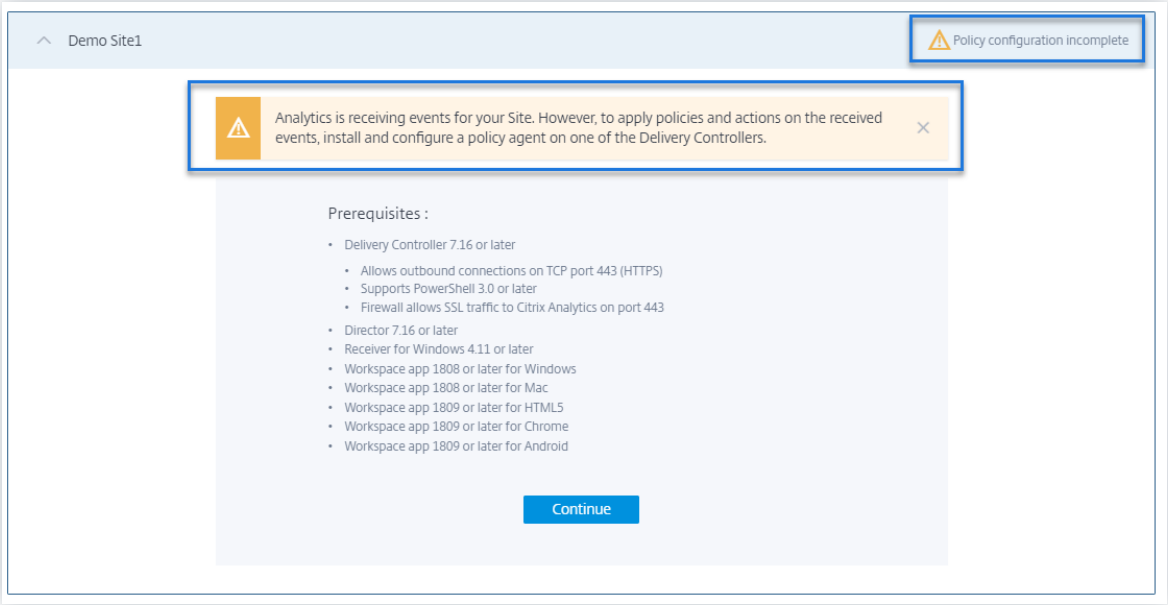
- Bei Citrix Content Collaboration Risikoindikatoren können Benutzer keine Aktionen auf den Risikozeitplan anwenden. [CAS-24844]
- Die Citrix Workspace-App für Chrome vor Version 1911 sendet keine Ereignisdetails an Citrix Analytics. [CAS-24938]

21. Oktober 2019

Neue Features

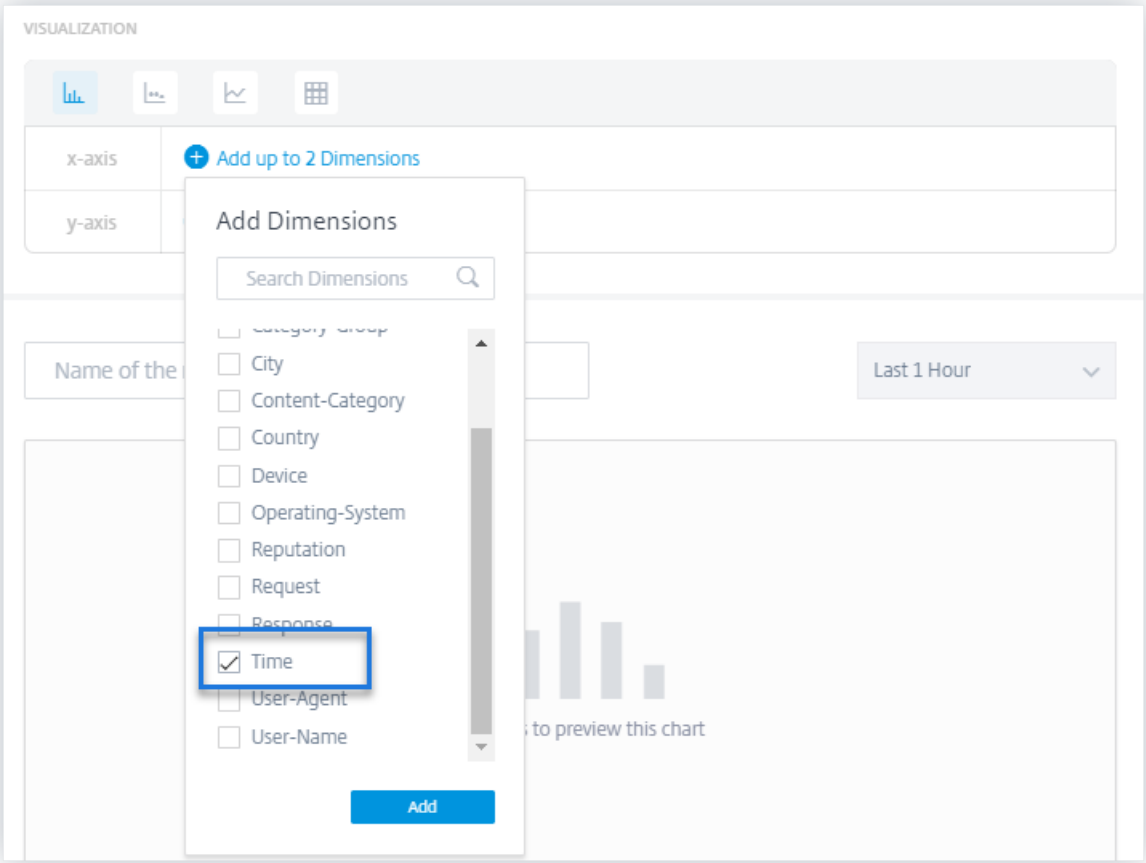
Name für Analytics-Agent geändert Der Name des Agents wird jetzt als **Analytics-Richtlinien-Agent** auf den Benutzeroberflächen erwähnt, um seine Rolle anzugeben. Beim Onboarding der on-premises Citrix Virtual Apps and Desktops Datenquellen benachrichtigt Citrix Analytics eindeutig, dass ein Richtlinien-Agent nur zum Konfigurieren von Richtlinien und Aktionen für Ihre Site erforderlich ist. Dieser Agent spielt keine Rolle bei der Übertragung von Daten aus der Datenquelle. Weitere Informationen finden Sie unter Citrix Virtual Apps and Desktops und Citrix DaaS-Datenquelle.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Unterstützung für die Zeitdimension für benutzerdefinierten Bericht Sie können die Ereignisse jetzt zeitbasiert gruppieren, indem Sie die Dimension **Zeit** für die X-Achse auswählen. Der Bericht zeigt die Gesamtzahl der empfangenen Ereignisse basierend auf den Zeitintervallen für den ausgewählten Zeitraum an. Weitere Informationen zum Erstellen von Berichten finden Sie unter Benutzerdefinierte Berichte.

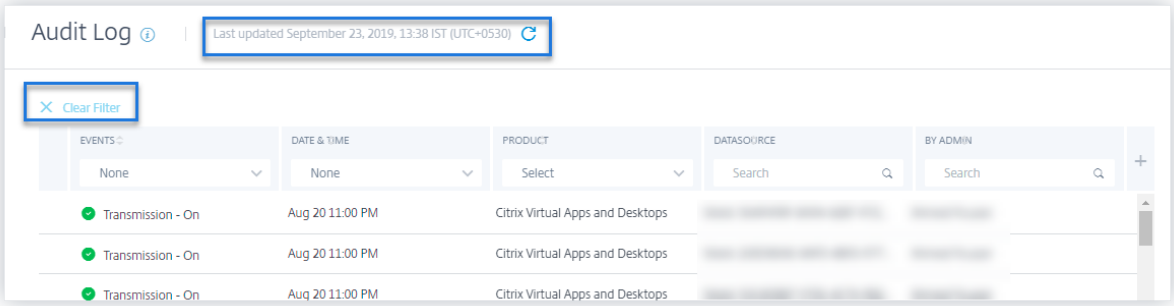
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Verbesserungen bei Audit-Protokollen Die Benutzerfreundlichkeit der Seite "**Audit-Log** "wurde verbessert.

- Sie können die Datums- und Uhrzeitdetails anzeigen, wann die Seite "**Audit-Log** "zuletzt aktualisiert wurde, und die Seite aktualisieren, um die neuesten Überwachungsprotokolle anzuzeigen.
- Sie können alle Filter löschen, die auf die Überwachungsprotokolle angewendet wurden.

Weitere Informationen zu den Audit-Daten finden Sie unter Audit-Protokolle.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Behobene Probleme

- Citrix Analytics kann den Risikoindikator für **anonyme IP-Adressen** nicht generieren, obwohl Microsoft Graph Security erfolgreich eingebunden wurde. [CAS-21329]
- Die Citrix Workspace-App für HTML5 vor Version 1910 sendet keine Ereignisdetails an Citrix Analytics. [CAS-24938]

23. September 2019

Behobene Probleme

- Auf den Datenquellen-Standortkarten zeigt das Feld **Neuestes Ereignis** falsche Datums- und Uhrzeitinformationen an. [CAS-24087]

30. August 2019

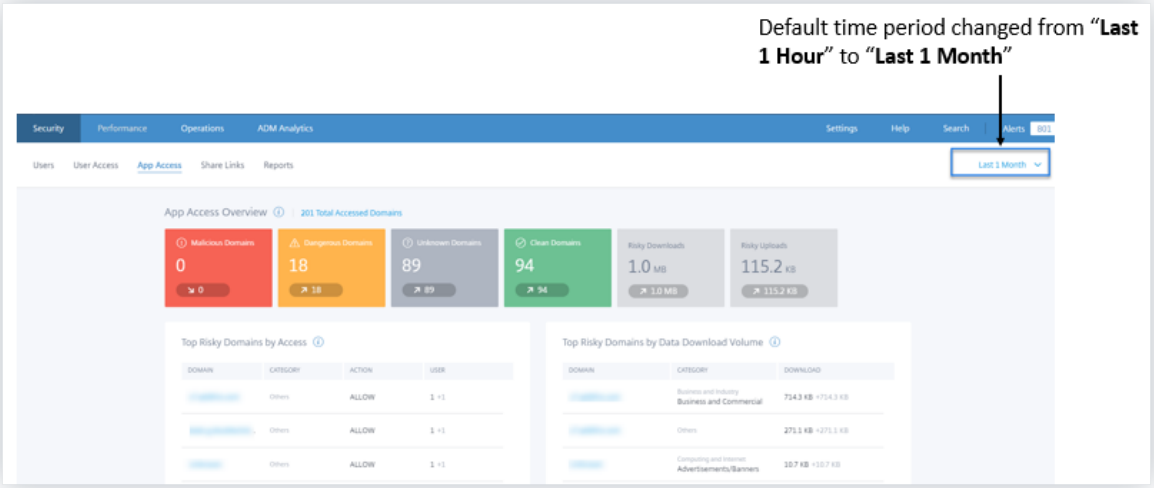
Neue Features

Änderung des Standardzeitraums über Dashboards hinweg Der Standardzeitraum in den folgenden Dashboards wird von **Letzte 1 Stunde** auf **Letzte 1 Monat**geändert:

- Benutzer
- Risiko-Timeline
- Benutzerzugriff
- App-Zugriff
- Links teilen
- Verlauf der Warnungen

Jetzt zeigen die Dashboards standardmäßig die Ereignisse für den letzten Monat an. Bei der Verwendung dieser Dashboards erhalten Sie eine ansprechendere Erfahrung. Wenn Sie beispielsweise das **App Access-Dashboard** öffnen, zeigt das Dashboard standardmäßig die App-Zugriffsereignisse für den letzten Monat an.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Behobene Probleme

- Bei Risikoindikatoren für Content Collaboration kann die auf **Benutzerrichtlinien basierende Aktion deaktivieren** nicht erfolgreich angewendet werden. [CAS-17304]
- Citrix Analytics kann keine Ereignisse von NetScaler Gateway 13.0 verarbeiten. Dieses Problem tritt auf, weil NetScaler Gateway 13.0 in den an Citrix Analytics gesendeten Anmeldeereignissen keine Benutzernamen angibt. [CAS-21339]

20. August 2019

Neue Features

Verbesserungen bei der Self-Service-Suche

- Die Benutzerfreundlichkeit der Self-Service-Seite wird verbessert. Sie können jetzt nahtlos zwischen der Zeitleiste des Benutzerrisikos und der Self-Service-Suchseite hin und her wechseln.
- Sie können Ihre Ereignisse jetzt nach Zeit sortieren. Standardmäßig werden die neuesten Ereignisse zuerst in der Ereignistabelle angezeigt. Klicken Sie auf das Sortiersymbol in der Spalte **TIME**, um die Ereignisse entweder nach der letzten oder der frühesten Zeit zu sortieren.

Weitere Informationen zur Verwendung der Self-Service-Suche finden Sie unter Self-Service-Suche.

Benutzerdefinierte Berichtsverbesserungen

- Für die Datenquellen Zugriffssteuerung, Content Collaboration und Apps and Desktops wurden neue Dimensionen hinzugefügt. Sie können diese Dimensionen auswählen, um Berichte zu erstellen. Die folgenden Dimensionen werden für die Datenquellen hinzugefügt:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

  - **Access Control**: Benutzeragent, Benutzername
  - **Content Collaboration**: Benutzer-E-Mail, Benutzername, Erstellt von, Konto-ID, OAuth Client-ID, Ereignis-ID, Ordner-ID, Ordnername, Ressourcen-ID, Formular-ID, Client-IP
  - **Apps und Desktops**: Benutzername, IP-Adresse, Geräte-ID, Jail gebrochen, Typ des Sitzungsstarts, Name des Sitzungsservers, Benutzername der Sitzung, Dateiname des Downloads, Dateipfad zum Herunterladen, Name des Druckers, Dateiname der Druckauftragsdetails, SaaS-App-Start-URL, Zwischenablage-Vorgang, Ergebnis der Zwischenablagedetails

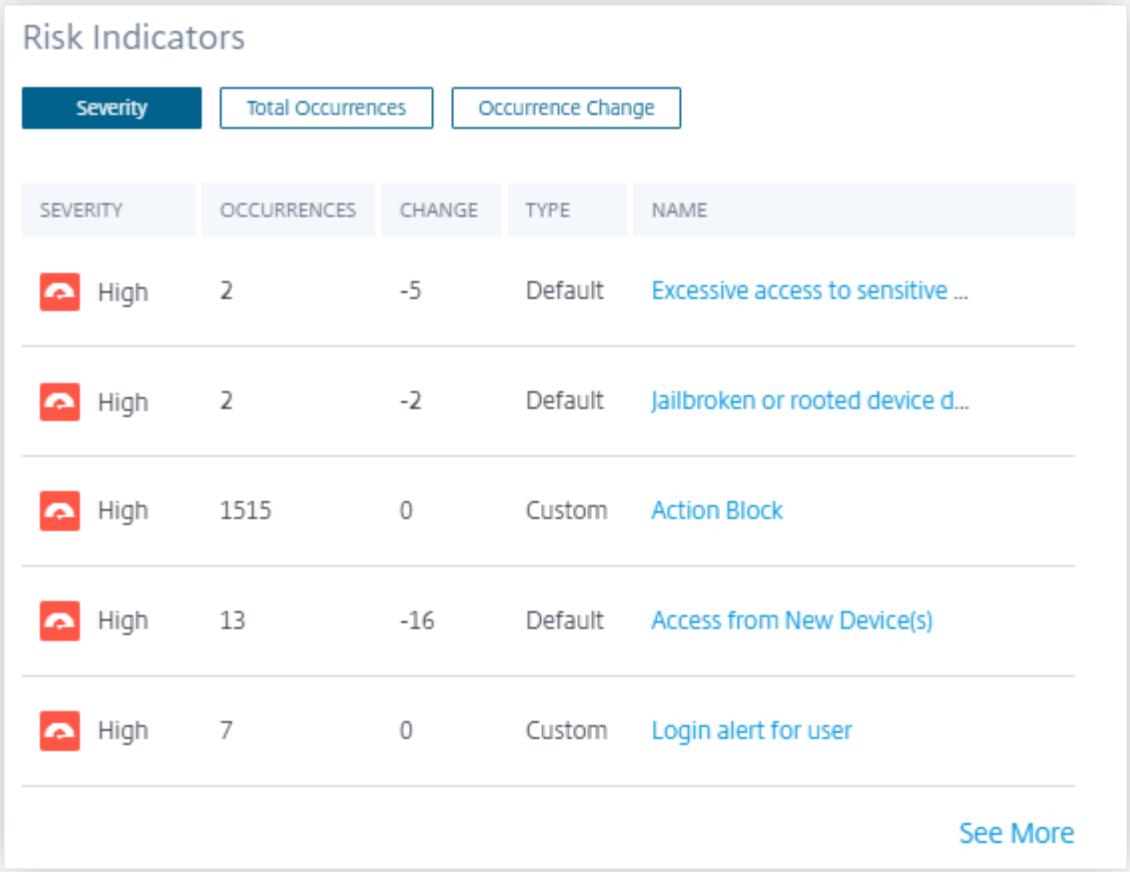
- Die Benutzeroberfläche für benutzerdefinierte Berichte wurde durch Unterstützung für Paginierung und eine Option "**Alle löschen** "für die Filter erweitert.

Weitere Informationen zum Erstellen eines benutzerdefinierten Berichts mithilfe dieser Dimensionen finden Sie unter Benutzerdefinierte Berichte.

Risikoindikatoren Dashboard Das Dashboard **Risikoindikatoren** wird auf der Seite **Benutzer** eingeführt. Es fasst die fünf wichtigsten Standard- und benutzerdefinierten Risikoindikatoren für einen Benutzer zusammen. Ein Link "Mehr anzeigen"leitet Sie zur Seite "**Risikoindikatorübersicht** "weiter. Diese Seite enthält detaillierte Informationen zu den Risikoindikatoren, die für einen ausgewählten Zeitraum generiert wurden.

Weitere Informationen finden Sie unter Benutzer-Dashboard.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

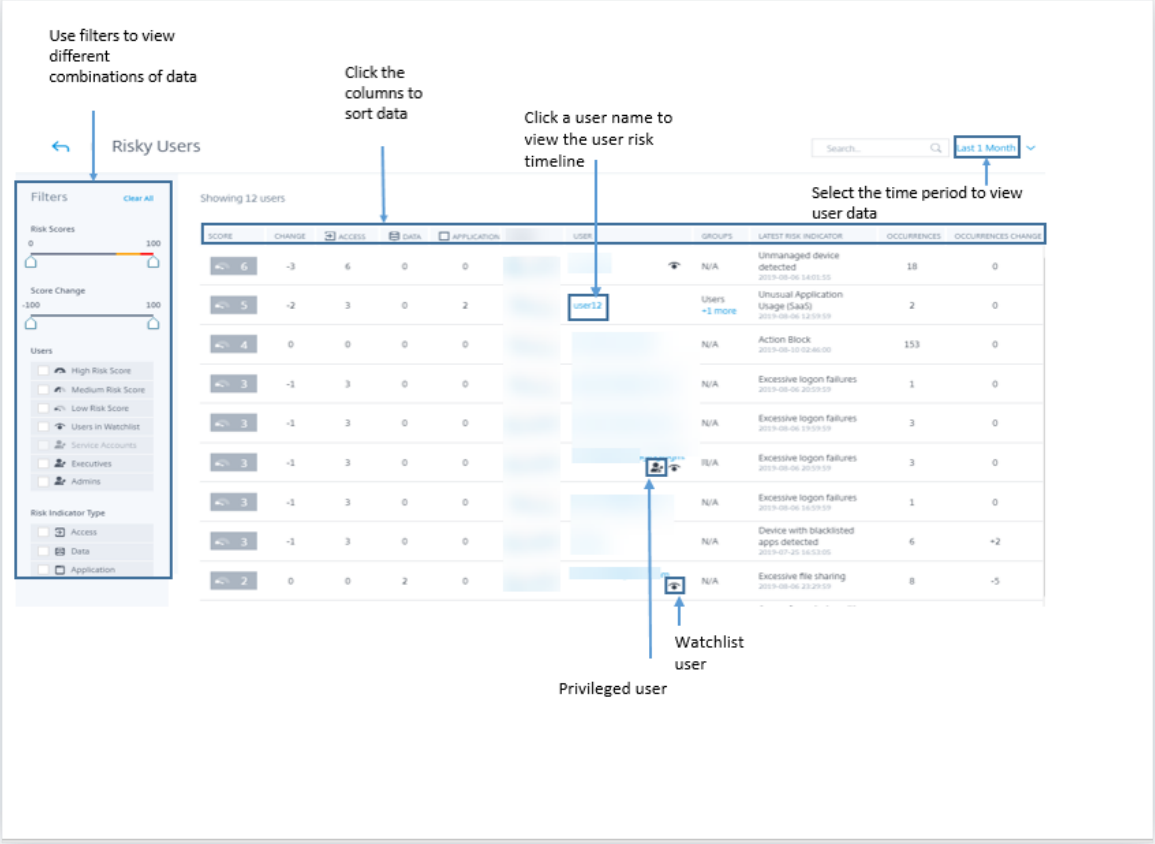


Verbesserungen des Dashboards für riskante Benutzer Citrix Analytics führt die Registerkarten **Risikoindikatoren** und **Änderung von Risikoindikatoren** im Dashboard **Riskante Benutzer** ein. Auf diesen Registerkarten können Sie die fünf riskanten Benutzer anzeigen. Das Dashboard führt auch die Spalte **Risikoindikatoren** ein. Es zeigt die Anzahl der Risikoindikatoren für einen Benutzer.

Auf der Seite **Riskante Benutzer** werden die Spalten **Vorkommen** und **Vorkommensänderungen** vorgestellt. In diesen Spalten werden die Gesamtereignisse und die Änderung der Vorkommen der benutzerdefinierten und der Standardrisikoindikatoren zusammengefasst.

Weitere Informationen finden Sie unter Benutzer-Dashboard.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Risikoindikator für Freigabelinks - Übermäßige Downloads Citrix Analytics erkennt Zugriffsbedrohungen basierend auf übermäßigen Downloads auf einem Freigabelink und löst den Risikoindikator für **übermäßige Downloads** aus. Indem Sie Share-Links mit übermäßigen Downloads basierend auf dem vorherigen Verhalten identifizieren, können Sie den Freigabelink auf mögliche Angriffe überwachen. Dieser Risikoindikator hilft Ihnen, eine übermäßige Aktivität zum Herunterladen von Dateien zu identifizieren.

Weitere Informationen finden Sie unter Übermäßige Downloads.

Self-Service-Suche nach den Authentifizierungsdaten Verwenden Sie die Self-Service-Suche, um Einblicke in die Authentifizierungsereignisse zu erhalten. Citrix Analytics erhält die Authentifizierungsereignisse wie Benutzeranmeldung, Benutzerabmeldung und Client-Update vom Identity and Access Management-Dienst von Citrix Cloud. Die Suche liefert einen detaillierten Bericht über die Authentifizierungsereignisse, hilft Ihnen, Authentifizierungsprobleme zu identifizieren und zu beheben. Sie können auch eine Suchabfrage definieren, um Ereignisse abzurufen, die Ihren definierten Kriterien entsprechen.

Um die Ereignisse anzuzeigen, wählen Sie **Authentifizierung** aus der Liste aus, wählen Sie den

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Zeitraum aus und klicken Sie dann auf **Suchen**.

Weitere Informationen finden Sie unter Self-Service-Suche nach Authentifizierung.

11. Juli 2019

Neue Features

Benutzerdefinierte Risikoindikatoren Die Standardrisikoindikatoren, die Citrix Analytics generiert, basieren auf Algorithmen für maschinelles Lernen. Mit Citrix Analytics können Sie jetzt benutzerdefinierte Risikoindikatoren erstellen. Basierend auf Benutzerereignissen können Sie die Bedingungen definieren und benutzerdefinierte Risikoindikatoren erstellen.

Wenn die definierten Bedingungen erfüllt sind, generiert Citrix Analytics die benutzerdefinierten Risikoindikatoren ähnlich den Standardrisikoindikatoren und zeigt sie in der Risikozeitleiste des Benutzers an. Benutzerdefinierte Risikoindikatoren sind mit einer Beschriftung auf der Risikozeitleiste des Benutzers gekennzeichnet.

Weitere Informationen finden Sie unter Benutzerdefinierte Risikoindikatoren.

Privilegierter Status auf dem Risikozeitplan

Die Zeitleiste für das Benutzerrisiko zeigt die folgenden Ereignisse an, wenn sich der Admin- oder Executive-Berechtigungsstatus eines Benutzers ändert:

- Zur Executive-Gruppe hinzugefügt
- Aus Executive-Gruppe entfernt
- Privileg auf Admin erhöht
- Admin-Berechtigung wurde entfernt

Wenn ein Risikoindikator für einen Benutzer ausgelöst wird, können Sie ihn mit dem angegebenen Ereignis zur Änderung des Berechtigungsstatus in Beziehung setzen. Bei Bedarf können Sie entsprechende Aktionen auf das Benutzerprofil anwenden.

Weitere Informationen finden Sie unter Zeitleiste für das Benutzerrisiko.

Aktion “Freigabelink”ablaufen

Mit Citrix Analytics können Sie Aktionen auf Risikoindikatoren für Freigabelinks anwenden. Derzeit ist die unterstützte Aktion **Freigabelink ablaufen**.

Weitere Informationen finden Sie unter Risikoindikatoren für Citrix Share-Links.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Verbesserungen bei der Self-Service-Suche

- **Unterstützung für Platzhalter* in der Suchabfrage**: Verwenden Sie das Sternchen (*) in Ihrer Suchabfrage, um ein beliebiges Zeichen Null oder mehrmals zu vergleichen. Die Suchanfrage Username = "John*"zeigt beispielsweise Ereignisse für alle Benutzernamen an, die mit John beginnen.
- **Die Option Alle löschen für Facetten hinzugefügt**: Klicken Sie auf **Alle löschen**, um alle ausgewählten Facetten gleichzeitig zu entfernen.
- **Versteckte Spaltendaten in der Ereignisliste anzeigen**: Nachdem Sie eine Spalte aus der Ereignistabelle entfernt haben, können Sie die entsprechenden Daten in der Benutzerereignisliste anzeigen. Erweitern Sie die Ereigniszeile für einen Benutzer und zeigen Sie die Daten an.

Weitere Informationen finden Sie unter Self-Service-Suche.

Datenfehlerstatus auf den Site-Karten

Auf den Sitekarten wird das Etikett **Keine Daten empfangen** in Rot angezeigt, wenn Citrix Analytics in der letzten Stunde keine Ereignisse von der Datenquelle empfängt. Es zeigt auch die Anzahl der empfangenen Ereignisse an und ist mit der entsprechenden Self-Service-Suchseite verknüpft. Mit dieser Funktion können Sie die entsprechenden Ereignisse auf der Self-Service-Suchseite anzeigen und nach Problemen bei der Datenübertragung suchen.

> **Hinweis**
>
> Derzeit ist die Self-Service-Suche nur für die Datenquellen Access, Content Collaboration und Apps and Desktop verfügbar.

Weitere Informationen finden Sie unter Aktivieren von Analytics auf Citrix Datenquellen.

Behobene Probleme

- Für die Access Control-Datenquelle stimmt die Anzahl der Ereignisse auf der Sitekarte nicht mit den Self-Service-Suchergebnissen überein. [CAS-18286]

19. Juni 2019

Behobene Probleme

- Auf der Seite "**Audit-Log** "wird der Status der Datenübertragung ein- oder ausgeschaltet jedes Mal angezeigt, wenn die Active Directory-Datenquelle erkannt wird. [CAS-17575]

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Das Zeitraummenü im **Benutzer-Dashboard** wird nicht genau geladen. Es zeigt eine Timeout-Fehlermeldung an. [CAS-19467]
- Benutzer erhalten eine Fehlermeldung in Citrix Analytics, während sie von Splunk aus eine Verbindung zu einem Mandanten herstellen. Gelegentlich schlägt das Onboarding neuer Datenquellen fehl. [CAS-19429]

17. Juni 2019

Neue Features

Konfigurieren in StoreFront

Wenn Ihre Organisation on-premises StoreFront verwendet, können Sie StoreFront jetzt so konfigurieren, dass eine Verbindung mit Citrix Analytics hergestellt wird. Die Konfiguration erfolgt mithilfe einer aus Citrix Analytics importierten Konfigurationsdatei. Nach erfolgreicher Konfiguration sendet die Citrix Workspace-App Benutzerereignisse an Citrix Analytics, um umsetzbare Einblicke in das Benutzerverhalten zu generieren. Die Erkenntnisse helfen Ihnen dabei, anomales Benutzerverhalten zu erkennen und proaktiv mit Sicherheitsbedrohungen in Ihrem Unternehmen umzugehen. Weitere Informationen finden Sie unter Onboarding von Citrix Virtual Apps and Desktops on-premises Sites mithilfe von StoreFront.

30. Mai 2019

Neue Features

Übermäßige Anmeldefehler

Citrix Analytics erkennt Zugriffsbedrohungen basierend auf übermäßiger Anmeldeaktivität und löst den Risikoindikator für übermäßige Anmeldefehler aus. Dieser Risikoindikator wird ausgelöst, wenn ein Benutzer mehrere fehlgeschlagene Anmeldeversuche aufnimmt, auf Content Collaboration zuzugreifen. Durch die Identifizierung von Benutzern mit übermäßigen Anmeldefehlern, basierend auf dem vorherigen Verhalten, können Administratoren das Benutzerkonto auf Brute-Force-Angriffe überwachen.

> **Hinweis**
>
> **Übermäßige Anmeldefehler** werden jetzt in **übermäßige Authentifizierungsfehler umbenannt**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Behobene Probleme

- Bei einigen Benutzerereignissen, die von Citrix Workspace-Apps übertragen werden, wird die Datenquelle fälschlicherweise als Endpoint Management anstelle von Citrix Virtual Apps and Desktops identifiziert.

  [CAS-17323]

- Das Laden des **Benutzer-Dashboards** für den Zeitraum des **letzten 1 Monats** dauert lange. Dieses Problem tritt auf, wenn die Anzahl der Benutzer hoch ist. In einigen Fällen können sogar 601-Fehler auftreten.

  [CAS-16300]

- Citrix Content Collaboration wird nicht als Datenquelle erkannt, obwohl einige Benutzer den Dienst in Citrix Cloud abonnieren.

  [CAS-16299]

09. Mai 2019

Neue Features

Erstellen von benutzerdefinierten Berichten

Sie können jetzt benutzerdefinierte Berichte basierend auf Ihren betrieblichen Anforderungen erstellen. Citrix Analytics bietet eine Liste von Dimensionen und Metriken gemäß der ausgewählten Datenquelle. Wählen Sie die erforderlichen Parameter und die Visualisierungstypen wie Balkendiagramm, Ereignisdiagramm, Liniendiagramm oder Tabelle aus, um Ihre Berichte zu erstellen. Durch das Erstellen von Berichten können Sie Ihre Daten grafisch organisieren und analysieren.

Um einen benutzerdefinierten Bericht zu erstellen, klicken Sie auf der Registerkarte **Sicherheit** auf **Berichte** > **Bericht erstellen**. Um Ihre zuvor erstellten Berichte anzuzeigen, klicken Sie auf der Registerkarte **Sicherheit** auf **Berichte**. Weitere Informationen finden Sie unter Benutzerdefinierte Berichte.

Privilegierte Benutzerüberwachung

Mit Citrix Analytics können Sie die Verhaltensanomalien privilegierter Benutzer in einer Organisation genau überwachen. Da privilegierte Benutzer sehr anfällig für Sicherheitsbedrohungen sind, wird es schwierig, ihre täglichen Aktivitäten von den böswilligen zu unterscheiden. Daher bleiben die böswilligen Aktivitäten privilegierter Benutzer lange unentdeckt. Mit dieser Funktion können Sie solche Aktivitäten proaktiv überwachen und geeignete Maßnahmen für die entsprechenden Benutzerkonten ergreifen. Privilegierte Benutzer werden durch ein Symbol im **Benutzer-Dashboard** dargestellt.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Citrix Analytics unterstützt die Überwachung für die folgenden Arten von privilegierten Benutzern:

- **Administratoren** - Benutzer, denen vom jeweiligen Citrix Dienst Administratorrechte zugewiesen wurden. Derzeit unterstützt Citrix Analytics die privilegierte Benutzerüberwachung für Benutzer mit Administratorrechten im Content Collaboration Service.
- **Führungskräfte** - In Citrix Analytics können Sie eine AD-Gruppe als Führungskräftegruppe markieren. Durch das Markieren einer AD-Gruppe als Führungsgruppe werden alle Benutzer in der Gruppe zu privilegierten Benutzern. Wenn die Verhaltensanomalien von Benutzern in einer AD-Gruppe nicht weiter unterstützt werden müssen, können Sie die Gruppe als Führungsgruppe entfernen.

Weitere Informationen finden Sie unter Privilegierte Benutzer.

Wöchentliche E-Mail-Zusammenfassung

Citrix Analytics sendet wöchentlich eine E-Mail an die Administratoren, in der die Sicherheitsrisikorisiken in der IT-Umgebung ihres Unternehmens zusammengefasst werden. Die E-Mail-Benachrichtigung wird jeden Dienstag an die Administratoren gesendet und zeigt die Sicherheitsereignisse, die in der vergangenen Woche aufgetreten sind. Diese E-Mail stellt sicher, dass die Administratoren über die Sicherheitsrisiken informiert werden, ohne sich bei Citrix Analytics anzumelden. Weitere Informationen finden Sie unter Wöchentliche E-Mail-Zusammenfassung.

26. April 2019

Neue Features

Delegierte Administratoren

Citrix Analytics unterstützt jetzt delegierte Administratorrollen. Mit dieser Funktion können Sie andere Administratoren zu Ihrem Citrix Cloud-Konto einladen, um Citrix Analytics für Ihre Organisation zu verwalten. Wenn Sie ein Citrix Analytics-Administrator mit voller Zugriffsberechtigung sind, können Sie Ihrem Citrix Cloud-Konto weitere Administratoren hinzufügen. Diese zusätzlichen Administratoren werden als delegierte Administratoren bezeichnet. Derzeit können Sie den delegierten Administratoren schreibgeschützten Zugriff zuweisen. Weitere Informationen finden Sie unter Delegierte Administratoren.

Behobene Probleme

Nur wenige Risikoindikatoren für die Datenquellen, die Datenstreaming verwenden, erzeugen keine Warnungen. Sie erhalten keine Warnbenachrichtigungen und richtlinienbasierte Aktionen werden

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

nicht automatisch angewendet, wenn einer der folgenden Risikoindikatoren ausgelöst wird:

- **Citrix Endpoint Management-Risikoindikatoren** - Nicht verwaltetes Gerät, Gerät mit Jailbreak oder Root und Gerät mit Apps auf der Sperrliste.
- **Citrix Virtual Apps and Desktops Risikoindikator** - Zugriff von einem Gerät mit nicht unterstütztem Betriebssystem (OS).
- **Citrix Content Collaboration Risikoindikator** - Übermäßiger Zugriff auf vertrauliche Dateien

[CAS-14590]

19. Februar 2019

Neue Features

Splunk-Integration

Citrix Analytics ist in Splunk integriert, um die Überwachung und Fehlerbehebung von Sicherheitsvorfällen zu verbessern. Diese Integration erweitert Ihre vorhandenen Datenquellen um die Risikoanalysefunktionen und Intelligenz von Citrix Analytics for Security wie Risikoindikatoren, Risikobewertungen und Benutzerprofile. Citrix Analytics exportiert Informationen zur Risikoanalyse in einen Kanal. Splunk zieht dasselbe von diesem Kanal.

Die Splunk-Integration umfasst die Konfiguration in Citrix Analytics, die Installation des **Citrix Analytics Add-ons für Splunk-App** und die Konfiguration der App. Stellen Sie sicher, dass Sie die Datenverarbeitung für mindestens eine Datenquelle aktivieren. Es hilft Citrix Analytics, den Splunk-Integrationsprozess zu beginnen.

Weitere Informationen finden Sie unter Splunk-Integration.

Dynamische Sitzungsaufzeichnung Citrix Analytics bietet die Möglichkeit, die Sitzungsaufzeichnung dynamisch für die aktuellen Virtual Apps and Desktops-Sitzungen der Benutzer auszulösen. Es hilft, Beweise zu erfassen, die für die Risikoanalyse erforderlich sind, und geeignete Maßnahmen zur Reaktion auf Vorfälle wie Trennen von Sitzungen und Blockieren von Benutzern zu ergreifen.

Weitere Informationen finden Sie unter Richtlinien und Aktionen.

Dashboard für Links teilen und Risikoindikator Citrix Analytics führt die Risikosichtbarkeit für Share-Links basierend auf Daten ein, die von Citrix Content Collaboration gesammelt wurden. Es hilft Ihnen, das Risiko von Freigabelinks anhand der Risikoindikatoren zu verstehen, die die Freigabelinks auslösen.

Weitere Informationen finden Sie unter Dashboard für Freigabelinks.

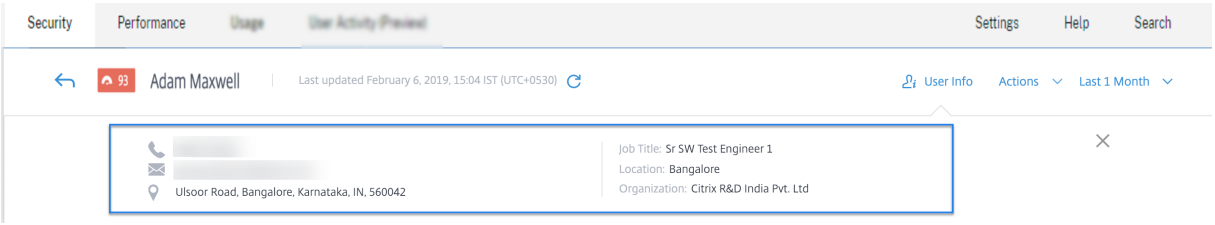
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Derzeit wird der Risikoindikator für anonyme sensible Freigaben für einen Freigabelink ausgelöst. Wenn Content Collaboration dieses riskante Verhalten erkennt, empfängt Citrix Analytics die Ereignisse. Sie werden im Warnmeldungsfenster **benachrichtigt** und der Risikoindikator für anonyme vertrauliche Freigaben wird zur Risikozeitleiste des Freigabelinks hinzugefügt.

Weitere Informationen finden Sie unter Share-Link-Risikozeitplan und Citrix Share Link-Risikoindikatoren.

Microsoft Active Directory-Integration Sie können jetzt Microsoft Active Directory in Citrix Analytics integrieren. Diese Integration erweitert den Kontext riskanter Benutzer mit zusätzlichen Informationen wie Berufsbezeichnung, Organisation, Bürostandort, E-Mail und Kontaktdaten. Sie können eine bessere Sichtbarkeit eines Benutzers auf der Benutzerprofilseite in Citrix Analytics erhalten.

Weitere Informationen finden Sie unter Integrieren von Analytics in Microsoft Active Directory.



04. Januar 2019

Neue Features

Hinzufügen der Spalte SOURCE für bestehende Risikoindikatoren Die Spalte **QUELLE** wurde im Abschnitt **EREIGNISDETAILS** für die folgenden Risikoindikatoren eingeführt:

- Übermäßige Dateiuploads
- Übermäßige Dateidownloads
- Übermäßige Dateifreigabe
- Übermäßiges Löschen von Dateien oder Ordnern

Weitere Informationen finden Sie unter Risikoindikatoren für Citrix Content Collaboration.

Erweitertes Benutzerprofil Die Ansicht **Benutzerinformationen** im Benutzerprofil wurde erweitert. Der Link **Trend View** wurde oben rechts in den Abschnitten **Anwendung**, **Geräte**und **Datennutzung** eingeführt. Der Link **Kartenansicht** wurde oben rechts im Abschnitt **Standorte** eingeführt. Diese Links bieten eine grafische Darstellung des historischen Verhaltens des Benutzers während eines bestimmten Zeitraums. Sie können in der Risikozeitleiste des Benutzers oder auf der Seite **Datenquellen** zu **Benutzerinformationen** navigieren.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Hinweis**
>
> Die **Authentifizierungs-** und **Domänendaten** sind derzeit nicht im Benutzerinformationsprofil verfügbar.

Weitere Informationen finden Sie unter Zeitleiste und Profil des Benutzerrisikos.

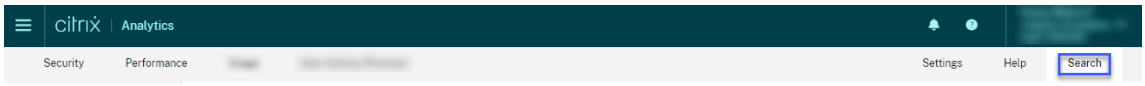
Microsoft Graph Sicherheitsrisikoindikatoren Das eingebundene Microsoft Graph Security kann Details zu Risikoindikatoren von einem der folgenden Sicherheitsanbieter erhalten und an Citrix Analytics weitergeben:

- Azure AD-Identitätsschutz
- Microsoft Defender für Endpoint

Weitere Informationen finden Sie unter Microsoft Graph Sicherheitsrisikoindikatoren.

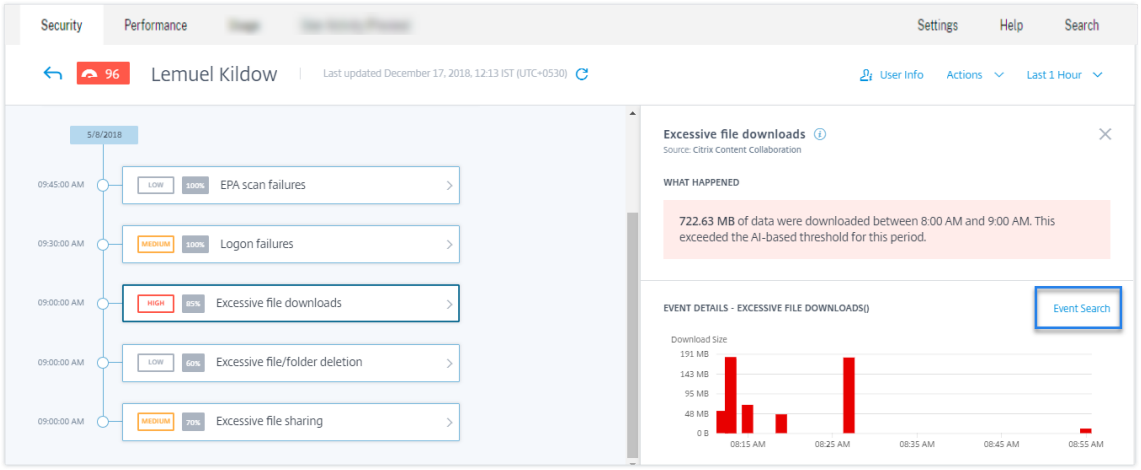
Möglichkeiten, die Self-Service-Suchseite aufzurufen Sie können jetzt mit den folgenden Optionen auf die Self-Service-Suchseite zugreifen:

- **Obere Leiste**: Klicken Sie in der oberen Leiste auf **Suchen**, um direkt auf die Suchseite zuzugreifen.



- **Risikozeitleiste auf der Benutzerprofilseite**: Klicken Sie auf **Ereignissuche**, um auf die Suchseite zuzugreifen und die Ereignisse anzuzeigen, die dem Risikoindikator eines bestimmten Benutzers und der Datenquelle entsprechen. Weitere Informationen finden Sie unter Self-Service-Suche.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Self-Service-Suche für Content Collaboration Verwenden Sie die Self-Service-Suche, um einen Einblick in die mit der Datenquelle Content Collaboration verbundenen Ereignisse zu Um die Ereignisse anzuzeigen, wählen Sie in der Liste **Content Collaboration** aus, wählen Sie den Zeitraum aus und klicken Sie dann auf **Suchen**.
Weitere Informationen finden Sie unter Self-Service-Suche für Content Collaboration.

Self-Service-Suche für Apps und Desktops Verwenden Sie die Self-Service-Suche, um einen Einblick in die Ereignisse zu erhalten, die mit der Datenquelle Apps und Desktops verknüpft sind. Um die Ereignisse anzuzeigen, wählen Sie **Apps und Desktops** aus der Liste aus, wählen Sie den Zeitraum aus und klicken Sie dann auf **Suchen**. Weitere Informationen finden Sie unter Self-Service-Suche nach Apps und Desktops.

Self-Service-Suchereignisse in CSV-Datei exportieren Sie können jetzt die Self-Service-Suchereignisse in eine CSV-Datei exportieren und die Datei zur zukünftigen Verwendung herunterladen. Weitere Informationen finden Sie unter Self-Service-Suche.

Verbessertes Onboarding für Citrix Virtual Apps and Desktops Der Onboarding-Prozess für die Citrix Virtual Apps and Desktops-Datenquelle wurde jetzt verbessert, um eine bessere Benutzererfahrung zu bieten. Die Site-Karten und die Schritte beim Einsteigen wurden geändert. Weitere Informationen finden Sie unter Citrix Virtual Apps and Desktops und Citrix DaaS-Datenquelle.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

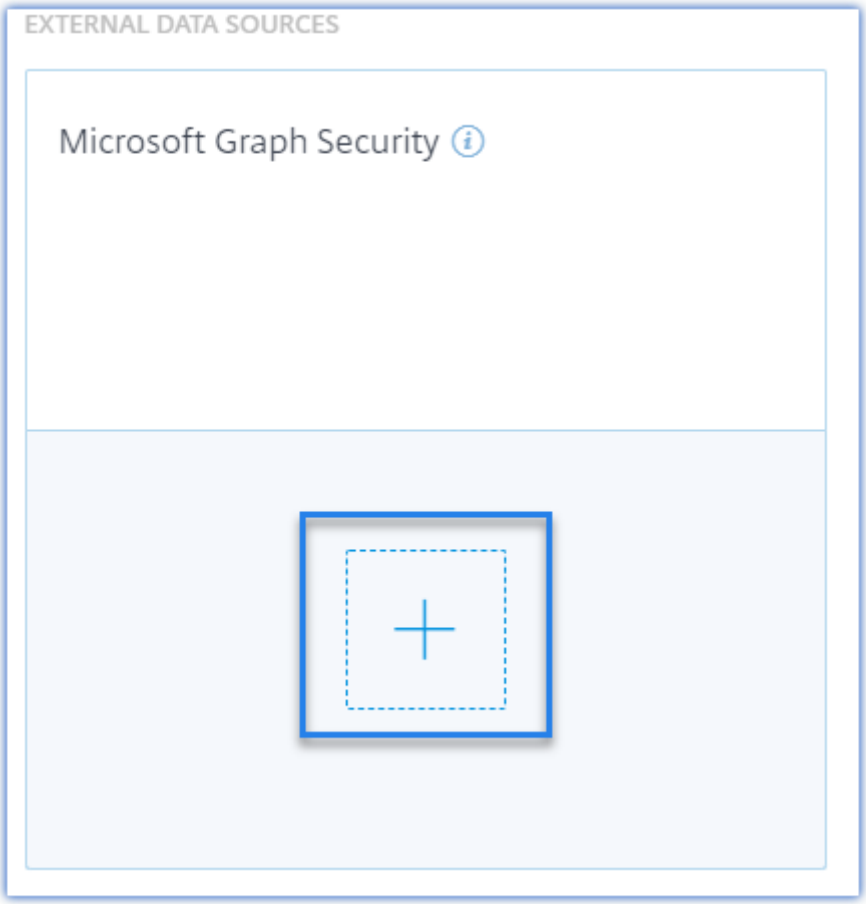
29. November 2018

Neue Features

Microsoft Security Graph-Datenquelle Microsoft Graph Security ist eine externe Datenquelle, die Daten von mehreren Sicherheitsanbietern aggregiert. Es bietet auch Zugriff auf die Benutzerinventardaten.

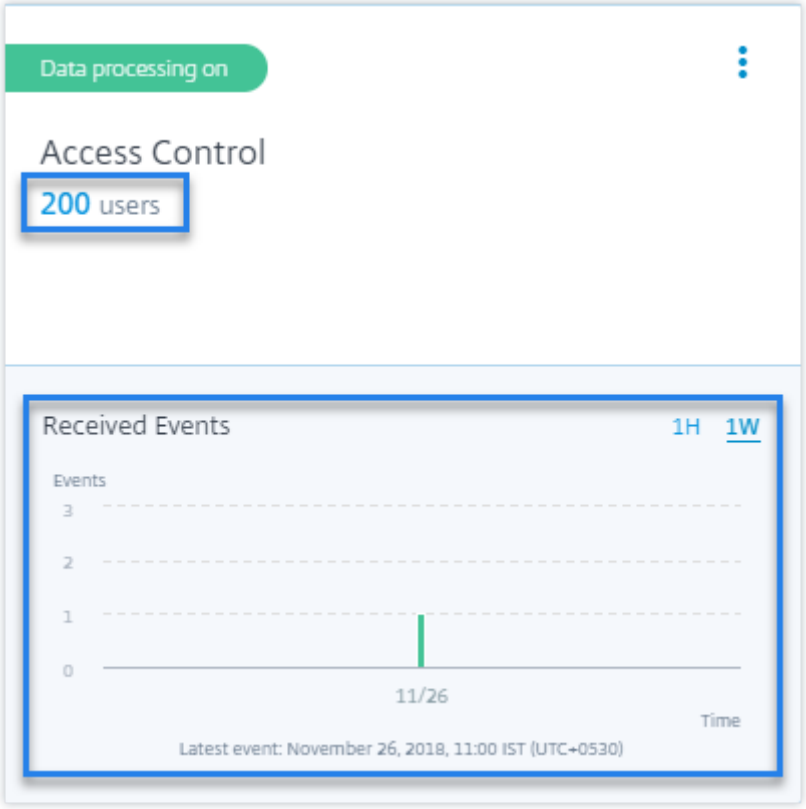
Citrix Analytics unterstützt derzeit den **Azure AD-Identitätsschutz** und **Microsoft Defender für Endpunkt-Sicherheitsanbieter**, die mit dieser Datenquelle verknüpft sind.

Um diese Datenquelle einzubauen, müssen Sie Berechtigungen von der Microsoft-Identitätsplattform erhalten. Weitere Informationen finden Sie unter Microsoft Graph-Sicherheit.



Anzeigen von Ereignisdetails und entdeckten Benutzern auf den Site-Karten für Datenquellen Die Site-Karten für die Datenquellen zeigen jetzt Ereignisdetails und die Anzahl der Benutzer an. Beispielsweise können Sie die Ereignisdetails und die Benutzer für Access Control auf der Sitekarte anzeigen. Weitere Informationen finden Sie unter Analytics für Datenquellen aktivieren.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



16. November 2018

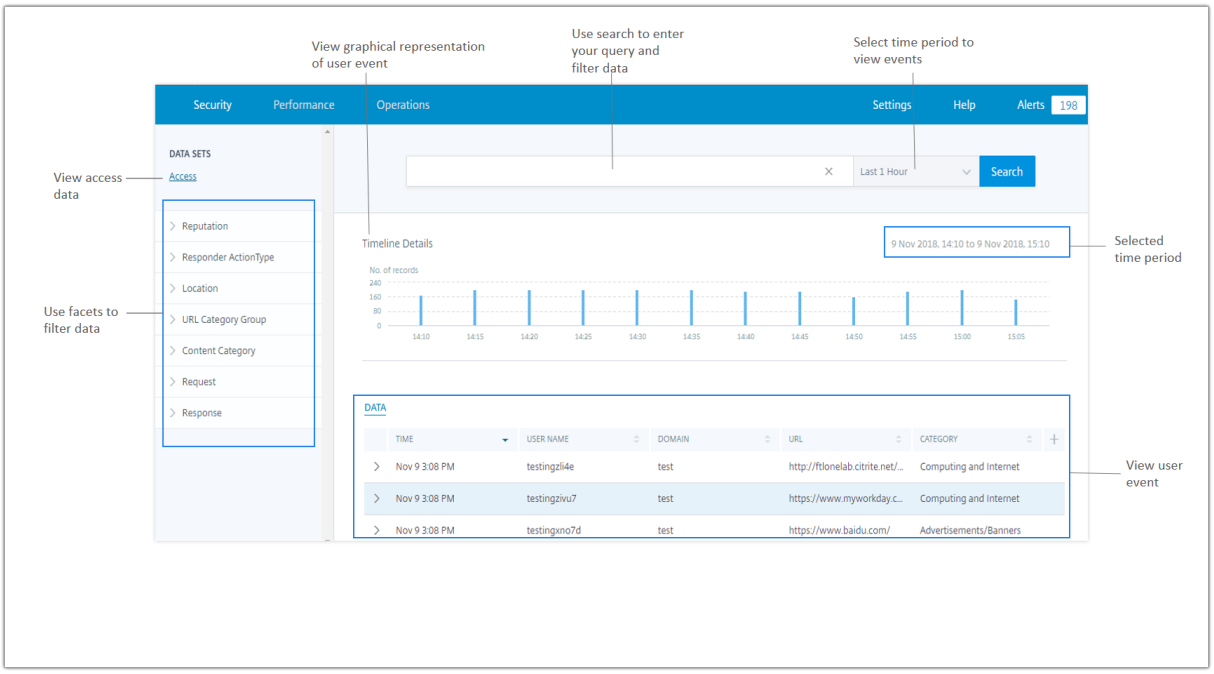
Neue Features

Self-Service-Suche nach Zugangsdaten Sie können die Self-Service-Suche verwenden, um Einblicke in die Zugriffsdetails für die Benutzer in Ihrem Unternehmen zu erhalten. Citrix Analytics sammelt die Zugriffsdetails der Benutzer vom Citrix Access Control-Dienst. Verwenden Sie die Facetten und die Suchabfrage, um Ihre Suchergebnisse einzuschränken.

Um die Self-Service-Suchseite zu verwenden, klicken Sie auf der Registerkarte **Sicherheit** auf **Ereignissuche**.

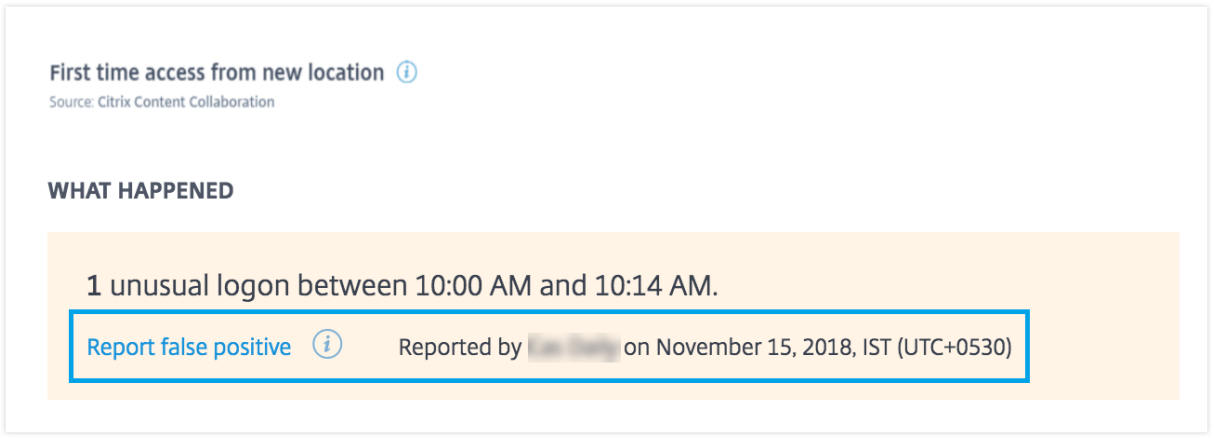
Weitere Informationen finden Sie unter Self-Service-Suche nach Access.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Risikoindikator-Feedback Mithilfe der Feedback-Funktion für Risikoindikatoren in Citrix Analytics können Sie Feedback zu einem Risikoindikator geben. Ihr Feedback hilft zu bestätigen, ob der gemeldete Sicherheitsvorfall korrekt ist oder nicht.

Derzeit wird diese Funktion für den Risikoindikator für **ungewöhnlichen Anmeldezugriff** unterstützt, der von der Datenquelle Content Collaboration ausgelöst wird. Wenn dieser ausgelöste Risikoindikator falsch ist, können Sie ihn als falsch positiv melden und Feedback geben. Sie können auch Feedback bearbeiten, das Sie zuvor abgegeben haben. Citrix Analytics erfasst Ihr Feedback und validiert die prognostizierten Informationen, um die Erkennung von anomalen Verhaltensweisen zu optimieren.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Behobene Probleme

- Sie können eine Richtlinie nicht bearbeiten und speichern, wenn Sie mit Internet Explorer 11.0 auf Citrix Analytics zugreifen.

Bekannte Probleme

December 12, 2023

Für Citrix Analytics for Security sind die folgenden Probleme bekannt:

- Die Citrix Workspace-App für Linux sendet keine Druckereignisse an Citrix Analytics, wenn Apps und Desktops über einen Webbrowser geöffnet und von ICA auf dem nativen Client gestartet werden. [CAS-36238]

  > **Hinweis**
  >
  > Weitere Informationen zu den Lebenszyklusdaten und Lebenszyklusphasen (Allgemeine Verfügbarkeit, Ende der Wartung und End of Life) der Citrix Workspace-App und Citrix Receiver auf allen Plattformen finden Sie unter Lebenszyklusmeilensteine für die Citrix Workspace-App und Citrix Receiver.

Citrix Analytics-Angebote

December 12, 2023

Citrix Analytics für Sicherheit

Sortiert und bietet Einblick in das Benutzer- und Anwendungsverhalten, das aus den verbundenen Datenquellen der Kunden wie Secure Private Access, Citrix Virtual Apps and Desktops, Citrix DaaS Site oder NetScaler Gateway erfasst wurde. Sie können jeden Aspekt des Verhaltens verfolgen und mithilfe fortschrittlicher Algorithmen für maschinelles Lernen zwischen normalem Verhalten und böswilligen Angreifern unterscheiden. Auf diese Weise können Sie interne und externe Bedrohungen proaktiv identifizieren und verwalten.

Erfahren Sie mehr: Citrix Analytics for Security

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Citrix Analytics für Leistung

Bietet ganzheitliche End-to-End-Sichtbarkeit für Hybridbereitstellungen von Citrix Virtual Apps and Desktops und Citrix DaaS-Sites. Die Leistung wird durch den User Experience Score angegeben, der historische Faktoren und Kennzahlen quantifiziert, die die Benutzererfahrung bei der Verwendung einer von Citrix bereitgestellten veröffentlichten Anwendung, eines veröffentlichten Desktops oder eines Remote-PCs definieren.

Erfahren Sie mehr: Citrix Analytics for Performance

Citrix Analytics —Nutzung (Ende des Lebenszyklus)

> **Hinweis**
>
> **Achtung**: Citrix Usage Analytics hat das Ende seiner Lebensdauer erreicht und steht Benutzern nicht mehr zur Verfügung.

Datenquellen

April 12, 2024

Datenquellen sind die Cloud-Dienste und die on-premises Produkte, die Daten an Citrix Analytics senden.

Citrix Datenquellen

In der folgenden Tabelle sind verschiedene Citrix Datenquellen aufgeführt, die von Citrix Analytics for Security unterstützt werden. Weitere Informationen finden Sie unter Erste Schritte.

Datenquelle	Bereitstellungstyp	Erforderliche Vertreter	Produkt Komponente und Version
Citrix Endpoint Management	Service	–	Citrix Endpoint Management
Gateway	On-Premises	Application Delivery Management-Agent	Citrix Gateway 12.0.56.16 oder höher
Citrix Identitätsanbieter	Service	–	Citrix Identitäts- und Zugriffsmanagement

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Datenquelle	Bereitstellungstyp	Erforderliche Vertreter	Produkt Komponente und Version
Citrix Secure Private Access	Service	(Nicht zutreffend)	Citrix Secure Private Access
Citrix Remote Browser Isolation	Service	–	Citrix Remote Browser Isolation
Citrix DaaS (früher Virtual Apps and Desktops Service)	Service	–	Citrix Workspace-App für Windows 1907 oder höher, Citrix Workspace-App für Mac 1910.2 oder höher, Citrix Workspace-App für HTML5 2007 oder höher, Citrix Workspace-App für Chrome-Neueste Version verfügbar im Chrome Web Store, Citrix Workspace-App für Android - neueste Version verfügbar in Google Play, Citrix Workspace-App für iOS —neueste Version verfügbar im Apple App Store, Citrix Workspace-App für Linux 2006 oder höher
Citrix Virtual Apps and Desktops	On-Premises	Agent für Virtual Apps and Desktops	Citrix Virtual Apps and Desktops 7 1808, Citrix XenApp und XenDesktop 7.16 und höher

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Datenquelle	Bereitstellungstyp	Erforderliche Vertreter	Produkt Komponente und Version
		Agent ist für erweiterte Funktionen wie Aktionen erforderlich.	Citrix Workspace-App für Windows 1907 oder höher, Citrix Workspace-App für Mac 1910.2 oder höher, Citrix Workspace-App für HTML5 2007 oder höher, Citrix Workspace-App für Chrome-Neueste Version verfügbar im Chrome Web Store, Citrix Workspace-App für Android - neueste Version verfügbar in Google Play, Citrix Workspace-App für iOS —neueste Version verfügbar im Apple App Store, Citrix Workspace-App für Linux 2006 oder höher Citrix Director 7.16 oder höher **Für Arbeitsbereich-benutzer**: Virtual Apps and Desktops on-premises Sites müssen mithilfe der Site-Aggregation zum Workspace hinzugefügt werden.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Datenquelle	Bereitstellungstyp	Erforderliche Vertreter	Produkt Komponente und Version
			Für StoreFront-Benutzer: StoreFront Bereitstellungsversion muss StoreFront 1906 oder höher sein. Auf StoreFront muss über einen der Clients zugegriffen werden: Citrix Receiver für Websites in HTML5-kompatiblen Browsern, Citrix Workspace-App 1907 für Windows oder höher, Citrix Workspace-App 2006 für Linux oder höher, Citrix Workspace-App 2006 für Mac oder höher. **LTSR-Unterstützung**: Für Citrix Virtual Apps and Desktops 7 1912 LTSR ist die unterstützte StoreFront-Version 1912.

> **Hinweis**
>
> Wenden Sie sich an die Citrix Cloud-Dienste, um mehr über die Citrix Produkte und deren Abonnements zu erfahren.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Externe Datenquellen

In der folgenden Tabelle sind die externen Datenquellen (Produkte von Drittanbietern) aufgeführt, die von Citrix Analytics for Security unterstützt werden.

Datenquelle	Bereitstellungstyp	Erforderliche Vertreter
Microsoft Graph Security	Service	–
Microsoft Active Directory	On-Premises	Citrix Cloud Connector

Unterstützte Heimatregionen

Citrix Analytics for Security wird in den folgenden Home-Regionen unterstützt:

- Vereinigte Staaten (US)
- Europäische Union (EU)
- Asien-Pazifik Süd (APS)

Je nach Standort Ihrer Organisation können Sie sich in einer der Heimatregionen bei Citrix Cloud einbinden.

Wenn Ihr Unternehmen in einer Heimatregion, in der eine Datenquelle nicht unterstützt wird, in Citrix Cloud integriert ist, erhalten Sie keine Benutzerereignisse von der Datenquelle.

Verwenden Sie die folgende Tabelle, um die Datenquellen und die Regionen anzuzeigen, in denen sie unterstützt werden.

Datenquelle	Unterstützt in der US-Region	Unterstützt in der EU-Region	In der APS-Region unterstützt
Citrix Endpoint Management	Ja	Ja	Ja
Citrix Gateway (on-premises)	Ja	Ja	Ja
Citrix Identitätsanbieter	Ja	Ja	Ja
Citrix Secure Private Access	Ja	Ja	Ja
Citrix Remote Browser Isolation	Ja	Ja	Ja

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Datenquelle	Unterstützt in der US-Region	Unterstützt in der EU-Region	In der APS-Region unterstützt
Citrix DaaS (früher Citrix Virtual Apps and Desktops Service)	Ja	Ja	Ja
Citrix Virtual Apps and Desktops on-premises	Ja	Ja	Ja
Microsoft Active Directory	Ja	Ja	Ja
Microsoft Graph Security	Ja	Ja	Ja

Versionsmatrix der Citrix Workspace-App

In diesem Abschnitt werden die unterstützten Versionen der Citrix Workspace-App angezeigt, die alle Telemetriedaten sendet und alle erforderlichen kritischen Bugfixes enthält.

In der folgenden Tabelle sind die unterstützten und nicht unterstützten Versionen der Citrix Workspace-App aufgeführt.

Plattform	Unterstützte Version
Windows	Alle LTSR 2203-Veröffentlichungen nach CU3 23.0.3.0 oder höher
HTML5	21.5.0.0 oder höher
Macintosh	21.0.4.0 oder höher
Linux	21.4.0.0 oder höher
Chrome	21.5.0.0 oder höher
iOS	21.4.0.0 oder höher
Android	21.5.0.0 oder höher

In der folgenden Tabelle ist die Mindestversion der Citrix Workspace-App aufgeführt, die erforderlich ist, damit das Betriebssystem die folgenden Benutzerereignisattribute in Citrix Analytics for Security erhält.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Event Attribute	Verbundene Funktionen	Windows	Mac	Linux	HTML5	Chrome	iOS	Android
Stadt, Land	Standort der Zugriffssicherung, Self-Service-Suche—Apps und Desktops	2008 oder höher	2006 oder höher	2104 oder höher	2007 oder höher	Neueste Version im Chrome Web Store verfügbar	Neueste Version im Apple App Store verfügbar	Neueste Version in Google Play verfügbar
Client-IP	Self-Service-Suche—Apps und Desktops	2008 oder höher	2006 oder höher	2104 oder höher	2007 oder höher	Neueste Version im Chrome Web Store verfügbar	Neueste Version im Apple App Store verfügbar	Neueste Version in Google Play verfügbar
Betriebssystem, Betriebssystemversion, zusätzliche Informationen zum Betriebssystem	Self-Service-Suche—Apps und Desktops	2109 oder höher	2108 oder höher	2104 oder höher	2007 oder höher	Neueste Version im Chrome Web Store verfügbar	Neueste Version im Apple App Store verfügbar	Neueste Version in Google Play verfügbar

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Event Attribute	Verbundene Funktionen	Windows	Mac	Linux	HTML5	Chrome	iOS	Android
Name des Druckers	Self-Service-Suche—Apps und Desktops	2106 oder höher	1809 oder höher	2006 oder höher	1911 oder höher	Neueste Version im Chrome Web Store verfügbar	Neueste Version im Apple App Store verfügbar	Neueste Version in Google Play verfügbar
Alle Benutzerereignisse für den Webstart	Self-Service-Suche—Apps und Desktops	2008 oder höher	2006 oder höher	2006 oder höher	Nicht zutreffend	Nicht unterstützt	Neueste Version im Apple App Store verfügbar	Neueste Version in Google Play verfügbar

Data Governance

December 12, 2023

Dieser Abschnitt enthält Informationen zur Erfassung, Speicherung und Aufbewahrung von Protokollen durch den Citrix Analytics Service. Alle großgeschriebenen Begriffe, die nicht im Abschnitt Definitionen definiert sind, haben die in der Citrix Endbenutzer-Dienstleistungsvereinbarungangegebene Bedeutung.

Citrix Analytics wurde entwickelt, um Kunden Einblick in Aktivitäten in ihrer Citrix Computerumgebung zu bieten. Citrix Analytics ermöglicht es Sicherheitsadministratoren, die Protokolle auszuwählen, die sie überwachen möchten, und basierend auf der protokollierten Aktivität gezielte Maßnahmen zu ergreifen. Diese Erkenntnisse helfen Sicherheitsadministratoren, den Zugriff auf ihre Computerumgebungen zu verwalten und Kundeninhalte in der Computerumgebung des Kunden zu schützen.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Datenresidenz

Citrix Analytics-Protokolle werden getrennt von den Datenquellen verwaltet und in mehreren Microsoft Azure Cloud-Umgebungen zusammengefasst, die sich in den USA, der Europäischen Union und dem asiatisch-pazifischen Süden befinden. Die Speicherung der Protokolle hängt von der Heimatregion ab, die von den Citrix Cloud-Administratoren beim Onboarding ihrer Organisationen in Citrix Cloud ausgewählt wurde. Wenn Sie beispielsweise beim Onboarding Ihres Unternehmens in Citrix Cloud die **europäische Region** auswählen, werden Citrix Analytics-Protokolle in Microsoft Azure-Umgebungen in der Europäischen Union gespeichert.

Weitere Informationen finden Sie unter Citrix Cloud Services Kundeninhalte und Protokollierung sowiegeografische Überlegungen.

Datensammlung

Citrix Cloud-Dienste sind dazu dienen, Protokolle an Citrix Analytics zu übertragen. Protokolle werden aus den folgenden Datenquellen gesammelt:

- Citrix ADC (on-premises) zusammen mit einem Abonnement für Citrix Application Delivery Management
- Citrix Endpoint Management
- NetScaler Gateway (on-premises)
- Citrix Identitätsanbieter
- Citrix Secure Browser
- Citrix Secure Private Access
- Citrix Virtual Apps and Desktops
- Citrix DaaS (früher Citrix Virtual Apps and Desktops Service)
- Microsoft Active Directory
- Microsoft Graph Security

Datenübertragung

Citrix Cloud-Protokolle werden sicher an Citrix Analytics übertragen. Wenn der Administrator der Kundenumgebung Citrix Analytics explizit aktiviert, werden diese Protokolle analysiert und in einer Kundendatenbank gespeichert. Dasselbe gilt für Citrix Virtual Apps and Desktops
Datenquellen mit konfiguriertem Citrix Workspace.

Für Citrix ADC-Datenquellen wird die Protokollübertragung nur initiiert, wenn der Administrator Citrix Analytics explizit für die bestimmte Datenquelle aktiviert.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Steuerung von Daten

An Citrix Analytics gesendete Protokolle können vom Administrator jederzeit ein- oder ausgeschaltet werden.

Wenn diese Option für on-premises Citrix ADC-Datenquellen deaktiviert ist, wird die Kommunikation zwischen der jeweiligen ADC-Datenquelle und Citrix Analytics gestoppt.

Wenn alle für andere Datenquellen deaktiviert sind, werden die Protokolle für die jeweilige Datenquelle nicht mehr analysiert und in Citrix Analytics gespeichert.

Datenaufbewahrung

Citrix Analytics-Protokolle werden in identifizierbarer Form für maximal 13 Monate oder 396 Tage aufbewahrt. Alle Protokolle und zugehörige Analysedaten wie Benutzerrisikoprofile, Details zur Bewertung des Nutzerrisikos, Details zu Benutzerrisikoereignissen, Benutzerbeobachtungsliste, Benutzeraktionen und Benutzerprofil werden für diesen Zeitraum aufbewahrt.

Wenn Sie beispielsweise Analytics für eine Datenquelle am 1. Januar 2021 aktiviert haben, werden die am 1. Januar 2021 gesammelten Daten standardmäßig bis zum 31. Januar 2022 in Citrix Analytics aufbewahrt. In ähnlicher Weise werden die am 15. Januar 2021 gesammelten Daten bis zum 15. Februar 2022 usw. aufbewahrt.

Diese Daten werden für den Standarddatenaufbewahrungszeitraum gespeichert, auch wenn Sie die Datenverarbeitung für die Datenquelle deaktiviert oder die Datenquelle aus Citrix Analytics entfernt haben.

Citrix Analytics löscht alle Kundeninhalte 90 Tage nach Ablauf des Abonnements oder des Testzeitraums.

Datenexport

In diesem Abschnitt werden die aus Citrix Analytics for Security und Citrix Analytics for Performance exportierten Daten erläutert.

Citrix Analytics for Performance sammelt und analysiert Leistungsmetriken aus den Datenquellen.

Sie können die Daten von der Self-Service-Suchseite als CSV-Datei herunterladen.

Citrix Analytics for Security sammelt Benutzerereignisse aus verschiedenen Produkten (Datenquellen). Diese Ereignisse werden verarbeitet, um Einblick in das riskante und ungewöhnliche Verhalten der Benutzer zu erhalten. Sie können diese verarbeiteten Daten in Bezug auf Risikoeinblicke der Benutzer und Benutzerereignisse in Ihren Service System Information and Event Management (SIEM) exportieren.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Derzeit können die Daten auf zwei Arten aus Citrix Analytics for Security exportiert werden:

- Integrieren von Citrix Analytics for Security in Ihren SIEM-Dienst
- Herunterladen der Daten von der Self-Service-Suchseite als CSV-Datei.

Wenn Sie Citrix Analytics for Security in Ihren SIEM-Dienst integrieren, werden die Daten entweder mithilfe des nach Norden gebundenen Kafka-Themas oder eines LogStash-basierten Datenconnectors an Ihren SIEM-Dienst gesendet.

Derzeit können Sie in die folgenden SIEM-Dienste integrieren:

- Splunk (durch Herstellen einer Verbindung über das Citrix Analytics-Add-on)
- Jeder SIEM-Dienst, der Kafka-Thema oder LogStash-basierte Datenconnectors wie Elasticsearch und Microsoft Azure Sentinel unterstützt

Sie können die Daten auch mithilfe einer CSV-Datei in Ihren SIEM-Dienst exportieren. Auf der Self-Service-Suchseite können Sie die Daten (Benutzerereignisse) für eine Datenquelle anzeigen und diese Daten als CSV-Datei herunterladen. Weitere Informationen zur CSV-Datei finden Sie unter Self-Service-Suche.

> **Wichtig**
>
> Nachdem die Daten in Ihren SIEM-Dienst exportiert wurden, ist Citrix nicht für die Sicherheit, Speicherung, Verwaltung und Verwendung der exportierten Daten in Ihrer SIEM-Umgebung verantwortlich.

Sie können die Datenübertragung von Citrix Analytics for Security zu Ihrem SIEM-Dienst ein- oder ausschalten.

Informationen zu den verarbeiteten Daten und der SIEM-Integration finden Sie unter Integration von Sicherheitsinformationen und Ereignismanagement (SIEM) und Citrix Analytics-Datenformat für SIEM.

Anlage zur Sicherheit von Citrix Diensten

Detaillierte Informationen zu den auf Citrix Analytics angewendeten Sicherheitskontrollen, einschließlich Zugriff und Authentifizierung, Sicherheitsprogramm-Management, Business Continuity und Incident-Management, sind in der Citrix Services Security Exhibit enthalten.

Definitionen

Kundeninhalte sind alle Daten, die zur Speicherung in ein Kundenkonto hochgeladen werden, oder Daten in einer Kundenumgebung, auf die Citrix Zugriff zur Erbringung von Diensten erhält.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Protokoll bezeichnet eine Aufzeichnung von Ereignissen mit Bezug zu den Services, darunter Messdaten zu Leistung, Stabilität, Nutzung, Sicherheit und Unterstützung.

Dienste bezeichnet die oben beschriebenen Citrix Cloud Services für die Zwecke von Citrix Analytics.

Datenerfassungsvertrag

Durch das Hochladen Ihrer Daten in Citrix Analytics und die Nutzung der Funktionen von Citrix Analytics erklären Sie sich damit einverstanden, dass Citrix technische, Benutzer- oder verwandte Informationen über Ihre Citrix Produkte und Dienstleistungen sammelt, speichert, überträgt, pflegt, verarbeitet und verwendet.

Citrix behandelt die empfangenen Informationen immer gemäß der Citrix Datenschutzrichtlinie.

Anhang: gesammelte Protokolle

- Citrix Analytics für Sicherheitsprotokolle
- Citrix Analytics for Performance Leistungsprotokolle

Citrix Analytics für Sicherheitsprotokolle

Allgemeine Protokolle

Im Allgemeinen enthalten Citrix Analytics-Protokolle die folgenden Header-Identifikationsdatenpunkte:

- Header-Schlüssel
- Geräte-Identifikation
- Identifizierung
- IP-Adresse
- Organisation
- Produkt
- Produktversion
- System-Zeit
- Mandanten-ID
- Typ
- Benutzer: E-Mail, ID, SAM-Kontoname, Domäne, UPN
- Version

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Citrix Endpoint Management-Dienstprotokolle

Die Citrix Endpoint Management-Dienstprotokolle enthalten die folgenden Datenpunkte:

- Konformität
- Unternehmen im Besitz
- Geräte-ID
- Geräte-Modell
- Gerätetyp
- Geo Breitengrad
- Geo Längengrad
- Hostname
- IMEI
- IP-Adresse
- Jail Broken
- Letzte Aktivität
- Verwaltungsmodus
- Betriebssystem
- Betriebssystemversion
- Informationen zur Plattform
- Grund
- Seriennummer
- Betreut

Citrix Secure Private Access-Protokolle

- AAA-Benutzername
- Name der Auth Policy-Aktion
- Authentifizierungssitzung ID
- URL anfragen
- Richtlinienname der URL Kategorie
- VPN Sitzungskennung

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- VServer-IP
- AAA-Benutzer-E-Mail-ID
- Aktueller Vorlagencode
- App FQDN
- App-Name
- App Name Vserver LS
- Anwendungsflags
- Authentifizierungstyp
- Phase der Authentifizierung
- Authentifizierungsstatuscode
- Backend-Server-DST-IPv4-Adresse
- IPv4-Adresse des Backend-Servers
- IPv6-Adresse des Backend-Servers
- Kategorie Domainname
- Kategorie Domainquelle
- Client-IP
- Client MSS
- Client Fast Retx Count
- Client TCP Jitter
- Client TCP Packets Retransmited
- Client TCP RTO Count
- Client TCP Zero Window Count
- Clt Flow Flags Rx
- Clt Flow Flags Tx
- Clt TCP Flags Rx
- Clt TCP Flags Tx
- Connection Chain Hop Count
- Connection Chain ID
- Egress Interface

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Exporting Process ID
- Flow Flags Rx
- Flow Flags Tx
- HTTP Content Type
- HTTP Domain Name
- HTTP Req Authorization
- HTTP Req Cookie
- HTTP Req Forw FB
- HTTP Req Forw LB
- HTTP Req Host
- HTTP Req Method
- HTTP Req Rcv FB
- HTTP Req Rcv LB
- HTTP Req Referer
- HTTP Req URL
- HTTP Req XForwarded For
- HTTP Res Forw FB
- HTTP Res Forw LB
- HTTP Res Location
- HTTP Res Rcv FB
- HTTP Res Rcv LB
- HTTP Res Set Cookie
- HTTP Rsp Len
- HTTP Rsp Status
- HTTP Transaction End Time
- HTTP Transaction ID
- IC Cont Grp Name
- IC Flags
- IC No Store Flags

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- IC Policy Name
- Ingress Interface Client
- Anwendungs-ID des NetScaler Gateway Service
- Name der NetScaler Gateway Service-App
- App-Typ des NetScaler Gateway Service
- NetScaler-Partitions-ID
- Observation Domain ID
- Observation Point ID
- Origin Res Status
- Origin Rsp Len
- Protocol Identifier
- Rate Limit Identifier Name
- Datensatztyp
- Aktionstyp des Responders
- Response-Medientyp
- Srv Flow Flags Rx
- Srv Flow Flags Tx
- Srvr Fast Retx Count
- Server TCP-Jitter
- Srvr TCP Packets Retransmitted
- Srvr TCP Rto Count
- Srvr TCP Null-Fensteranzahl
- SSL Cipher Value BE
- SSL Cipher Value FE
- SSL Client Cert Size BE
- SSL Client Cert Size FE
- SSL Clnt Cert Sig Hash BE
- SSL Clnt Cert Sig Hash FE
- SSL Err App Name

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- SSL Err Flag
- SSL FLags BE
- SSL FLags FE
- SSL Handshake Error Msg
- SSL Server Cert Size BE
- SSL Server Cert Size FE
- SSL Session ID BE
- SSL Session ID FE
- SSL Sig Hash Alg BE
- SSL Sig Hash Alg FE
- SSL Srvr Cert Sig Hash BE
- SSL Srvr Cert Sig Hash FE
- SSL iDomain Category
- SSL iDomain Category Group
- SSL iDomain Name
- SSL iDomain Reputation
- SSL iExecuted Action
- SSL iPolicy Action
- SSL iReason For Action
- SSL iURL Set Matched
- SSL iURL Set Private
- Abonnenten-Kennung
- Svr Tcp Flags Rx
- Svr Tcp Flags Tx
- Tenant Name
- Tracing Req Parent Span ID
- Tracing Req Span ID
- Tracing Trace ID
- Trans Clt Dst IPv4 Address

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Trans Clt Dst IPv6 Address
- Trans Clt Dst Port
- Trans Clt Flow End Usec Rx
- Trans Clt Flow End Usec Tx
- Trans Clt Flow Start Usec Rx
- Trans Clt Flow Start Usec Tx
- Trans Clt IPv4 Address
- Trans Clt IPv6 Address
- Trans Clt Packet Tot Cnt Rx
- Trans Clt Packet Tot Cnt Tx
- Trans Clt RTT
- Trans Clt Src Port
- Trans Clt Tot Rx Oct Cnt
- Trans Clt Tot Tx Oct Cnt
- Trans Info
- Trans Srv Dst Port
- Trans Srv Packet Tot Cnt Rx
- Trans Srv Packet Tot Cnt Tx
- Trans Srv Src Port
- Trans Svr Flow End Usec Rx
- Trans Svr Flow End Usec Tx
- Trans Svr Flow Start Usec Rx
- Trans Svr Flow Start Usec Tx
- Trans Svr RTT
- Trans Svr Tot Rx Oct Cnt
- Trans Svr Tot Tx Oct Cnt
- Transaktion-ID
- URL-Kategorie
- URL Category Group

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- URL Category Reputation
- URL Category Action Reason
- URL Set Matched
- URL set Private
- URL Object ID
- VLAN Number

Citrix Virtual Apps and Desktops und Citrix DaaS-Protokolle

Die Citrix Virtual Apps and Desktops und Citrix DaaS-Protokolle enthalten die folgenden Datenpunkte:

- App-Name
- Browser
- Kunden-ID
- Details: Formatgröße, Formattyp, Initiator, Ergebnis
- Geräte-ID
- Gerätetyp
- Feedback
- Feedback-ID
- Dateiname
- Datei-Pfad
- Größe der Datei
- Ist wie
- Jail Broken
- Job-Details: Dateiname, Format, Größe
- Ort: Geschätzt, Breitengrad, Längengrad

  > **Hinweis**
  >
  > Die Standortinformationen werden auf Stadt- und Landesebene bereitgestellt und stellen keine genaue Geolocation dar.

- Lange CMD-Leitung

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Modul-Dateipfad
- Vorgang
- Betriebssystem
- Zusätzliche Informationen zur Plattform
- Name des Druckers
- Frage
- Fragen-ID
- SaaS-App-Name
- Sitzungsdomäne
- Name des Sitzungsservers
- Benutzername der Sitzung
- Sitzungs-GUID
- Zeitstempel
- Time Zone: Bias, DST, Name
- Total Copies Printed
- Total Pages Printed
- Typ
- URL
- Benutzeragent

Citrix ADC-Protokolle

Die Citrix ADC-Protokolle enthalten die folgenden Datenpunkte:

- Container
- Dateien
- Format
- Typ

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Citrix DaaS Standard für Azure-Protokolle

Die Citrix DaaS Standard for Azure-Protokolle enthalten die folgenden Datenpunkte:

- App-Name
- Browser
- Details: Formatgröße, Formattyp, Initiator, Ergebnis
- Geräte-ID
- Gerätetyp
- Dateiname
- Datei-Pfad
- Größe der Datei
- Jail Broken
- Job-Details: Dateiname, Format, Größe
- Ort: Geschätzt, Breitengrad, Längengrad

  > **Hinweis**
  >
  > Die Standortinformationen werden auf Stadt- und Landesebene bereitgestellt und stellen keine genaue Geolocation dar.

- Lange CMD-Leitung
- Modul-Dateipfad
- Vorgang
- Betriebssystem
- Zusätzliche Informationen zur Plattform
- Name des Druckers
- SaaS-App-Name
- Sitzungsdomäne
- Name des Sitzungsservers
- Benutzername der Sitzung
- Sitzungs-GUID
- Zeitstempel
- Time Zone: Bias, DST, Name

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Typ
- URL
- Benutzeragent

Citrix Identity Provider-Protokolle

- Benutzer-Login:
  - Authentication Domains: Name, Product, IdP Type, IdP Display Name
    - IdP Properties: App, Auth Type, Customer Id, Client Id, Directory, Issuer, Logo, Resources, TID
    - Verlängerungen:
      - Workspace: Background Color, Header Logo, Logon Logo, Link Color, Text Color, StoreFront Domains
      - ShareFile: Customer Id, Customer Geo
      - Long Lived Token: Enabled, Expiry Type, Absolute Expiry Seconds, Sliding Expiry Seconds
  - Authentication Result: User Name, Error Message
  - Sign-in Message: Client Id, Client Name
  - User Claim: AMR, Access Token Hash, Aud, Auth Time, CIP Cred, Auth Alias, Auth Domains, Groups, Product, System Aliases, Email, Email Verified, Exp, Family Name, Given Name, IAT, IdP, ISS, Locale, Name, NBF, SID, Sub
    - Auth Alias Claims: Name, Value
    - Directory Context: Domain, Forrest, Identity Provider, Tenant Id
    - User: Customers, Email, OID, SID, UPN
    - IdP Extra Fields: Azure AD OID, Azure AD TID
- User Logoff: Client Id, Client Name, Nonce, Sub
- Client Update: Action, Client Id, Client Name

NetScaler Gateway Protokolle

- Transaktions-Ereignisse:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- ICA App: Record Type, Actual Template Code, Observation Domain Id, Observation Point Id, Exporting Process Id, ICA Session Guid, MSI Client Cookie, Flow Id Rx, ICA Flags, Connection Id, Padding Octets Two, ICA Device Serial Number, IP Version 4, Protocol Identifier, Source IPv4 Address Rx, Destination IPv4 Address Rx, Source Transport Port Rx, Destination Transport Port Rx, ICA Application Start up Duration, ICA Launch Mechanism, ICA Application Start up Time, ICA Process ID Launch, ICA Application Name, ICA App Module Path, ICA Application Termination Type, ICA Application Termination Time, Application Name App Id, ICA App Process ID Terminate, ICA App
- ICA Event: Record Type, Actual Template Code, Source IPv4 Address Rx, Destination IPv4 Address Rx, ICA Session Guid, MSI Client Cookie, Connection Chain ID, ICA Client Version, ICA Client Host Name, ICA User Name, ICA Domain Name, Logon Ticket Setup, Server Name, Server Version, Flow Id Rx, ICA Flags, Observation Point Id, Exporting Process Id, Observation Domain Id, Connection Id, ICA Device Serial Number, ICA Session Setup Time, ICA Client IP, NS ICA Session Status Setup, Source Transport Port Rx, Destination Transport Port Rx, ICA Client Launcher, ICA Client Type, ICA Connection Priority Setup, NS ICA Session Server Port, NS ICA Session Server IP Address, IPv4, Protocol Identifier,Connection Chain Hop Count, Access Type
- ICA Update: Record Type, Actual Template Code, Observation Domain Id, Observation Point Id, Exporting Process Id, ICA Session Guid, MSI Client Cookie, Flow Id Rx,ICA Flags, Connection Id, ICA Device Serial Number, IPv4, Protocol Identifier, Padding Octets Two, ICA RTT, Client Side RX Bytes, Client Side Packets Retransmit, Server Side Packets Retransmit, Client Side RTT, Client Side Jitter, Server Side Jitter, ICA Network Update Start Time, ICA Network Update End Time, Client Side SRTT, Server Side SRTT,Client Side Delay, Server Side Delay, Host Delay, Client Side Zero Window Count, Server Side Zero Window Count, Client Side RTO Count, Server Side RTO Count, L7 Client Latency, L7 Server Latency, App Name App Id, Tenant Name, ICA Session Update Begin Sec, ICA Session Update End Sec, ICA Channel Id 1, ICA Channel Id 2, ICA Channel Id 2 Bytes, ICA Channel Id 3, ICA Channel Id 3 Bytes, ICA Channel Id 4, ICA Channel Id 4 Bytes, ICA Channel Id 5, ICA Channel Id 5 Bytes
- AppFlow Config: Record Type, Actual Template Code, Observation Domain Id, Observation Point Id, Exporting Process Id, System Rule Flag 1, System Safety Index, AppFlow Profile Relaxed Flags, AppFlow Profile Block Flags, AppFlow Profile Log Flags, AppFlow Profile Learn Flags, AppFlow Profile Stats Flags, AppFlow Profile None Flags, AppFlow App Name Id, AppFlow Profile Sign Disabled, AppFlow Profile Sign Block Count, AppFlow Profile Sign Log Count, AppFlow Profile Sign Stat Count, AppFlow Incarnation Number,AppFlow Sequence Number, AppFlow Profile Sign Auto Update, AppFlow Safety Index, AppFlow App Safety Index, AppFlow Profile Sec Checks Safety Index, AppFlow Profile Type, Iprep App Safety Index, AppFlow Profile Name, AppFlow Sig Name, AppFlow App Name Ls, AppFlow Sig Rule ID1, AppFlow Sig Rule ID2, AppFlow Sig Rule ID3, AppFlow Sig Rule ID4, AppFlow

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Sig Rule ID5, AppFlow Sig Rule Enabled Flags, AppFlow Sig Rule Block Flags, AppFlow Sig Rule Log Flags, AppFlow Sig Rule File Name, AppFlow Sig Rule Category1, AppFlow Sig Rule Logstring1, AppFlow Sig Rule Category2, AppFlow Sig Rule Logstring2, AppFlow Sig Rule Category3, AppFlow Sig Rule Category4, AppFlow Sig Rule Logstring4, AppFlow Sig Rule Category5, AppFlow Sig Rule LogString5

- AppFlow: Actual Template Code, Observation Domain Id, Observation Point Id, Exporting Process Id, Transaction Id, Appfw Violation Occurred Time, App Name App Id, Appfw Violation Severity, Appfw Violation Type, Appfw Violation Location, Appfw Violation Threat Index, Appfw NS Longitude, Appfw NS Latitude, Source IPv4 Address Rx, Appfw Http Method, Appfw App Threat Index, Appfw Block Flags, Appfw Transform Flags, Appfw Violation Profile Name, Appfw Session Id, Appfw Req Url, Appfw Geo Location, Appfw Violation Type Name 1, Appfw Violation Name Value 1, Appfw Sig Category 1, Appfw Violation Type Name 2, Appfw Violation Name Value 2, Appfw Sig Category 2, Appfw Violation Type Name 3, Appfw Violation Name Value 3, Appfw Sig Category3, Appfw Req X Forwarded For, Appfw App Name Ls,App Name Ls, Iprep Category, Iprep Attack Time, Iprep Reputation Score, Iprep NS Longitude, Iprep NS Latitude, Iprep Severity, Iprep HTTP Method, Iprep App Threat Index, Iprep Geo Location, Tcp Syn Attack Cntr, Tcp Slow Ris Cntr, Tcp Zero Window Cntr, Appfw Log Expr Name, Appfw Log Expr Value, Appfw Log Expr Comment
- VPN: Actual Template Code, Observation Domain Id, Access Insight Flags, Observation Point Id, Exporting Process Id, Access Insight Status Code, Access Insight Timestamp, Authentication Duration, Device Type, Device ID, Device Location, App Name App Id, App Name App Id1, Source Transport Port Rx, Destination Transport Port Rx, Authentication Stage, Authentication Type, VPN Session ID, EPA Id, AAA User Name, Policy Name, Auth Agent Name, Group Name, Virtual Server FQDN, cSec Expression, Source IPv4 Address Rx, Destination IPv4 Address Rx, Cur Factor Policy Label, Next Factor Policy Label, App Name Ls, App Name 1 Ls,AAA User Email Id, Gateway IP, Gateway Port, Application Byte Count, VPN Session State, VPN Session Mode, SSO Auth Method, IIP Address, VPN Request URL, SSO Request URL, Backend Server Name, VPN Session Logout Mode, Logon Ticket File Info, STA Ticket, Session Sharing Key, Resource Name, SNIP Address, Temp VPN Session ID
- HTTP: Actual Template Code, Http Req Method, Http Req Url, Http Req User Agent, Http Content Type, Http Req Host, Http Req Authorization, Http Req Cookie, Http Req Referer, Http Res Set Cookie, Ic Cont Grp Name, Ic Flags, Ic Nostore Flags, Ic Policy Name, Response Media Type, Ingress Interface Client, Origin Res Status, Origin Rsp Len, Srv Flow Flags Rx, Srv Flow Flags Tx, Flow Flags Rx, Flow Flags Tx, App Name, Observation Point Id, Exporting Process Id, Observation Domain Id, Http Trans End Time, Transaction Id, Http Rsp Status, Trans Clt Ipv4 Address, Trans Clt Dst Ipv4 Address, Backend Svr Dst Ipv4 Address, Backend Svr Ipv4 Address, Http Rsp Len, Trans Svr RTT, Trans Clt RTT, Http Req Rcv FB, Http Req Rcv LB, Http Res Rcv FB, Http Res Rcv LB, Http Req Forw FB, Http Req Forw LB, Http Res Forw

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

FB, Http Res Forw LB, Http Req X Forwarded For, Http Domain Name, Http Res Location, Protocol Identifier, Egress Interface, Backend Svr Ipv6 Address, SSL Flags BE, SSL Flags FE, SSL Session IDFE, SSL Session IDBE, SSL Cipher Value FE, SSL Cipher Value BE, SSL Sig Hash Alg BE, SSL Sig Hash Alg FE, SSL Srvr Cert Sig Hash BE, SSL Srvr Cert Sig Hash FE, SSL Clnt Cert Sig Hash FE, SSL Clnt Cert Sig Hash BE, SSL Server Cert Size FE, SSL Server Cert Size BE, SSL Client Cert Size FE, SSL Client Cert Size BE, SSL Err App Name, SSL Err Flag, SSL Handshake Error Msg, Client IP, Virtual Server IP, Connection Chain Id, Connection Chain Hop Count, Trans Clt Tot Rx Oct Cnt, Trans Clt TotTx Oct Cnt, Trans Clt Src Port, Trans Clt Dst Port, Trans Srv Src Port, Trans Srv Dst Port, VLAN Number, Client Mss, Trans Info, Trans Clt Flow End Usec Rx, Trans Clt Flow End Usec Tx, Trans Clt Flow Start Usec Rx, Trans Clt Flow Start Usec Tx, Trans Svr Flow End Usec Rx, Trans Svr Flow End Usec Tx, Trans Svr Flow Start Usec Rx, Trans Svr Flow Start Usec Tx, Trans Svr Tot Rx Oct Cnt, Trans Svr Tot Tx Oct Cnt, Clt Flow Flags Tx, Clt Flow Flags Rx, Trans Clt Ipv6 Address, Trans Clt Dst Ipv6 Address, Subscriber Identifier, SSLi Domain Name, SSLi Domain Category, SSLi Domain Category Group, SSLi Domain Reputation, SSLi Policy Action, SSLi Executed Action, SSLi Reason For Action, SSLi URL Set Matched, SSLi URL Set Private, URL Category, URL Category Group, URL Category Reputation, Responder Action Type, URL Set Matched, URL Set Private, Category Domain Name, Category Domain Source, AAA User Name, VPN Session ID, Tenant Name

- Metrikereignisse:
  - VServer LB: Bind Entity Name, Entity Name, Mon Service Binding, NetScaler Id, Representation, Schema Type, Time, CPU, GSLB Server, GSLB VServer, Interface, Memory Pool, Server Service Group, Server Svc Cfg, VServer Authn, VServer Cr, VServer Cs, VServer LB: RATE Si Tot Request Bytes, RATE Si Tot Requests, RATE Si Tot Response Bytes, RATE Si Tot Responses, RATE Si Tot Clt Ttlb Transactions, RATE Si Tot Clt Ttlb Pkt Rcvd, RATE Si Tot Clt Ttlb Pkt Sent, RATE Vsvr Tot Hits, Si Cur Clients, Si Cur Conn Established, Si Cur Servers, Si Cur State, Si Tot Request Bytes, Si Tot Responses, Si Tot Clt Ttlb, Si Tot Clt Ttlb Transactions, Si Tot Pkt Rcvd, Si Tot Pkt Sent, Si Tot Ttlb Frustrating Transactions, Si Tot Ttlb Tolerating Transactions, Vsvr Active Svcs, Vsvr Tot Hits, Vsvr tot Req Resp Invalid, Vsvr Tot Req Resp Invalid Dropped
  - CPU: Bind Entity Name, Entity Name, Mon Service Binding, NetScaler Id, Representation, Schema Type, Time, Cc CPU Use GSLB Server, GSLB Vserver, Interface, Memory Pool, NetScaler, Server Service Group, Server Svc Cfg, VServer Authn, VServer Cr, VServer Cs, VServer Lb, VServer SSL, VServer User
  - Server Service Group: Bind Entity Name, Entity Name, Mon Service Binding, NetScaler Id, Representation, Schema Type, Time, Cc CPU Use, GSLB Server, GSLB Vserver, Interface, Memory Pool, NetScaler, Server Svc Cfg, VServer Authn, VServer Cr, VServer Cs, VServer Lb, VServer SSL, VServer User, Server Service Group: RATE Si Tot Request Bytes, RATE Si Tot

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Requests, RATE Si Tot_Response Bytes, RATE Si Tot Responses, RATE Si Tot Clt Ttlb, RATE Si Tot Clt Ttlb Transactions, RATE Si Tot Svr Ttfb, RATE Si Tot Svr Ttfb Transactions, RATE Si Tot Svr Ttlb, RATE Si Tot Svr Ttlb Transactions, RATE Si Tot Ttlb Frustrating Transactions, RATE Si Tot Ttlb Tolerating Transactions, Si Cur State, Si Tot Request Bytes, Si Tot Requests, Si Tot Response Bytes, Si Tot Responses, Si Tot Clt Ttlb, Si Tot Clt Ttlb Transactions, Si Tot Svr Ttfb, Si Tot Svr Ttfb Transactions,Si Tot Svr Tlb, Si Tot Svr Ttlb Transactions, Si Tot Ttlb Frustrating Transactions, Si Tot Ttlb Tolerating Transactions

- Server SVC CFG: Bind Entity Name, Entity Name, Mon Service Binding, NetScaler Id, Representation, Schema Type, Time, CPU Use, GSLB Server, GSLB Vserver, Interface, Memory Pool, NetScaler, VServer Authn, VServer Cr, VServer Cs, VServer Lb, VServer SSL, VServer User, Server Svc Cfg: RATE Si Tot Request Bytes, RATE Si Tot Requests, RATE Si Tot Response Bytes, RATE Si Tot Responses, Si Tot Clt Ttlb, RATE Si Tot Clt Ttlb Transactions, RATE Si Tot Pkt Rcvd, RATE Si Tot Pkt Sent, RATE Si Tot Svr Busy Err, RATE Si Tot Svr Ttfb, RATE Si Tot Svr Ttfb Transactions, RATE Si Tot Svr Ttlb, RATE Si Tot Svr Ttlb Transactions, RATE Si Tot Ttlb Frustrating Transactions, RATE Si Tot Ttlb Tolerating Transactions, Si Cur State, Si Cur Transport, Si Tot Request Bytes, Si Tot Requests, Si Tot Response Bytes, Si Tot Responses, Si Tot Clt Ttlb, Si Tot Clt Ttlb Transactions, Si Tot Pkt Rcvd, Si Tot Pkt Sent, Si Tot Svr Busy Err, Si Tot Svr Ttfb, Si Tot Svr Ttfb Transactions, Si Tot Svr Ttlb, Si Tot Svr Ttlb Transactions, Si Tot Ttlb Frustrating Transactions, Si Tot Ttlb Tolerating Transactions
- NetScaler: Bind Entity Name, Entity Name, Mon Service Binding, NetScaler Id, Representation, Schema Type, Time, GSLB Server, GSLB VServer, Interface, Memory Pool, Server Service Group, Server Svc Cfg, VServer Authn, VServer Cr, VServer Cs, VServer Lb, VServer SSL, VServer User, NetScaler: RATE All Nic Tot Rx Mbits, RATE All Nic Tot Rx Mbits, RATE Dns Tot Queries, RATE Dns Tot Neg Nxdmn Entries,RATE Http Tot Gets, RATE Http Tot Others, RATE Http Tot Posts, RATE Http Tot Requests, RATE Http Tot Requests 1.0, RATE Http Tot Requests 1.1, RATE Http Tot Responses, RATE Http Tot Rx Request Bytes, RATE Http Tot Rx Response Bytes, RATE Ip Tot Rx Mbits, RATE Ip Tot Rx Bytes, RATE Ip Tot Rx Pkts, RATE Ip Tot Tx Mbits, RATE Ip Tot Tx Bytes, RATE Ip Tot Tx Pkts, RATE SSL Tot Dec Bytes, RATE SSL Tot Enc Bytes,RATE SSL Tot SSL Info Session Hits, RATE SSL Tot SSL Info Total Tx Count, RATE Tcp Err Rst, RATE Tcp Tot Client Open, RATE Tcp Tot Server Open, RATE Tcp Tot Rx Bytes, RATE Tcp Tot Rx Pkts, RATE Tcp Tot Syn, RATE Tcp Tot Tx Bytes, RATE Tcp Tot Tx Pkts, RATE Udp Tot Rx Bytes, RATE Udp Tot Rx Pkts, RATE Udp Tot Tx Bytes, RATE Udp Tot Tx Pkts, All Nic Tot Rx Mbits, All Nic Tot Tx Mbits, Cpu Use, Dns Tot Queries, Dns Tot Neg Nxdmn Entries, Http Tot Gets, Http Tot Others, Http Tot Posts, Http Tot Requests, Http Tot Requests1.0, Http Tot Requests1.1, Http Tot Responses, Http Tot Rx Request Bytes, Http Tot Rx Response Bytes, Ip Tot Rx Mbits, Ip Tot Rx Bytes, Ip Tot Rx Pkts, Ip Tot Tx Mbits, Ip Tot Tx Bytes, Ip Tot Tx Pkts, Mem Cur Free size, Mem Cur Free size Actual, Mem Cur Used size, Mem Tot Available, Mgmt Additional Cpu Use, Mgmt Cpu 0 Use, Mgmt Cpu Use, SSL Tot Dec Bytes, SSL Tot Enc Bytes, SSL Tot SSL Info Session Hits, SSL Tot SSL Info Total Tx

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Count, Sys Cpus, Tcp Cur Client Conn, Tcp Cur Client Conn Closing, Tcp Cur Client Conn Est, Tcp Cur Server Conn, Tcp Cur Server Conn Closing, Tcp Cur Server Conn Est, Tcp Err Rst, Tcp Tot Client Open, Tcp Tot Server Open, Tcp Tot Rx Bytes, Tcp Tot Rx Pkts, Tcp Tot Syn, Tcp Tot Tx Bytes, Tcp Tot Tx Pkts, Udp Tot Rx Bytes, Udp Tot Rx Pkts, Udp Tot Tx Bytes, Udp Tot Tx Pkts

- Memory Pool: Bind Entity Name, Entity Name, Mon Service Binding, NetScaler Id, Schema Type, Time, CPU, Gslb Server, Gslb VServer, Interface, NetScaler, Server Service Group, Server Svc Cfg, VServer Authn, VServer Cr, VServer Cs, VServer Lb, VServer SSL, VServer User, Memory Pool: Mem Cur Alloc Size, Mem Err Alloc Failed, Mem Tot Available
- Monitoring Service Binding: Bind Entity Name, Entity Name, NetScalerId, SchemaType, Time, CPU, Gslb Server, Gslb VServer, Interface, Memory Pool, NetScaler, Server Service Group, Server Svc Cfg, VServer Authn, VServer Cr, VServer Cs, Vserver Lb, VServer SSL, VServer User, Mon Service Binding: RATE Mon Tot Probes, Mon Tot Probes
- Interface: Bind Entity Name, Entity Name, Mon Service Binding, NetScaler Id, Schema Type, Time, CPU, Gslb Server, Gslb VServer, Memory Pool, NetScaler, Server Service Group, Server Svc Cfg, VServer Authn, VServer Cr, VServer Cs, Vserver Lb, VServer SSL, VServer User, Interface: RATE NIC Tot Rx Bytes, RATE NIC Tot Rx Packets, RATE NIC Tot Tx Bytes, RATE NIC Tot Tx Packets, NIC Tot Rx Bytes, NIC Tot Rx Packets, NIC Tot Tx Bytes, NIC Tot Tx Packets
- VServer CS: Bind Entity Name, Entity Name, Mon Service Binding, NetScaler Id, Schema Type, Time, CPU, Gslb Server, Gslb VServer, Memory Pool, NetScaler, Server Service Group, Server Svc Cfg, VServer Authn, VServer Cr, VServer Cs, Vserver Lb, VServer SSL, VServer User, VServer Cs: RATE Si Tot Request Bytes, RATE Si Tot Requests, RATE Si Tot Response Bytes, RATE Si Tot Responses, RATE Si Tot Clt Ttlb,RATE Si Tot Clt Ttlb Transactions, RATE Si Tot Pkt Rcvd, RATE Si Tot Pkt Sent, RATE Si Tot Ttlb Frustrating Transactions, RATE Si Tot Ttlb Tolerating Transactions, RATE Vsvr Tot Hits, Si Cur State, Si Tot Request Bytes, Si Tot Requests, Si Tot Response Bytes, Si Tot Responses, Si Tot Clt Ttlb, Si Tot Clt Ttlb Transactions, Si Tot Pkt Rvd, Si Tot Pkt Sent, Si Tot Ttlb Frustrating Transactions, Si Tot Tlb Tolerating Transactions, Vsvr Tot Hits, Vsvr Tot Req Resp Invalid, Vsvr Tot Req Resp Invalid Dropped

Secure Browser-Protokolle

- Anwendung veröffentlichen:
  - Logs before the published application: Authentication, Browser, Change Id, Created, Customer Name, Destination URL, E-Tag, Gateway Service Product Id, Session Id, Legacy Icon, Application Name, Policies, Published Application Id, Region, Resource Zone, Resource Zone Id, Subscription, Session Idle Timeout, Session Idle Timeout Warning, Watermark, Whitelist External, Whitelist Internal, Whitelist Redirect

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

  - Logs after the published application: Authentication, Browser, Change Id, Created, Customer Name, Destination, E-Tag, Gateway Service Product Id, Session Id, Legacy Icon, Application Name, Policies, Published Application Id, Region, Resource Zone, Resource Zone Id, Subscription, Session Idle Timeout, Session Idle Timeout Warning, Watermark, Whitelist External URL, Whitelist Internal URL, Whitelist Redirect URL

- Anwendung löschen:
  - Logs before the published application: Authentication, Browser, Change Id, Created, Customer Name, Destination URL, E-Tag, Gateway Service Product Id, Session Id, Legacy Icon, Application Name, Policies, Published Application Id, Region, Resource Zone, Resource Zone Id, Subscription, Session Idle Timeout, Session Idle Timeout Warning, Watermark, Whitelist External, Whitelist Internal, Whitelist Redirect
  - Logs after the published application: Authentication, Browser, Change Id, Created, Customer Name, Destination, E-Tag, Gateway Service Product Id, Session Id, Legacy Icon, Application Name, Policies, Published Application Id, Region, Resource Zone, Resource Zone Id, Subscription, Session Idle Timeout, Session Idle Timeout Warning, Watermark, Whitelist External URL, Whitelist Internal URL, Whitelist Redirect URL
- Anwendungs-Update:
  - Logs before the published application: Authentication, Browser, Change Id, Created, Customer Name, Destination URL, E-Tag, Gateway Service Product Id, Session Id, Legacy Icon, Application Name, Policies, Published Application Id, Region, Resource Zone, Resource Zone Id, Subscription, Session Idle Timeout, Session Idle Timeout Warning, Watermark, Whitelist External, Whitelist Internal, Whitelist Redirect
  - Logs after the published application: Authentication, Browser, Change Id, Created, Customer Name, Destination, E-Tag, Gateway Service Product Id, Session Id, Legacy Icon, Application Name, Policies, Published Application Id, Region, Resource Zone, Resource Zone Id, Subscription, Session Idle Timeout, Session Idle Timeout Warning, Watermark, Whitelist External URL, Whitelist Internal URL, Whitelist Redirect URL
- Anspruch erstellen:
  - Logs before the entitlement creation: Approved, Customer Id, Data Retention Days, End Date, Grace Period Days, Session Id, Product SKU, Quantity, Serial Numbers, Start Date, State, Type
  - Logs after the entitlement creation: Approved, Customer Id, Data Retention Days, End Date, Grace Period Days, Session Id, Product SKU, Quantity, Serial Numbers, Start Date, State, Type
- Anspruchsupdate:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

  - Logs before the entitlement update: Approved, Customer Id, Data Retention Days, End Date, Grace Period Days, Session Id, Product SKU, Quantity, Serial Numbers, Start Date, State, Type
  - Logs after the entitlement update: Approved, Customer Id, Data Retention Days, End Date, Grace Period Days, Session Id, Product SKU, Quantity, Serial Numbers, Start Date, State, Type
- Session Access Host: Accept Host, Client IP, Date Time, Host, Session, User Name
- Sitzung verbinden:
  - Logs before the session connection: Application Id, Application Name, Browser, Created, Customer Id, Duration, Session Id, IP Address, Last Updated, Launch Source, User Name
  - Logs after the session connection: Application Id, Application Name, Browser, Created, Customer Id, Duration, Session Id, IP Address, Last Updated, Launch Source, User Name
- Start der Sitzung:
  - Logs before the session launch: Application Id, Application Name, Browser, Created, Customer Id, Duration, Session Id, IP Address, Last Updated, Launch Source, User Name
  - Logs after the session launch: Application Id, Application Name, Browser, Created, Customer Id, Duration, Session Id, IP Address, Last Updated, Launch Source, User Name
- Session Tick:
  - Logs before the session tick: Application Id, Application Name, Browser, Created, Customer Id, Duration, Session Id, IP Address, Last Updated, Launch Source, User Name
  - Logs after the session tick: Application Id, Application Name, Browser, Created, Customer Id, Duration, Session Id, IP Address, Last Updated, Launch Source, User Name

Microsoft Graph-Sicherheitsprotokoll

- Mandanten-Id
- Benutzer-ID
- Indikator-ID
- Indikator UUID
- Uhrzeit des Ereignisses
- Zeit erstellen
- Kategorie der Warnung

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Ort der Anmeldung
- Anmelde-IP
- Anmelde-Typ
- Typ des Benutzerkontos
- Informationen des Anbieters
- Anbieter-Anbieterinformationen
- Sicherheitsrisikostatus
- Sicherheitsrisikoschweregrad

Microsoft Active Directory Protokolle

- Mandanten-Id
- Zeit sammeln
- Typ
- Directory-Kontext
- Gruppen
- Identität
- Benutzertyp
- Kontoname
- Anzahl schlechter Kennwörter
- Ort
- Allgemeiner Name
- Firma
- Land
- Tage bis zum Ablauf des Kennworts
- Abteilung
- Beschreibung
- Anzeigename
- Ausgezeichneter Name
- E-Mail

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Fax-Nummer
- Vorname
- Gruppenkategorie
- Umfang der Gruppe
- Telefon zu Hause
- Initialen
- IP-Telefon
- Ist das Konto aktiviert
- Ist das Konto gesperrt
- Ist Sicherheitsgruppe
- Nachname
- Managerin
- Mitglied von
- Handy
- Pager
- Kennwort läuft nie ab
- Name des physischen Zustellbüros
- Postfach
- PLZ
- Primäre Gruppen-ID
- Status
- Adresse
- Titel
- Benutzerkontensteuerung
- Liste der Benutzergruppen
- Benutzerprinzipalname
- Telefon für die Arbeit

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Citrix Analytics for Performance Leistungsprotokolle

- actionid
- actionreason
- actiontype
- adminfolder
- agentversion
- allocationtype
- applicationid
- applicationname
- applicationpath
- applicationtype
- applicationversion
- associateduserfullnames
- associatedusername
- associatedusernames
- associateduserupns
- authenticationduration
- autoreconnectcount
- autoreconnecttype
- AvgEndpointThroughputBytesReceived
- AvgEndpointThroughputBytesSent
- blobcontainer
- blobendpoint
- blobpath
- brokerapplicationchanged
- brokerapplicationcreated
- brokerapplicationdeleted
- brokeringdate
- brokeringduration

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- brokerloadindex
- brokerregistrationstarted
- browsername
- catalogchangeevent
- catalogcreatedevent
- catalogdeletedevent
- catalogid
- catalogname
- catalogsync
- clientaddress
- clientname
- clientplatform
- clientsessionvalidatedate
- clientversion
- collecteddate
- connectedviahostname
- connectedviaipaddress
- connectionid
- connectioninfo
- connectionstate
- connectiontype
- controllerdnsname
- cpu
- cpuindex
- createddate
- currentloadindexid
- currentpowerstate
- currentregistrationstate
- currentsessioncount

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- datetime
- deliverygroupadded
- deliverygroupchanged
- deliverygroupdeleted
- deliverygroupid
- deliverygroupmaintenancemodechanged
- deliverygroupname
- deliverygroupsync
- deliverytype
- deregistrationreason
- desktopgroupdeletedevent
- desktopgroupid
- desktopgroupname
- desktopkind
- disconnectcode
- disconnectreason
- disk
- diskindex
- dnsname
- domainname
- effectiveloadindex
- enddate
- errormessage
- establishmentdate
- eventreporteddate
- eventtime
- exitcode
- failurecategory
- failurecode

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- failuredata
- failuredate
- failurereason
- failuretype
- faultstate
- functionallevel
- gpoenddate
- gpostartdate
- hdxenddate
- hdxstartdate
- Host
- hostedmachineid
- hostedmachinename
- hostingservername
- hypervisorconnectionchangedevent
- hypervisorconnectioncreatedevent
- hypervisorid
- hypervisorname
- hypervisorsync
- icartt
- icarttms
- ID
- idletime
- inputbandwidthavailable
- inputbandwidthused
- instancecount
- interactiveenddate
- interactivestartdate
- ipaddress

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- isassigned
- isinmaintenancemode
- ismachinephysical
- ispendingupdate
- ispreparing
- isremotepc
- issecureica
- lastderegisteredcode
- launchedviahostname
- launchedviaipaddress
- lifecyclestate
- LinkSpeed
- logonduration
- logonenddate
- logonscriptsenddate
- logonscriptsstartdate
- logonstartdate
- long
- machineaddedtodesktopgroupevent
- machineassignedchanged
- machinecatalogchangedevent
- machinecreatedevent
- machinedeletedevent
- machinederegistrationevent
- machinednsname
- machinefaultstatechangeevent
- machinehardregistrationevent
- machineid
- machinemaintenancemodechangeevent

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- machinename
- machinepvdstatechanged
- machineregistrationendedevent
- machineremovedfromdesktopgroupevent
- machinerole
- machinesid
- machineupdatedevent
- machinewindowsconnectionsettingchanged
- memory
- memoryindex
- modifieddate
- NGSConnector.ICAConnection.Start
- NGSConnector.NGSSyntheticMetrics
- NGSConnector.NGSPassiveMetrics
- NGSConnector.NGSSystemMetrics
- network
- networkindex
- networklatency
- networkinfoperiodic
- NetworkInterfaceType
- ostype
- outputbandwidthavailable
- outputbandwidthused
- path
- percentcpu
- persistentuserchanges
- powerstate
- processname
- profileloadenddate

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- profileloadstartdate
- protocol
- provisioningschemeid
- provisioningtype
- publishedname
- registrationstate
- serversessionvalidatedate
- sessioncount
- sessionend
- sessionfailure
- sessionid
- sessionidlesince
- sessionindex
- sessionkey
- sessionstart
- sessionstate
- sessionsupport
- sessiontermination
- sessiontype
- sid
- SignalStrength
- siteid
- sitename
- startdate
- totalmemory
- triggerinterval
- triggerlevel
- triggerperiod
- triggervalue

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- usedmemory
- userid
- userinputdelay
- username
- usersid
- vdalogonduration
- vdaprocessdata
- vdaresourcedata
- version
- vmstartenddate
- vmstartstartdate
- windowsconnectionsetting
- xd.SessionStart

Systemanforderungen

April 12, 2024

Bevor Sie Citrix Analytics for Security verwenden, sollten Sie die folgenden Anforderungen überprüfen.

Citrix Analytics for Security-Abonnement

Dieses Analytics-Produkt ist ein abonnementbasiertes Angebot. Sie müssen über ein gültiges Abonnement verfügen, um Security Analytics verwenden zu können. Weitere Informationen finden Sie auf der Produktübersichtsseite .

Anforderungen an Datenquellen

Citrix Analytics for Security empfängt Ereignisse aus verschiedenen Datenquellen. Damit Analytics korrekt funktioniert, müssen Sie über ein gültiges Abonnement verfügen, um mindestens eines der folgenden Produkte verwenden zu können, die als Datenquellen für Analytics dienen:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Citrix ADC (on-premises) zusammen mit Abonnement für Citrix Application Delivery Management
- Citrix Endpoint Management-Service
- NetScaler Gateway (on-premises)
- Citrix Identitätsanbieter
- Citrix Remote Browser Isolation
- Citrix Secure Private Access Service
- Citrix Virtual Apps and Desktops oder Citrix DaaS (früher Citrix Virtual Apps and Desktops Service)
- Microsoft Active Directory
- Microsoft Graph Security

Unterstützte Browser

Um auf Analytics zugreifen zu können, muss Ihre Arbeitsstation über den folgenden unterstützten Webbrowser verfügen:

- Aktuelle Version von Google Chrome
- Aktuelle Version von Mozilla Firefox
- Aktuelle Version von Microsoft Edge
- Aktuelle Version von Apple Safari

Administratorrollen für Security Analytics verwalten

December 12, 2023

Als Citrix Cloud-Administrator mit vollen Zugriffsberechtigungen können Sie andere Administratoren einladen, das Security Analytics-Angebot zu verwalten und ihnen eine der folgenden benutzerdefinierten Rollen zuzuweisen:

- **Sicherheitsanalysen —Volladministrator**
- **Sicherheitsanalysen —Nur-Lese-Administrator**

Sie können neue Administratoren auf zwei Arten hinzufügen: einzeln als Benutzer oder mithilfe von Azure Active Directory-Gruppen. Weitere Informationen zum Hinzufügen neuer Administratoren finden Sie unter Administratorrollen verwalten.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Hinweis:**
> Wenn einem Benutzer direkt als Benutzer und über eine Azure Active Directory-Gruppe Zugriff gewährt wird, wird der dem Benutzer individuell gewährte Zugriff wirksam.

Berechtigungen für die benutzerdefinierten Rollen

Administratoren mit der Rolle "**Security Analytics** —**Volladministrator** "können auf alle Features und Funktionen des Security Analytics-Angebots zugreifen. Sie können die Funktionen entsprechend ihren organisatorischen Anforderungen verwenden und modifizieren. Ein Volladministrator kann beispielsweise benutzerdefinierte Risikoindikatoren erstellen, Geofence aktivieren und Richtlinien erstellen.

Die Administratoren mit der Rolle **Security Analytics** —**Read Only Administrator** können nur auf die Sicherheits-Dashboards —Benutzer, Benutzerzugriff, App-Zugriff, Zugriffssicherung und Berichte —zugreifen und diese anzeigen. Sie können das Benutzerverhalten überwachen und die Benutzerereignisse auf diesen Dashboards anzeigen. Sie dürfen jedoch keine kritischen Aufgaben ausführen wie:

- Ein- oder Ausschalten der Datenverarbeitung für die Datenquellen
- Richtlinien und Aktionen erstellen oder entfernen
- Wenden Sie Aktionen manuell auf die Risikoindikatoren an, die auf der Benutzerrisikozeitleiste angezeigt werden
- Benutzerdefinierte Risikoindikatoren erstellen, ändern oder löschen
- Erstellen benutzerdefinierter Berichte
- Einen weiteren Admin-Benutzer hinzufügen, ändern oder löschen
- Geofence für den Standort der Zugangssicherung hinzufügen oder ändern

Benachrichtigungen über Sicherheitswarnungen für Administratoren

Wie die Citrix Cloud-Administratoren mit vollen Zugriffsberechtigungen erhalten die Administratoren mit den benutzerdefinierten Rollen (Vollzugriff und schreibgeschützter Zugriff) E-Mail-Benachrichtigungen von Security Analytics.

Die Administratoren erhalten zwei Arten von E-Mail-Benachrichtigungen:

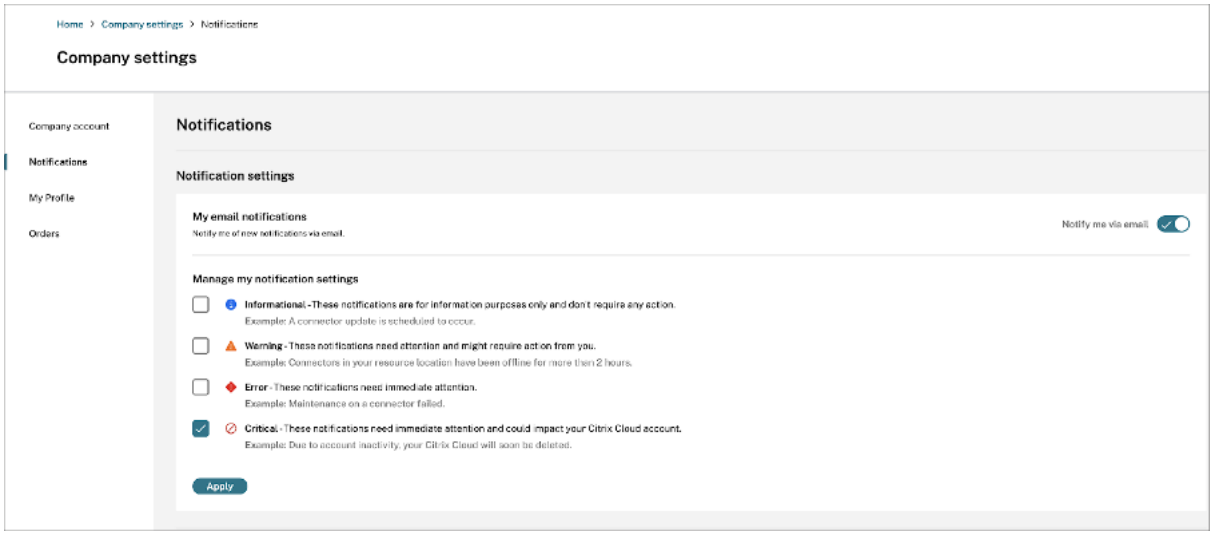
- Wöchentliche Benachrichtigung über die Sicherheitsinformationen in ihrer Organisation. Weitere Informationen finden Sie unter Wöchentliche E-Mail-Benachrichtigung.
- Benachrichtigungen, die auf der Aktion Administratoren benachrichtigen basieren. Weitere Informationen finden Sie unter Richtlinien und Aktionen.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Wenn Sie ein Citrix Cloud-Administrator mit vollständiger oder benutzerdefinierter Zugriffsberechtigung sind, sind die E-Mail-Benachrichtigungen in Ihrem Citrix Cloud-Konto standardmäßig deaktiviert. Um E-Mail-Benachrichtigungen von Citrix Cloud-Diensten wie Citrix Analytics zu erhalten, aktivieren Sie die Benachrichtigungsoption in Ihrer Citrix Cloud. Weitere Informationen finden Sie unter Erhaltene E-Mail-Benachrichtigungen. Die Benachrichtigungseinstellungen sind für Administratoren, die über Active Directory/Azure AD-Gruppen hinzugefügt wurden, nicht verfügbar.

Die Benachrichtigungspräferenz wird beim Senden von Benachrichtigungen wie wöchentlichen E-Mails, Aktions-E-Mails für Administratoren benachrichtigen und Benachrichtigungen für Datenexporte genutzt. Für die E-Mail-Benachrichtigungen muss Sie ein Administrator mit vollem Zugriff auf Security Analytics aus der Verteilerliste entfernen, wenn Sie keine E-Mails mehr erhalten möchten. Weitere Informationen zur Verteilerliste finden Sie unter E-Mail-Verteilerliste.

> **Hinweis:**
>
> Citrix Cloud-Administratoren (mit vollständiger oder benutzerdefinierter Zugriffsberechtigung) erhalten keine Benachrichtigungen von anderen Citrix Cloud-Diensten, die die **Benachrichtigungseinstellungen**nutzen.



Weitere Informationen finden Sie unter Verwalten von Administratoren für Citrix Analytics.

Erste Schritte

December 12, 2023

In diesem Dokument wird beschrieben, wie Sie zum ersten Mal mit Citrix Analytics for Security beginnen.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Schritt 1: Anmelden bei Citrix Cloud

Um Citrix Analytics for Security verwenden zu können, müssen Sie über ein Citrix Cloud-Konto verfügen. Gehen Sie zu https://citrix.cloud.com und melden Sie sich mit Ihrem vorhandenen Citrix Cloud-Konto an.

Wenn Sie kein Citrix Cloud-Konto haben, müssen Sie zuerst ein Citrix Cloud-Konto erstellen oder einem vorhandenen Konto beitreten, das von einer anderen Person in Ihrer Organisation erstellt wurde. Ausführliche Prozesse und Anweisungen zur weiteren Vorgehensweise finden Sie unter Anmelden für Citrix Cloud.

Schritt 2: Zugriff auf Security Analytics

Sie können auf Citrix Analytics for Security auf eine der folgenden Arten zugreifen:

- **Fordern Sie eine Testversion von Citrix Analytics for Security**an. Gehen Sie nach der Anmeldung bei Citrix Cloud wie folgt vor:
  1. Klicken Sie im Abschnitt **Verfügbare Dienste** auf der **Analytics-Kachel** auf **Verwalten** . Sie werden zur Analytics-Übersichtsseite weitergeleitet.
  2. Klicken Sie auf der Kachel **Sicherheit** auf **Testversion anfordern** oder wenden Sie sich direkt an Ihr Citrix-Konto oder Ihren Citrix Partner.
- **Abonnieren Sie Citrix Analytics for Security**. Um ein Abonnement für Citrix Analytics for Security zu erwerben, besuchen Sie https://www.citrix.com/en-in/products/citrix-analytics/form/inquiry/ und wenden Sie sich an einen Citrix Analytics-Experten, der Ihnen helfen kann.

> **Hinweis**
>
> - Mit Wirkung vom 8. März 2023 wird Citrix Analytics for Security nicht mehr als eigenständiges Angebot mit ShareFile/Citrix Content Collaboration erhältlich sein. Wir kündigen das

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

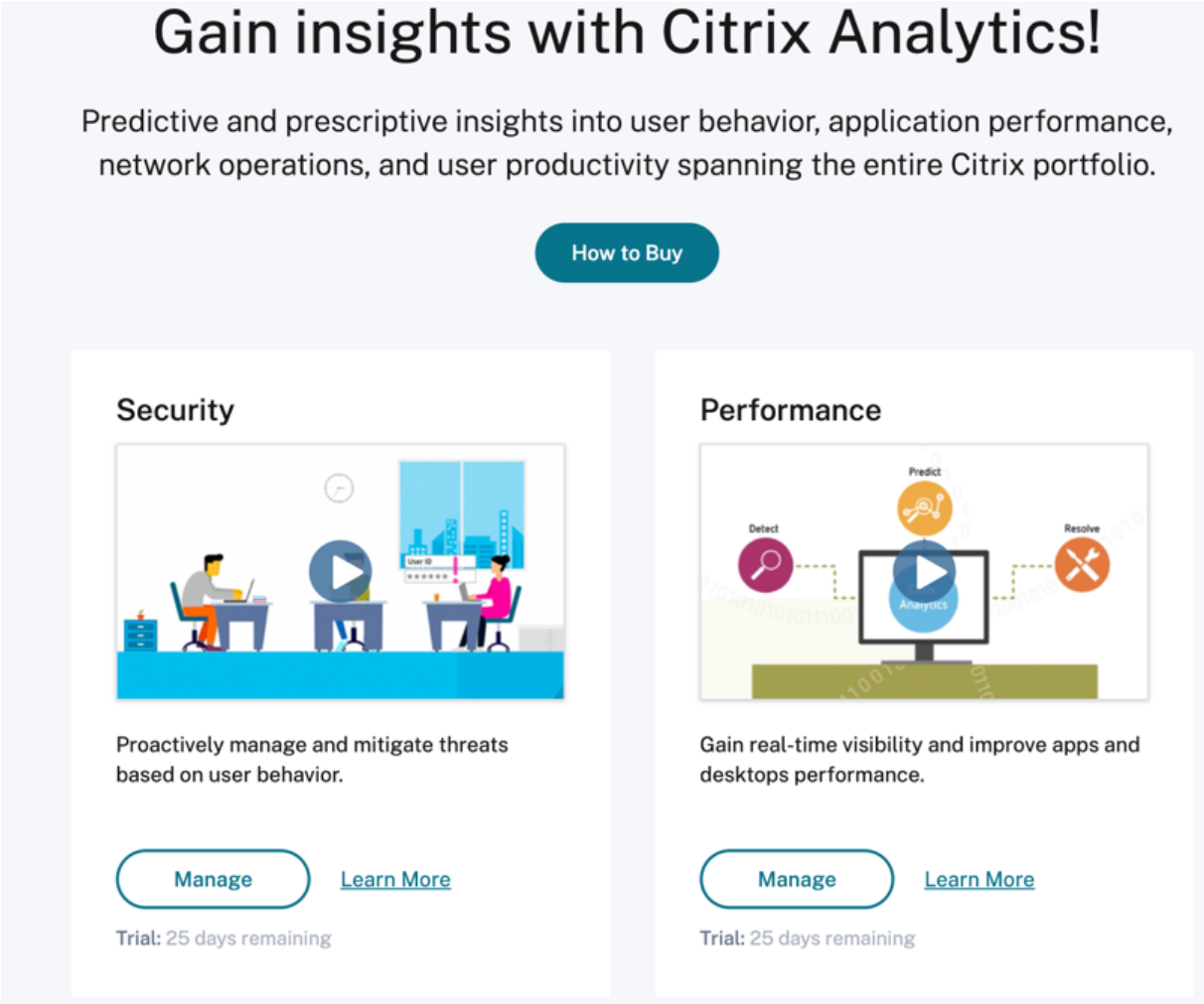
Ende des Vertriebs (EOS) und das Ende der Verlängerung (EOR) des eigenständigen Citrix Analytics Service-Add-ons für ShareFile/Citrix Content Collaboration an. Die bestehenden Berechtigungen der Kunden für Citrix Analytics for Security bleiben gültig, bis ihr Abonnement abläuft. Testversionen, Verlängerungen und Neukäufe werden jedoch für Sharefile/Citrix Content Collaboration-Integrationen nicht unterstützt. Citrix Analytics Service-Integrationen für andere Citrix-Produkte werden weiterhin als eigenständige Angebote oder als Bündelangebote mit bestehenden Citrix DaaS-Plänen, Citrix Virtual Apps and Desktops-Bereitstellungen und Citrix Workspace-Bereitstellungen angeboten.

- Mit Wirkung vom 03. Februar 2020 ist Citrix Analytics for Security nicht mehr in den Workspace Premium- und Workspace Premium Plus-Abonnements enthalten. Kunden, die das Workspace Premium- oder das Workspace Premium Plus-Abonnement vor dem 03. Februar 2020 erworben haben, können im Rahmen des Workspace-Abonnements bis zum Ablauf ihres Abonnements auf Citrix Analytics for Security zugreifen. Citrix Analytics for Security wird jetzt als Zusatzdienst mit den Citrix Workspace-Paketen Workspace Standard, Workspace Premium und Workspace Premium Plus angeboten. Weitere Informationen finden Sie unter Citrix Cloud-Dienste.

Schritt 3: Verwalten von Sicherheitsanalysen

Nachdem Sie das erforderliche Abonnement haben oder für den Zugriff auf die Testversion autorisiert sind, ändert sich auf der Analytics-Übersichtsseite die Schaltfläche **Testversion anfordern** für das Sicherheitsangebot in **Verwalten**. Klicken Sie auf **Verwalten**, um das Benutzer-Dashboard anzuzeigen.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Analytics unterstützt sowohl Citrix Datenquellen als auch externe Datenquellen. Es erkennt automatisch die Citrix Datenquellen, die mit Ihrem Citrix Cloud-Konto verknüpft sind. Um Daten aus externen Datenquellen zu empfangen, müssen Sie die externen Datenquellen in Analytics integrieren. Um die erkannten Datenquellen anzuzeigen, klicken Sie auf **Einstellungen > Datenquellen > Sicherheit**.

Nächste Schritte

- Die Datenverarbeitung wird für die folgenden Cloud-Dienste aktiviert, wenn deren Citrix Analytics for Security-Berechtigung genehmigt wurde:
  - Citrix Datenquellen
    - Citrix Secure Private Access
    - Citrix Virtual Apps and Desktops von Citrix und Citrix DaaS
- Informationen zum Überprüfen des Datenverarbeitungsstatus oder zur manuellen Aktivierung finden Sie in den folgenden Artikeln:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

    - Citrix Datenquellen:
        - Citrix Endpoint Management
        - Citrix Gateway
    - Externe Datenquellen:
        - Microsoft Graph Security
        - Microsoft Active Directory

- Exportieren Sie verarbeitete Daten aus Analytics in die folgenden Produkte:
    - Splunk
    - Microsoft Azure Sentinel
    - Elasticsearch
    - Andere SIEMs verwenden Kafka- oder Logstash-basierten Datenconnector
- Verwenden Sie das Benutzerdashboard, um die erkannten Benutzer und ihre Sicherheitsrisikoprofile anzuzeigen. Das **Benutzerdashboard** ist der Ausgangspunkt für die Analyse des Benutzerverhaltens und die Bedrohungsprävention.

  > **Hinweis**
  >
  > Wenn Sie Analytics zum ersten Mal verwenden, dauert es einige Zeit, bis die Benutzerrisikoprofile im Dashboard angezeigt werden. Analytics verwendet maschinelles Lernen, um das Risikomuster oder die Anomalien in den Benutzerereignissen zu ermitteln, und identifiziert die Benutzerprofile basierend auf der Schwere der Risiken als hohes Risiko, mittleres Risiko und geringes Risiko.

- Verwenden Sie die Self-Service-Suchfunktion, um die aus den Datenquellen empfangenen Benutzerereignisse (Rohdaten) anzuzeigen und zu filtern.

Citrix Endpoint Management-Datenquelle

December 6, 2021

Die **Endpoint Management-Datenquelle** stellt den Citrix Endpoint Management-Dienst dar, der mit Ihrem Citrix Cloud-Konto verknüpft ist. Wenn Benutzer diesen Dienst verwenden, erhält Citrix Analytics die Benutzerereignisse im Zusammenhang mit den Endpunkten der Benutzer und deren Aktivitäten in Echtzeit. Die Benutzerereignisse werden verarbeitet, um Sicherheitsbedrohungen zu erkennen.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Voraussetzungen

- Abonnieren Sie Citrix Endpoint Management, das in Citrix Cloud angeboten wird. Informationen zum Einrichten Ihres Endpoint Management-Dienstes finden Sie unter Onboarding und Ressourceneinrichtung.
- **Cloud-Website und Unternehmensverzeichnis eingerichtet**. Stellen Sie sicher, dass Sie zwei Computer haben, auf denen Windows 2012 R2 oder Windows 2016 Server ausgeführt wird, um den Cloud Connector zu installieren.
- **Cloud Connector ist installiert**. Laden Sie den Cloud Connector herunter und installieren Sie ihn auf einer virtuellen Maschine, die Teil von Active Directory ist.
- Prüfen Sie die Systemanforderungen und stellen Sie sicher, dass Ihre Umgebung die Anforderungen erfüllt.

Datenquelle anzeigen und Datenverarbeitung einschalten

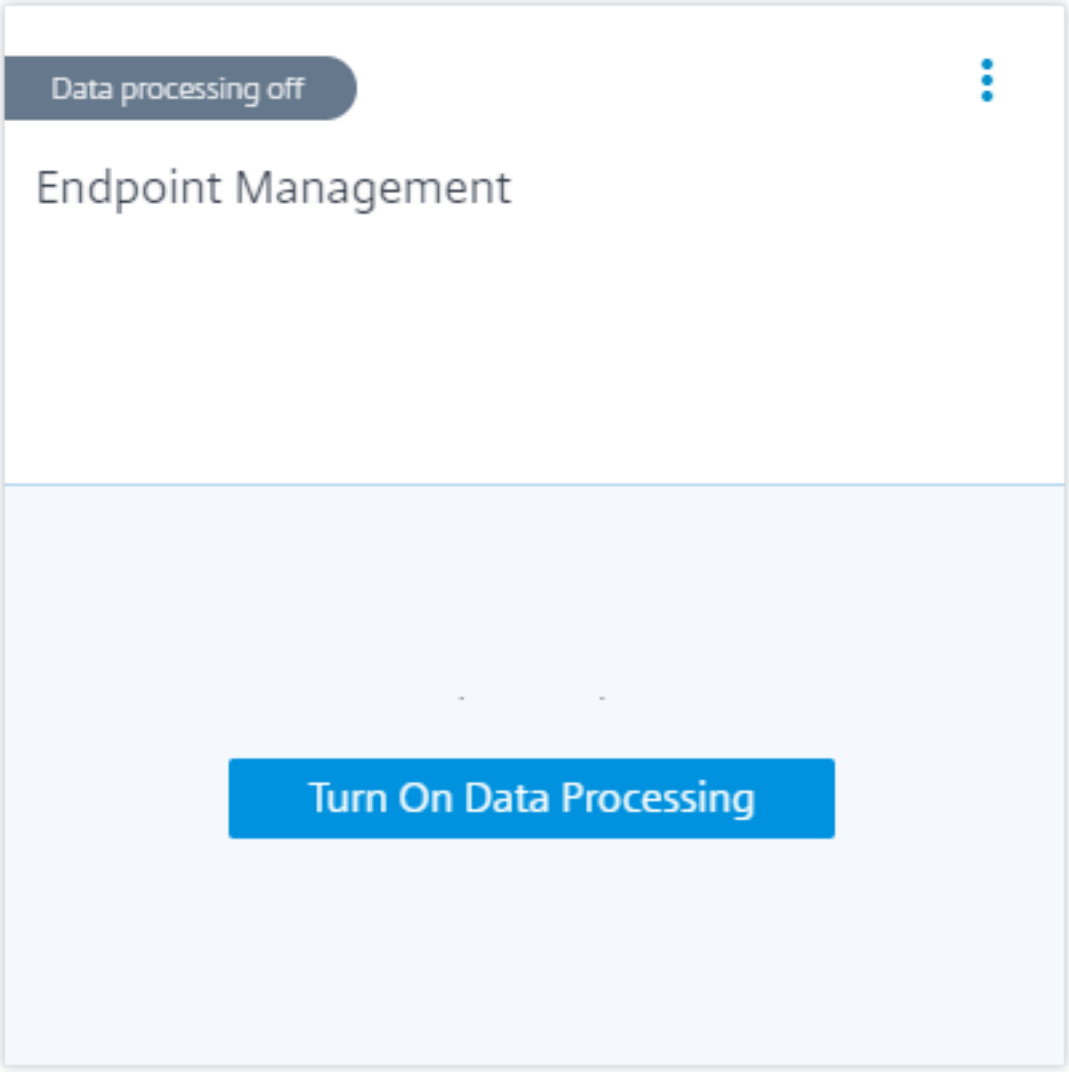
Citrix Analytics erkennt automatisch alle Endpoint Management-Datenquellen, die mit Ihrem Citrix Cloud-Konto verknüpft sind.

So zeigen Sie die Datenquelle an:

Klicken Sie in der oberen Leiste auf **Einstellungen** > **Datenquellen** > **Sicherheit**.

Eine Sitekarte für die Endpoint Management-Datenquelle wird auf der Seite **Datenquellen** angezeigt. Klicken Sie **auf Datenverarbeitung einschalten**, damit Citrix Analytics mit der Verarbeitung von Daten für diese Datenquelle beginnen kann.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

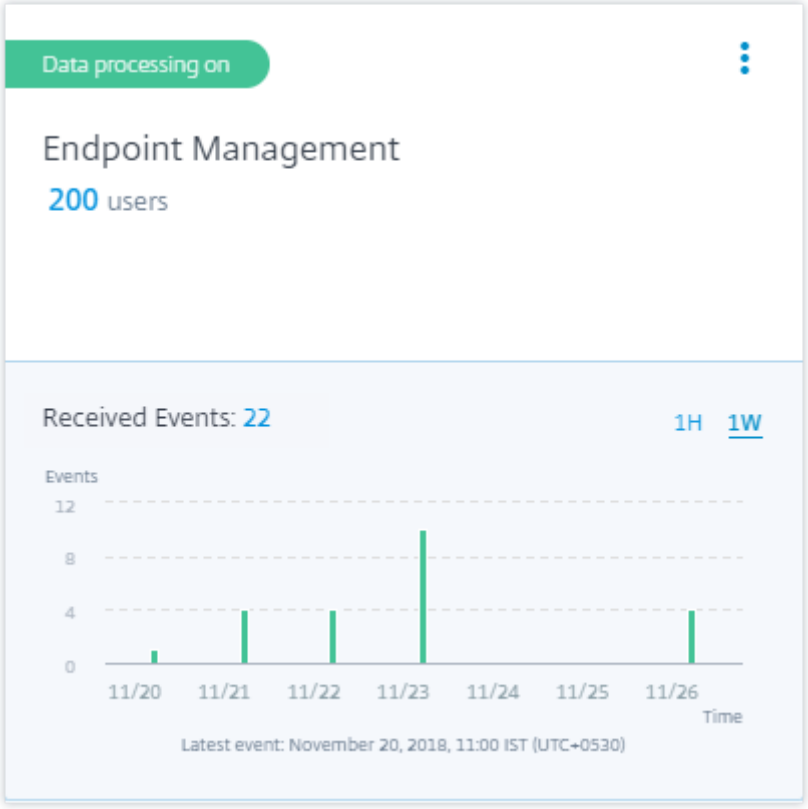


Benutzer und empfangene Ereignisse anzeigen

Die Sitekarte zeigt die Anzahl der Endpoint Management-Benutzer, Geräte und die empfangenen Ereignisse für die letzte Stunde an, was die Standardzeitauswahl ist. Sie können auch 1 Woche (**1 W**) auswählen und die Daten anzeigen.

Klicken Sie auf die Anzahl der Benutzer, um die Benutzerdetails auf der Seite **Benutzer** anzuzeigen.

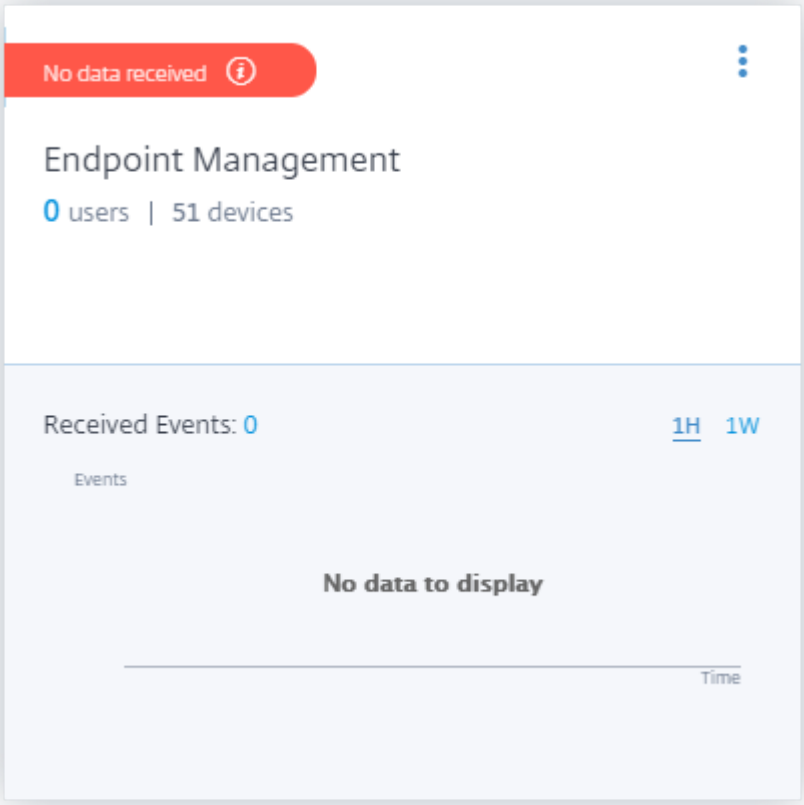
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Nachdem Sie die Datenverarbeitung aktiviert haben, zeigt die Site-Karte möglicherweise den Status **Keine empfangenen Daten** an. Dieser Status wird aus zwei Gründen angezeigt:

1. Wenn Sie die Datenverarbeitung zum ersten Mal aktiviert haben, benötigen die Ereignisse einige Zeit, um den Ereignis-Hub in Citrix Analytics zu erreichen. Wenn Citrix Analytics die Ereignisse empfängt, ändert sich der Status in **Datenverarbeitung am**. Wenn sich der Status nach einiger Zeit nicht ändert, aktualisieren Sie die Seite **Datenquellen**.
2. Analytics hat in der letzten Stunde keine Ereignisse von der Datenquelle erhalten.

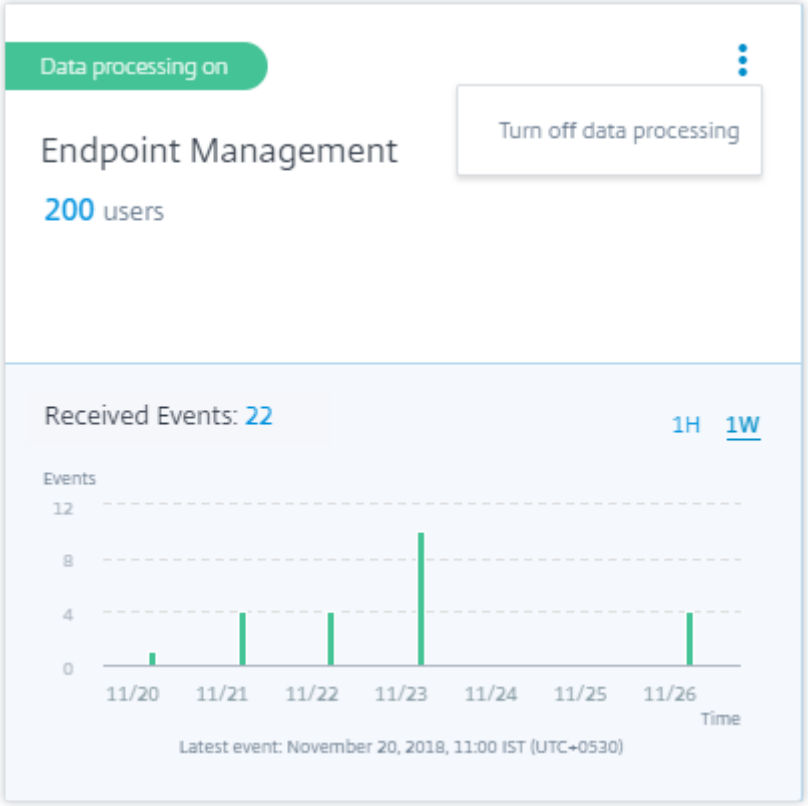
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Aktivieren oder Deaktivieren der Datenverarbeitung

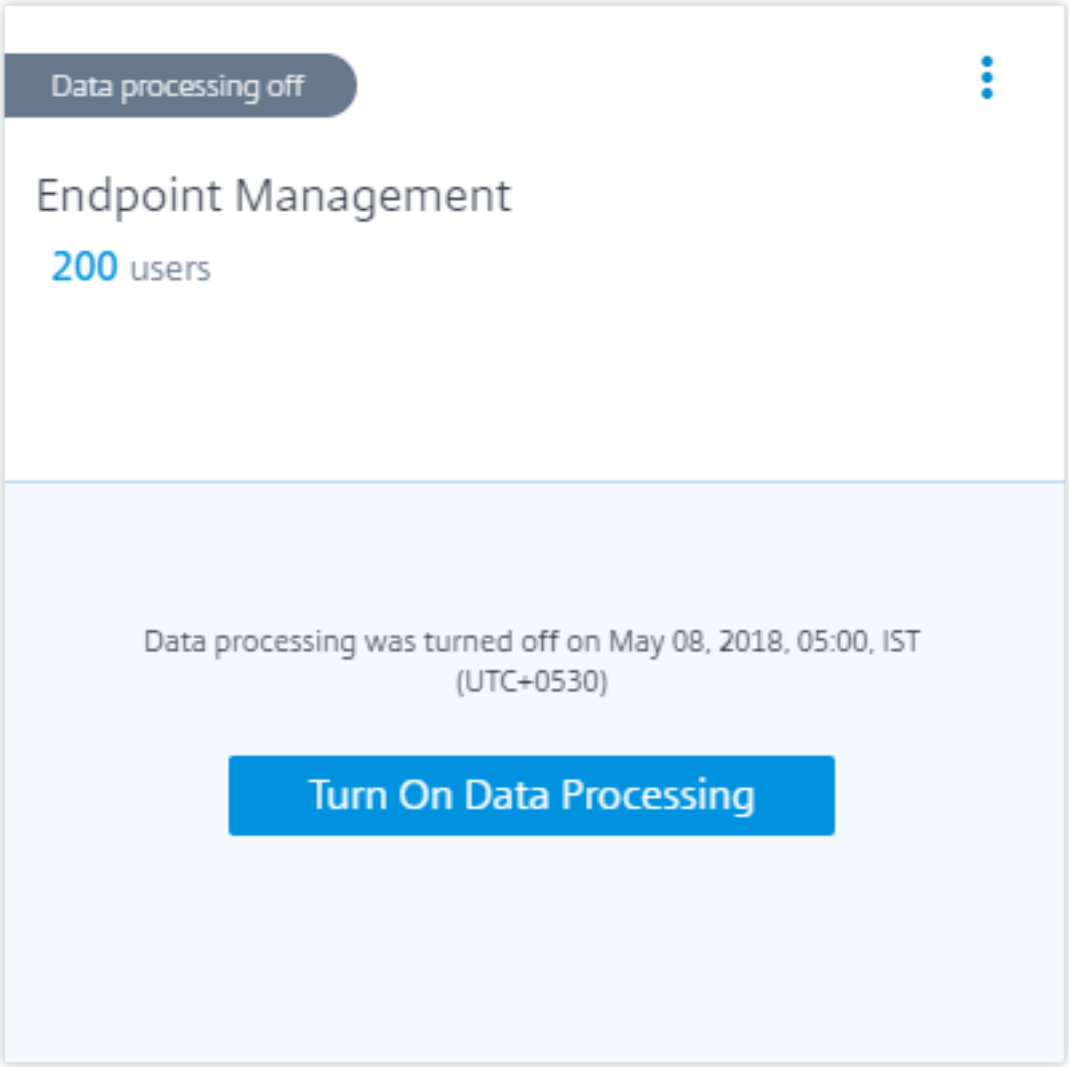
Um die Datenverarbeitung zu beenden, klicken Sie auf die vertikale Ellipse () auf der Standortkarte, und klicken Sie dann auf **Datenverarbeitung ausschalten**. Citrix Analytics beendet die Verarbeitung von Daten für diese Datenquelle.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Um die Datenverarbeitung wieder zu aktivieren, klicken Sie auf **Datenverarbeitung einschalten**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Citrix Gateway (on-premises) -Datenquelle

April 12, 2024

Die **Gateway-Datenquelle** stellt die on-premises Citrix Gateway-Instanzen in Ihrer Umgebung dar. Citrix Analytics erkennt automatisch die Citrix Application Delivery Management (ADM)-Agenten und die Gateway-Instanzen, die dem Citrix ADM Service hinzugefügt wurden.

Wenn Benutzer über Gateway auf Dienste oder Anwendungen zugreifen, empfängt Citrix Analytics die Benutzerzugriffsereignisse in Echtzeit. Die Benutzerereignisse werden verarbeitet, um Sicherheitsbedrohungen zu erkennen.

Informationen zu den Voraussetzungen und den Onboarding-Schritten finden Sie im Citrix Gateway-

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Datenquellenartikel in der Citrix Analytics Analytics-Plattformdokumentation.

Citrix Remote Browser Isolation-Datenquelle

March 22, 2023

Der Citrix Remote Browser Isolation Service isoliert das Surfen im Internet, um das Unternehmensnetzwerk vor browserbasierten Angriffen zu schützen. Er bietet konsistenten, sicheren Remotezugriff auf im Internet gehostete Webanwendungen, ohne dass eine Benutzergerätekonfiguration erforderlich ist.

In Citrix Analytics for Security können Sie die Benutzerereignisse einer veröffentlichten Remote Browser Isolation-Sitzung anzeigen. Weitere Informationen zu den Benutzerereignissen finden Sie unter Self-Service-Suche für Remote Browser Isolation.

Um die Benutzerereignisse aus einer veröffentlichten Remote Browser Isolation-Sitzung zu empfangen, aktivieren Sie die **Hostnamen-Tracking-Richtlinie** in der Remote Browser Isolation. Standardmäßig ist die Richtlinie deaktiviert.

Durch die Aktivierung der **Hostnamen-Tracking-Richtlinie** kann Remote Browser Isolation Hostnamen, die während der Benutzersitzung verwendet wurden, an Citrix Analytics for Security senden. Weitere Informationen finden Sie unter Veröffentlichte Remote-Browser-Isolationen verwalten.

Citrix Secure Private Access-Datenquelle

April 12, 2024

Die **Secure Private Access-Datenquelle** stellt den Citrix Secure Private Access Dienst dar, der Ihrem Citrix Cloud Cloud-Konto zugeordnet ist. Wenn Benutzer diesen Dienst verwenden, empfängt Citrix Analytics die Benutzerzugriffsereignisse (Protokolle) in Echtzeit. Die Benutzerereignisse werden verarbeitet, um Sicherheitsbedrohungen zu erkennen.

Voraussetzungen

- Abonnieren Sie den auf Citrix Cloud angebotenen Citrix Secure Private Access Dienst. Weitere Informationen zu den ersten Schritten finden Sie unter Secure Private Access-Dienst.
- Prüfen Sie die Systemanforderungen und stellen Sie sicher, dass Ihre Umgebung die Anforderungen erfüllt.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

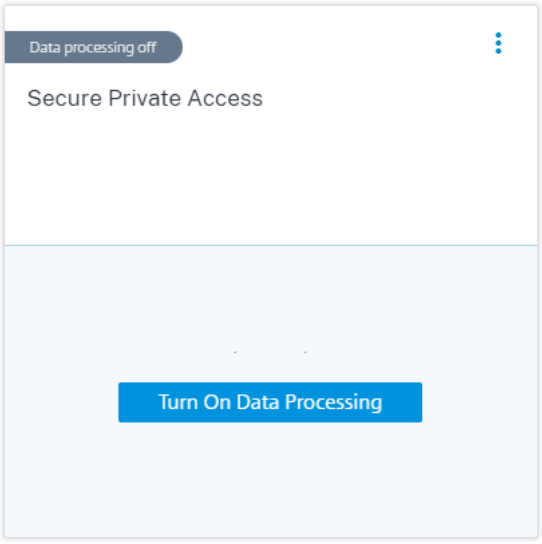
Datenquelle anzeigen und Datenverarbeitung einschalten

Citrix Analytics erkennt automatisch die Secure Private Access-Datenquelle, die Ihrem Citrix Cloud Cloud-Konto zugeordnet ist.

So zeigen Sie die Datenquelle an:

Klicken Sie in der oberen Leiste auf **Einstellungen** > **Datenquellen** > **Sicherheit**.

Auf der Seite **Datenquellen** wird eine Sitekarte für die **Secure Private Access-Datenquelle** angezeigt. Klicken Sie **auf Datenverarbeitung einschalten**, damit Citrix Analytics mit der Verarbeitung von Daten für diese Datenquelle beginnen kann.

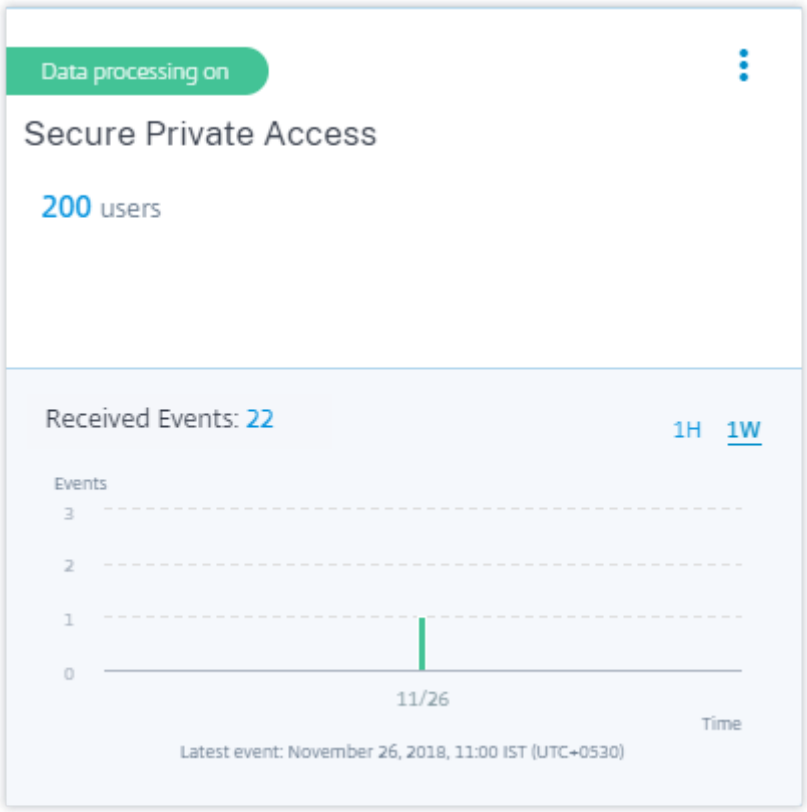


Benutzer und empfangene Ereignisse anzeigen

Die Sitekarte zeigt die Anzahl der aktiven Benutzer und die Ereignisse an, die von der Datenquelle für die letzte Stunde empfangen wurden. Dies ist die Standardzeitauswahl. Sie können auch 1 Woche (1 W) auswählen und die Daten anzeigen.

Klicken Sie auf die Anzahl der Benutzer, um die Benutzerdetails auf der Seite **Benutzer** anzuzeigen. Klicken Sie auf die Anzahl der eingegangenen Ereignisse, um die Ereignissdetails auf der Self-Service-Suchseite anzuzeigen.

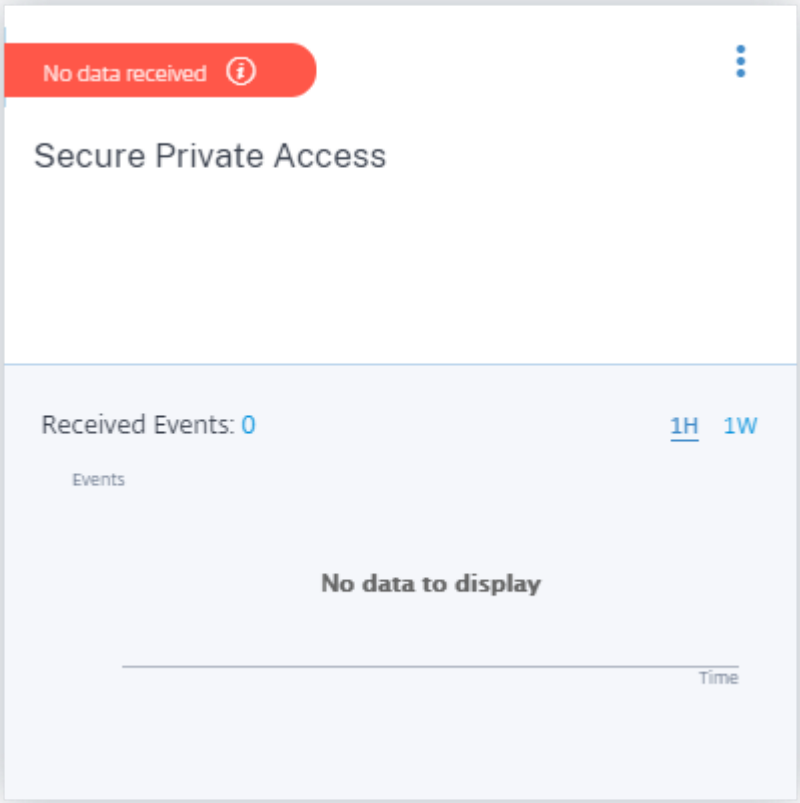
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Nachdem Sie die Datenverarbeitung aktiviert haben, zeigt die Site-Karte möglicherweise den Status **Keine empfangenen Daten** an. Dieser Status wird aus zwei Gründen angezeigt:

1. Wenn Sie die Datenverarbeitung zum ersten Mal aktiviert haben, dauert es eine gewisse Zeit, bis die Ereignisse den Ereignis-Hub in Citrix Analytics erreichen. Wenn Citrix Analytics die Ereignisse empfängt, ändert sich der Status in **Data processing on**. Wenn sich der Status nach einiger Zeit nicht ändert, aktualisieren Sie die Seite **Datenquellen**.
2. Analytics hat in der letzten Stunde keine Ereignisse von der Datenquelle erhalten.

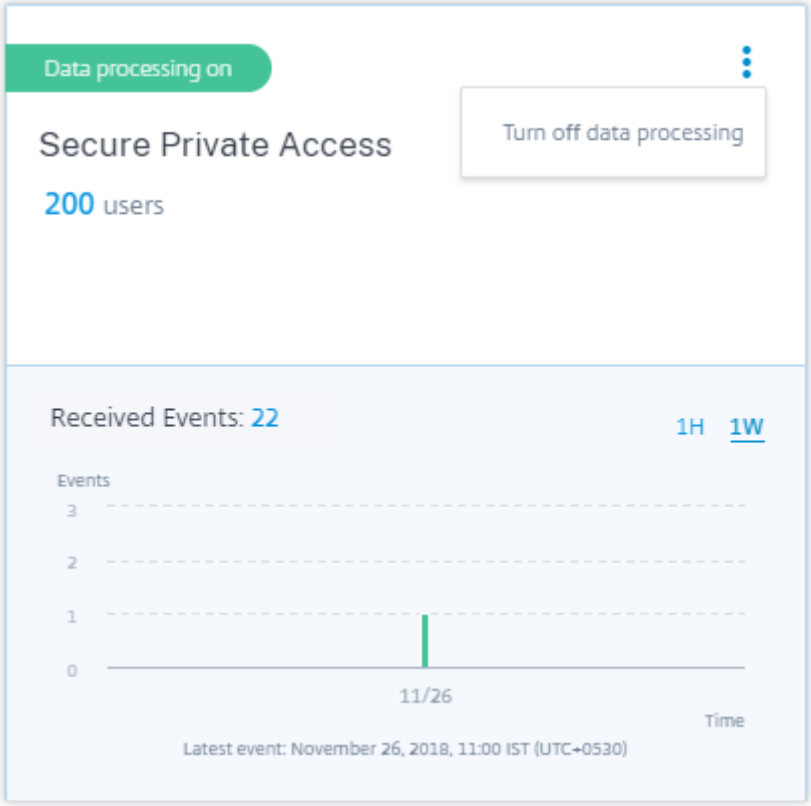
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



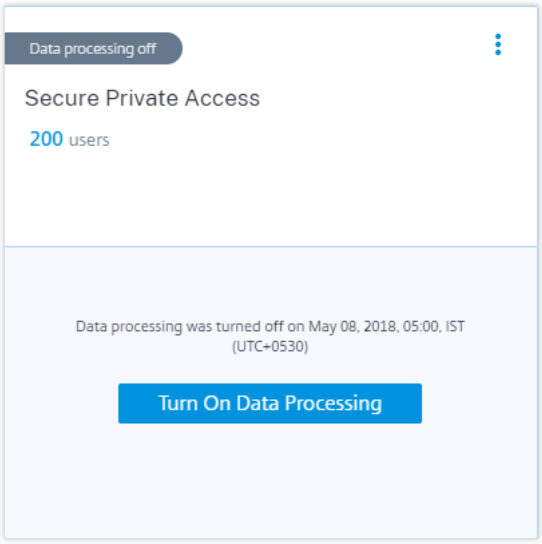
Aktivieren oder Deaktivieren der Datenverarbeitung

Um die Datenverarbeitung zu beenden, klicken Sie auf die vertikale Ellipse () auf der Standortkarte, und klicken Sie dann auf **Datenverarbeitung ausschalten**. Citrix Analytics beendet die Verarbeitung von Daten für diese Datenquelle.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Um die Datenverarbeitung wieder zu aktivieren, klicken Sie auf **Datenverarbeitung einschalten**.



Citrix Virtual Apps and Desktops und Citrix DaaS-Datenquelle

April 12, 2024

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Die Datenquelle **Apps and Desktops** stellt on-premises Citrix Virtual Apps and Desktops und Citrix DaaS (früher Citrix Virtual Apps and Desktops Service) in Ihrer Organisation dar.

Citrix Analytics for Security unterstützt beide Angebote und empfängt Benutzerereignisse von der Datenquelle. Dieser Artikel führt Sie durch die Voraussetzungen und Verfahren, um Analytics für beide Angebote zu aktivieren.

Citrix Analytics for Security empfängt Benutzerereignisse von den folgenden Komponenten der Citrix Virtual Apps and Desktops und der Citrix DaaS-Datenquelle:

- Die Citrix Workspace-App ist auf den Benutzergeräten installiert
- Citrix Director für die On-Premises-Bereitstellung
- Citrix Monitor-Dienst
- Sitzungsaufzeichnungsserver

Die Benutzerereignisse werden in Citrix Analytics for Security in Echtzeit empfangen, wenn Benutzer virtuelle Apps oder virtuelle Desktops verwenden.

Unterstützte Clientversionen

Citrix Analytics empfängt Benutzerereignisse, wenn eine unterstützte Clientversion auf den Benutzerendpunkten verwendet wird. Wenn Benutzer nicht unterstützte Clientversionen verwenden, müssen sie ihre Clients auf eine der folgenden Versionen aktualisieren:

- Citrix Workspace-App für Windows 1907 oder höher
- Citrix Workspace-App für Mac 1910.2 oder höher
- Citrix Workspace-App für HTML5 2007 oder höher
- Citrix Workspace-App für Chrome-Neueste Version im Chrome Web Store verfügbar
- Citrix Workspace-App für Android - Neueste Version in Google Play verfügbar
- Citrix Workspace-App für iOS —neueste Version im Apple App Store verfügbar
- Citrix Workspace-App für Linux 2006 oder höher

Analytics auf Citrix DaaS aktivieren

Voraussetzungen

- Abonnieren Sie Citrix DaaS, das in der Citrix Cloud angeboten wird. Informationen zu den ersten Schritten mit Citrix DaaS finden Sie unter Installieren und Konfigurieren.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Lesen Sie den Abschnitt **Systemanforderungen** und stellen Sie sicher, dass Sie die Anforderungen erfüllen.

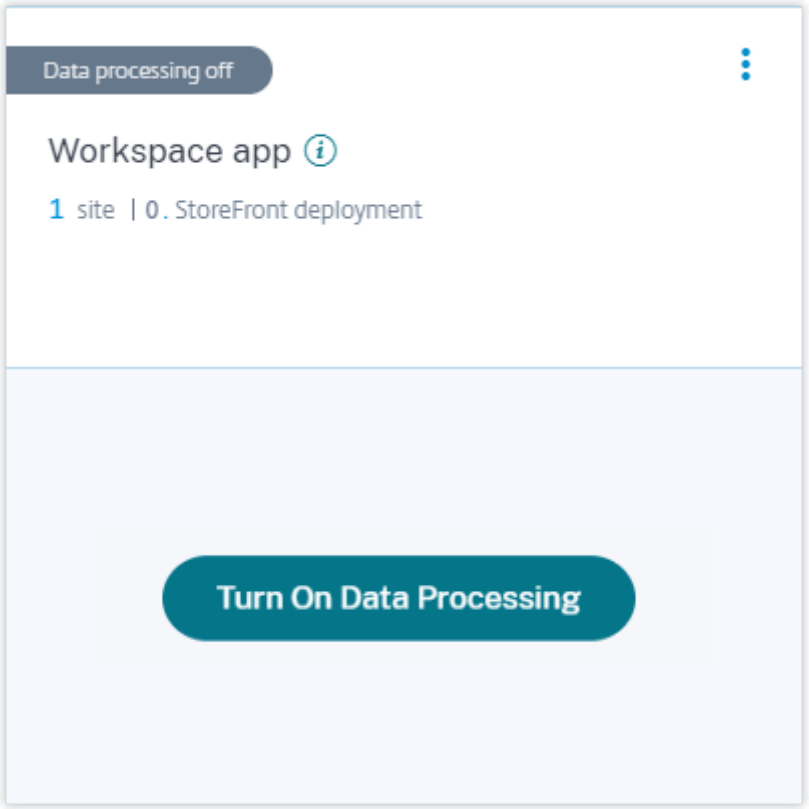
Zeigen Sie die Datenquelle an und schalten Sie die Datenverarbeitung ein

Citrix Analytics erkennt automatisch Citrix DaaS, die mit Ihrem Citrix Cloud-Konto verknüpft sind.

So zeigen Sie die Datenquelle an:

Klicken Sie in der oberen Leiste auf **Einstellungen** > **Datenquellen** > **Sicherheit**.

Die **App-Site-Karte Apps und Desktops** —**Workspace** wird auf der Seite **Datenquellen** angezeigt. Klicken Sie auf **Datenverarbeitung einschalten**, damit Citrix Analytics mit der Verarbeitung von Daten für diese Datenquelle beginnen kann.

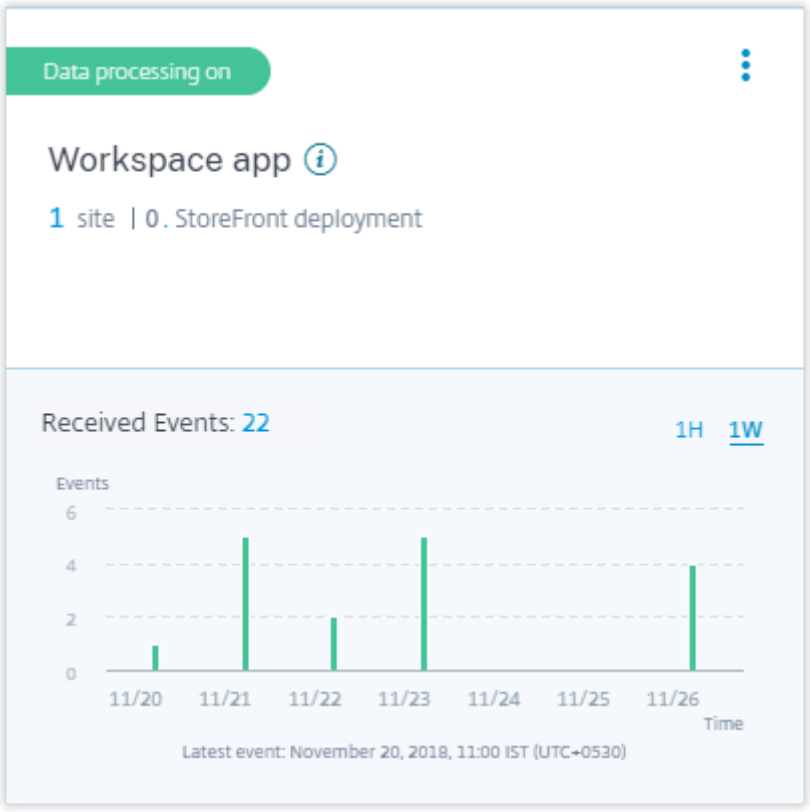


Cloud-Site, Benutzer und empfangene Ereignisse anzeigen

Auf der Sitekarte werden die Anzahl der Apps- und Desktops-Benutzer, die erkannte Cloud-Site und die empfangenen Ereignisse für die letzte Stunde angezeigt. Dies ist die Standardzeitauswahl. Sie können auch 1 Woche (1 W) auswählen und die Daten anzeigen.

Klicken Sie auf die Anzahl der eingegangenen Ereignisse, um die Ereignisse auf der Self-Service-Suchseite anzuzeigen.

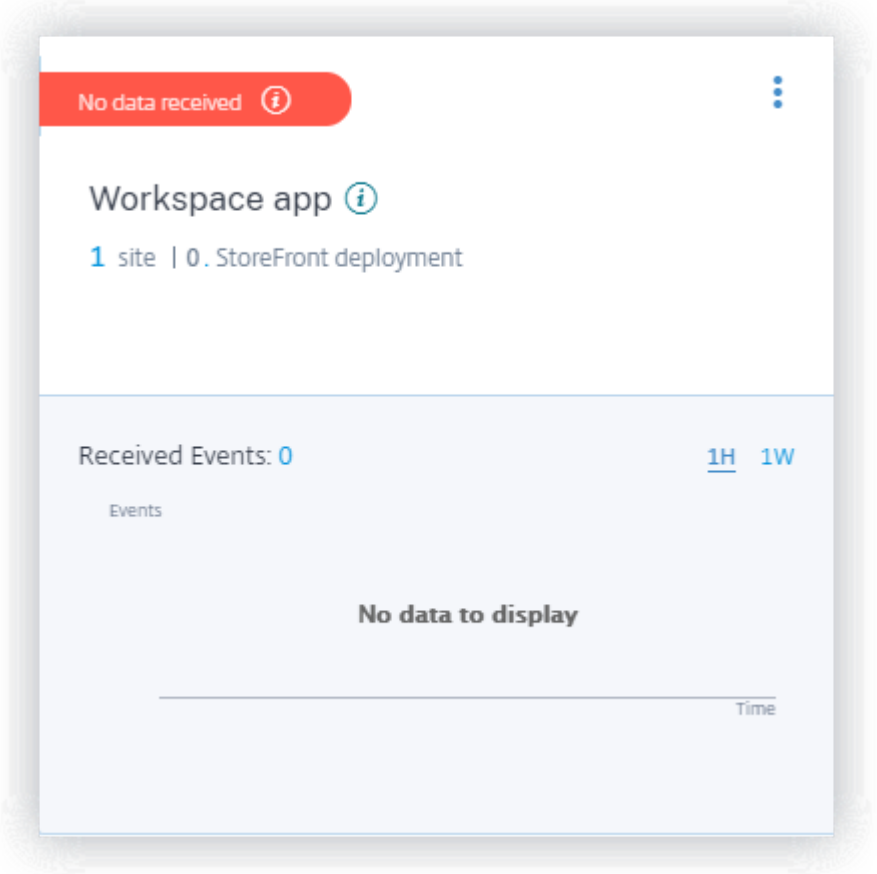
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Nachdem Sie die Datenverarbeitung aktiviert haben, wird auf der Sitekarte möglicherweise der Status **No data received** angezeigt. Dieser Status wird aus zwei Gründen angezeigt:

1. Wenn Sie die Datenverarbeitung zum ersten Mal aktiviert haben, dauert es eine gewisse Zeit, bis die Ereignisse den Ereignis-Hub in Citrix Analytics erreichen. Wenn Citrix Analytics die Ereignisse empfängt, ändert sich der Status in **Data processing on**. Wenn sich der Status nach einiger Zeit nicht ändert, aktualisieren Sie die Seite **Datenquellen**.
2. Analytics hat in der letzten Stunde keine Ereignisse von der Datenquelle erhalten.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Analytics auf on-premises Citrix Virtual Apps and Desktops aktivieren

Citrix Analytics empfängt Benutzerereignisse von on-premises Sites, die zu Workspace hinzugefügt wurden, und Websites, auf die über StoreFront-Bereitstellungen zugegriffen wird

Wenn Ihre Organisation on-premises Websites verwendet, müssen Sie eine der folgenden Methoden verwenden, um Ihre Websites einzubinden, damit Analytics die Websites erkennt:

- Integrieren Sie Ihre on-premises Websites mit StoreFront
- Integrieren Sie Ihre on-premises Websites mithilfe von Workspace

Voraussetzungen

- Sie benötigen eine Lizenz, um die on-premises Citrix Virtual Apps and Desktops verwenden zu können. Informationen zu den ersten Schritten mit Citrix Virtual Apps and Desktops on-premises finden Sie unter Installieren und Konfigurieren.
- Lesen Sie den Abschnitt **Systemanforderungen** und stellen Sie sicher, dass Sie die Anforderungen erfüllen.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Ihr Director ist Version 1912 CU2 oder höher. Weitere Informationen finden Sie in der Featurekompatibilitätsmatrix.
- **Abonnement für Citrix Workspace**. Wenn Sie Ihre Sites zu Citrix Workspace hinzufügen möchten, benötigen Sie ein Workspace-Abonnement.

  Um ein Citrix Workspace-Abonnement zu erwerben, besuchen Sie https://www.citrix.com/products/citrix-workspace/get-started.html und wenden Sie sich an einen Citrix Workspace-Experten, der Ihnen helfen kann.
- **Websites wurden zu Workspace hinzugefügt**. Citrix Analytics erkennt automatisch die Sites, die zu Citrix Workspace hinzugefügt wurden. Fügen Sie Ihre Sites zu Citrix Workspace hinzu, bevor Sie mit dem Onboarding von Citrix Analytics fortfahren. Dieser Prozess wird als **Siteaggregation** bezeichnet.

  Für die Site-Aggregation müssen Sie Cloud Connector installieren, NetScaler Gateway STA-Server für interne und externe Konnektivität zu Workspace-Ressourcen konfigurieren und dann die Standorte zu Workspace hinzufügen. Ausführliche Anweisungen zur Site-Aggregation finden Sie unter Aggregation on-premises virtueller Apps und Desktops in Arbeitsbereichen.
- **StoreFront-Version**. Wenn Sie eine StoreFront-Bereitstellung für Ihre Sites verwenden, stellen Sie sicher, dass die StoreFront-Version 1906 oder höher ist.

Integrieren von Citrix Virtual Apps and Desktops on-premises Sites mit StoreFront

Informationen zu den Voraussetzungen und den Onboarding-Schritten finden Sie im Datenquellartikel Citrix Virtual Apps and Desktops in der Citrix Analytics-Plattformdokumentation.

Onboarding von on-premises Citrix Virtual Apps and Desktops mit Workspace

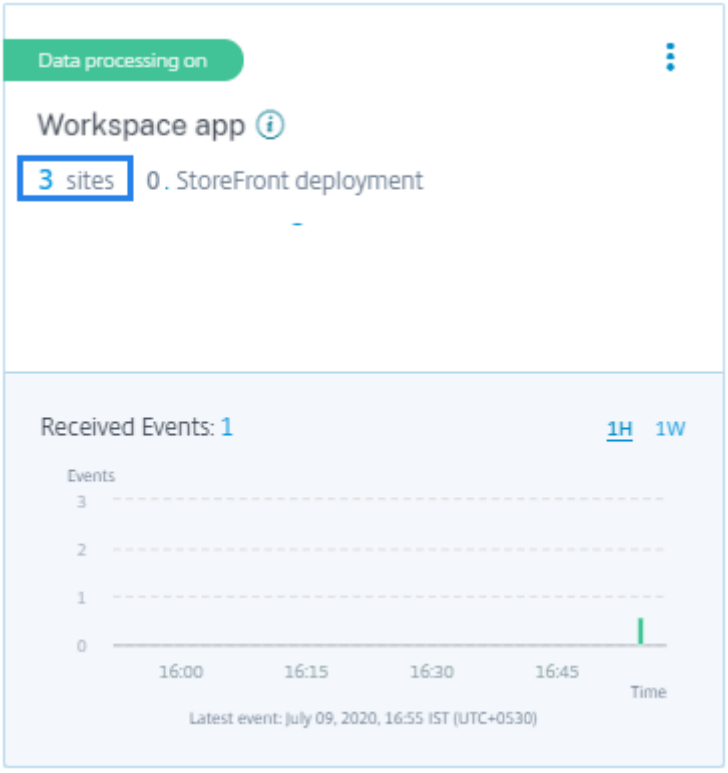
Websites, die bereits zu Citrix Workspace hinzugefügt wurden Citrix Analytics erkennt automatisch die on-premises Sites, die bereits zu Citrix Workspace hinzugefügt wurden, und zeigt sie auf der Datenquell-Site-Karte an.

So zeigen Sie die Datenquelle an:

Klicken Sie in der oberen Leiste auf **Einstellungen** > **Datenquellen** > **Sicherheit**.

Auf der Sitekarte **Apps und Desktops** wird die Anzahl der zu Workspace hinzugefügten Sites und der mit diesen Sites verbundenen Benutzer angezeigt. Klicken Sie auf die Site-Anzahl, um die entdeckten Sites anzuzeigen. Klicken Sie auf die Benutzeranzahl, um die erkannten Benutzer auf der Seite **Benutzer** anzuzeigen.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

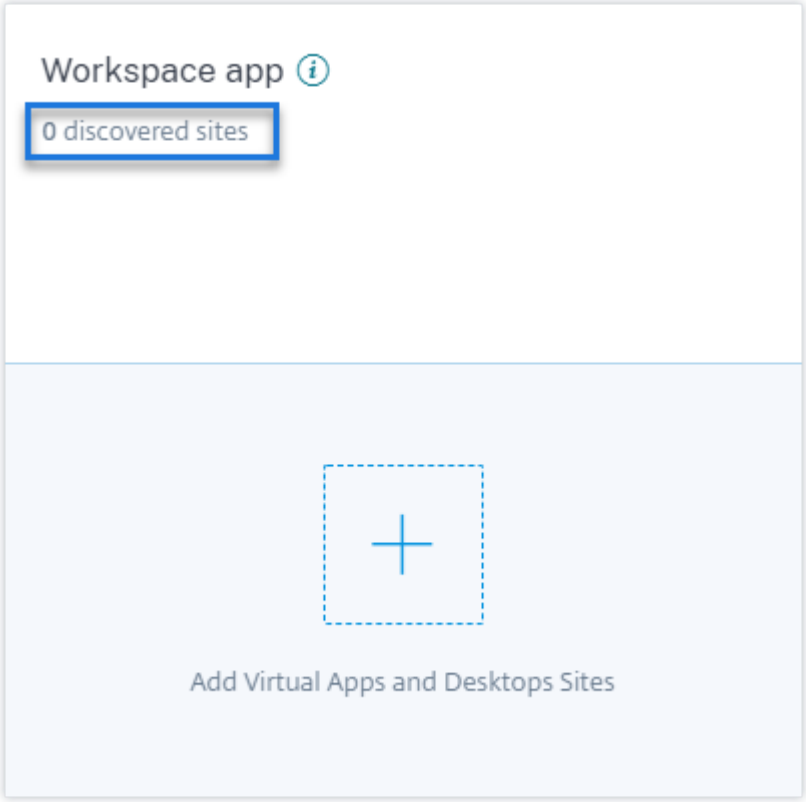


Websites, die nicht zu Citrix Workspace hinzugefügt wurden Wenn Sie Ihre on-premises Websites noch nicht zu Workspace hinzugefügt haben, kann Analytics Ihre Websites nicht erkennen. Die Site-Karte zeigt **0 entdeckte Websites**an.

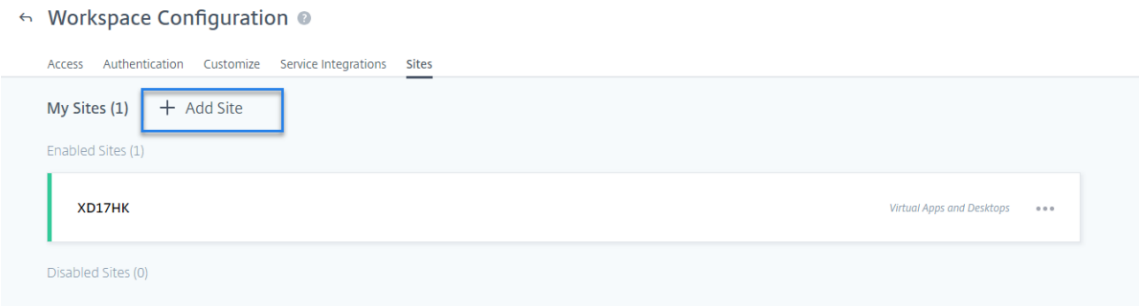
So fügen Sie eine Website zu Workspace hinzu:

1. Klicken Sie auf der Site-Karte auf +.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



2. Klicken Sie auf der Seite **Workspace-Konfiguration** auf **+Site hinzufügen**.

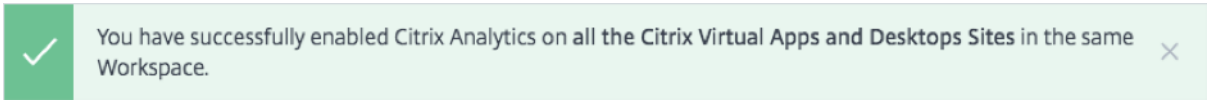


3. Folgen Sie den Anweisungen auf dem Bildschirm, um eine Site hinzuzufügen. Weitere Informationen finden Sie unter Aggregieren on-premises virtueller Apps und Desktops in Arbeitsbereichen.
4. Nachdem Sie die Site hinzugefügt haben, melden Sie sich wieder bei Citrix Analytics an und aktualisieren Sie die Seite **Datenquellen**, um die kürzlich hinzugefügte Site auf der Sitekarte anzuzeigen.

Aktivieren Sie die Datenverarbeitung und sehen Sie empfangene Ereignisse Damit Analytics mit der Verarbeitung von Daten für die erkannten Sites beginnen kann, klicken Sie **auf der Sitekarte auf Datenverarbeitung einschalten** und folgen Sie den Anweisungen auf dem Bildschirm.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

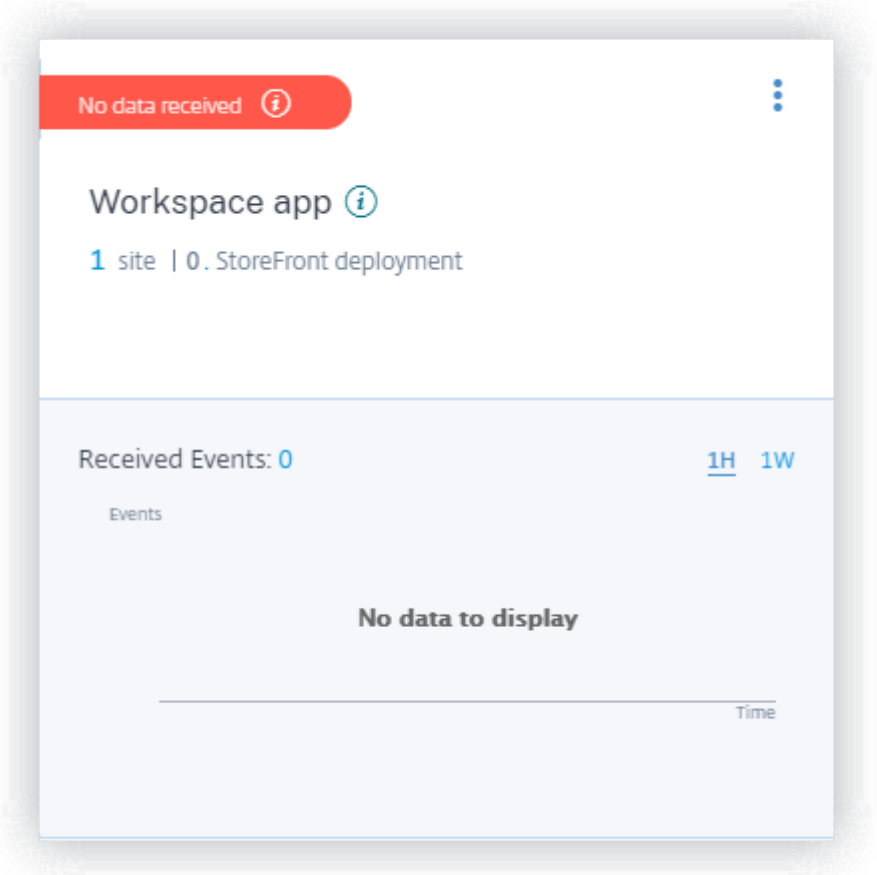
Wenn Sie mehrere Websites zum selben Workspace hinzugefügt haben, verarbeitet und speichert Analytics Daten für alle Websites im Arbeitsbereich. Sie erhalten eine Erfolgsmeldung, wenn Analytics auf allen Ihren Websites erfolgreich aktiviert wurde.



Die Standortkarte zeigt die empfangenen Ereignisse für die letzte Stunde an, was die Standardzeitauswahl ist. Sie können auch 1 Woche (1 W) auswählen und die Daten anzeigen. Klicken Sie auf die Anzahl der empfangenen Ereignisse, um die Ereignisse auf der entsprechenden Self-Service-Suchseite anzuzeigen.

Nachdem Sie die Datenverarbeitung aktiviert haben, wird auf der Sitekarte möglicherweise der Status **No data received** angezeigt. Dieser Status wird aus zwei Gründen angezeigt:

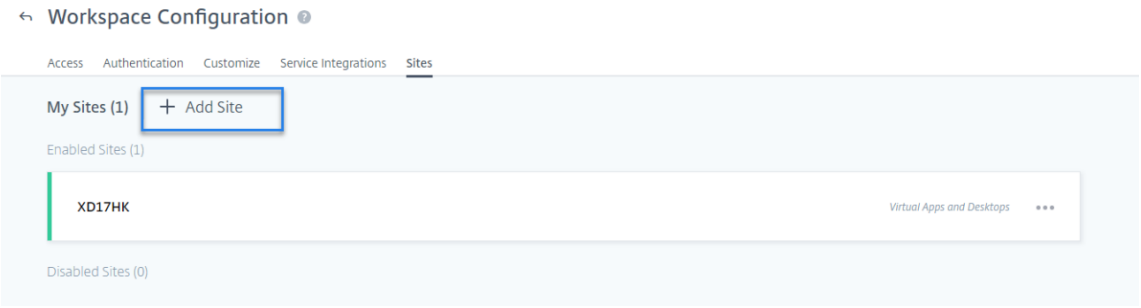
1. Wenn Sie die Datenverarbeitung zum ersten Mal aktiviert haben, dauert es eine gewisse Zeit, bis die Ereignisse den Ereignis-Hub in Citrix Analytics erreichen. Wenn Citrix Analytics die Ereignisse empfängt, ändert sich der Status in **Data processing on**. Wenn sich der Status nach einiger Zeit nicht ändert, aktualisieren Sie die Seite **Datenquellen**.
2. Analytics hat in der letzten Stunde keine Ereignisse von der Datenquelle erhalten.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Eine Seite hinzufügen Wenn Sie eine weitere on-premises Website zu Workspace hinzufügen möchten, können Sie sie aus Analytics hinzufügen:

1. Klicken Sie auf der Workspace-Konfigurationsseite auf **+Site hinzufügen.**



2. Folgen Sie den Anweisungen auf dem Bildschirm, um eine Website hinzuzufügen. Weitere Informationen finden Sie unter Aggregieren on-premises virtueller Apps und Desktops in Arbeitsbereichen.
3. Nachdem Sie die Site hinzugefügt haben, gehen Sie zu Citrix Analytics und aktualisieren Sie die Seite **Datenquellen**, um die kürzlich hinzugefügte Site auf der Sitekarte anzuzeigen.

Verbinden Sie sich mit Citrix Director für on-premises Sites

Citrix Director ist eine Konsole für Überwachung und Fehlerbehebung für Citrix Virtual Apps and Desktops. Sie können Director verwenden, um Ihre on-premises Sites für Citrix Analytics for Security (Security Analytics) zu konfigurieren. Nachdem die Sites konfiguriert wurden, sendet Director Überwachungsereignisse an Security Analytics.

Wenn Sie Citrix DaaS verwenden, sendet der Citrix Monitor-Dienst Ereignisse von Ihrer Cloud-Site an Security Analytics.

In einer Hybridumgebung, in der Sie sowohl Cloud- als auch on-premises Bereitstellungen haben, empfängt Security Analytics Ereignisse vom Citrix Monitor-Dienst und den in Citrix Director integrierten Sites.

Voraussetzung und Konfigurationsschritte

> **Hinweise**
>
> - Derzeit zeigt die Director-Benutzeroberfläche die Konfigurationsschritte an, die sich auf Citrix Analytics for Performance (Performance Analytics) beziehen. Diese Konfigurationsschritte gelten auch für Citrix Analytics for Security (Security Analytics). Wenn Sie über eine aktive Citrix Cloud-Berechtigung für Security Analytics verfügen, können Sie eine Verbindung zu Citrix Director herstellen, indem Sie diese Schritte ausführen.

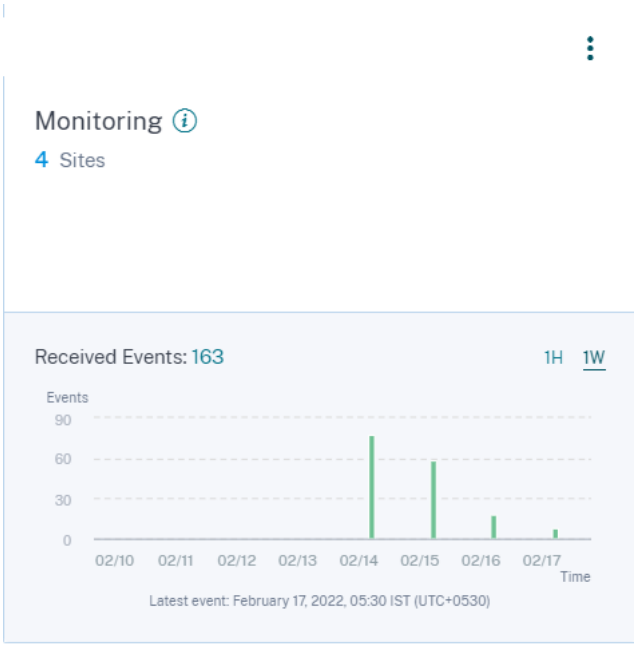
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Wenn Ihr Citrix Cloud-Konto über aktive Berechtigungen sowohl für Sicherheitsanalysen als auch für Performance Analytics verfügt und Sie Ihre Site bereits für Performance Analytics konfiguriert haben, müssen Sie Director nicht erneut für Security Analytics konfigurieren.

Informationen zu den Voraussetzungen und Konfigurationsschritten finden Sie in der Dokumentation zu Citrix Analytics for Performance.

Zeigen Sie Ihre verbundenen Websites und empfangene Ereignisse an

1. Wechseln Sie in Citrix Analytics zur Seite **Datenquellen** .
2. Klicken Sie auf die Registerkarte **Sicherheit**.
3. Auf der Site-Karte **Apps und Desktops** —**Überwachung** können Sie Ihre lokalen Sites oder die Cloud-Site (je nachdem, was zutreffend ist) anzeigen. Sie sehen auch die Ereignisse, die von den Websites empfangen wurden.



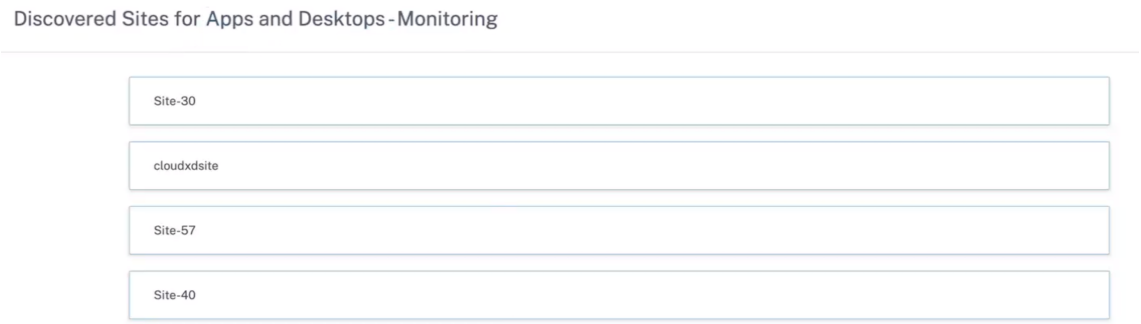
Hinweise

- Wenn Sie zum ersten Mal einen on-premises Standort in Director konfigurieren, kann es einige Zeit dauern (etwa eine Stunde), bis Ereignisse von der Site verarbeitet werden. Dies führt zu einer Verzögerung bei der Anzeige der verbundenen Site auf der Karte **Apps und Desktops** —**Überwachung** der Site.
- Auf der Monitor-Site-Karte ist die Datenverarbeitung für den Monitor-Dienst oder die Director-Datenquelle standardmäßig aktiviert. Sie können die Datenverarbeitung auch je nach Anforderung ausschalten. Es wird jedoch empfohlen, die Datenverar-

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> beitung beizubehalten, um den größtmöglichen Nutzen aus Security Analytics zu ziehen.

4. Klicken Sie auf die Website, um die Details anzuzeigen.



Verbinden mit der Sitzungsaufzeichnungsbereichstellung

Mit derSitzungsaufzeichnung können Sie die Bildschirmaktivität jeder Benutzersitzung in Citrix Virtual Apps and Desktops und Citrix DaaS aufzeichnen. Sie können die Sitzungsaufzeichnungsserver so konfigurieren, dass die Benutzerereignisse an Citrix Analytics for Security gesendet werden. Die Benutzerereignisse werden verarbeitet, um umsetzbare Einblicke in das riskante Verhalten der Benutzer zu erhalten.

Voraussetzungen

Bevor Sie beginnen, stellen Sie Folgendes sicher:

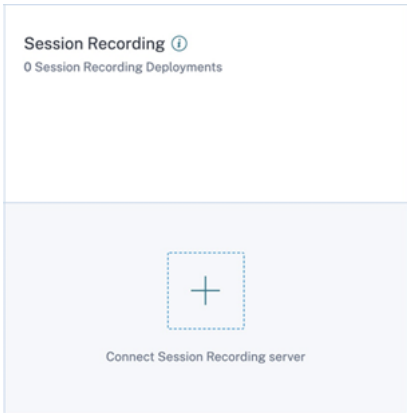
- Ihr Sitzungsaufzeichnungsserver und der VDA-Agent müssen 2103 oder höher sein.
- Der Sitzungsaufzeichnungsserver muss in der Lage sein, eine Verbindung zu den erforderlichen Adressen herzustellen. Weitere Informationen zu den URLs finden Sie unter Netzwerkanforderungen.
- Für die Sitzungsaufzeichnungsbereitstellung muss Port 443 für ausgehende Internetverbindungen geöffnet sein. Alle Proxyserver im Netzwerk müssen diese Kommunikation mit Citrix Analytics für Sicherheit zulassen.
- Wenn Sie Citrix Virtual Apps and Desktops 7 1912 LTSR verwenden, ist die unterstützte Version der Sitzungsaufzeichnung 2103 oder höher.

> **Hinweis:**
>
> Stellen Sie sicher, dass Sie die zusätzlichen Konnektivitätsanforderungen überprüfen, während Sie den **Sitzungsaufzeichnungsdienst** verwenden.

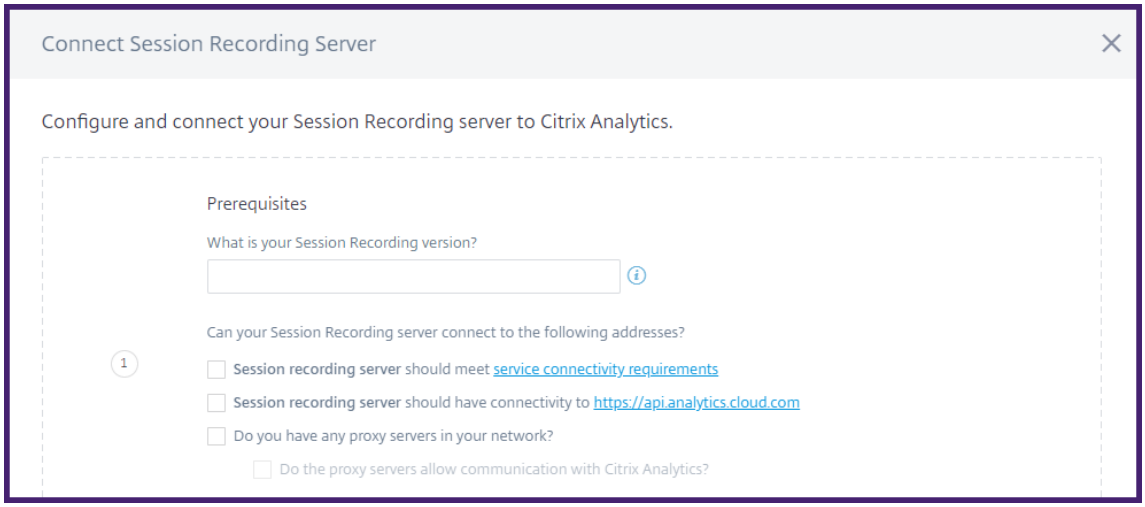
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Konfigurieren Sie Ihren Sitzungsaufzeichnungsserver

1. Klicken Sie auf der Sitekarte **Apps und Desktops** —**Sitzungsaufzeichnung** auf **Sitzungsaufzeichnungsserver verbinden**.



2. Überprüfen Sie auf der Seite **Connect Session Recording Server** die Checkliste und wählen Sie alle erforderlichen Anforderungen aus. Wenn Sie keine zwingende Anforderung auswählen, ist die Option Datei herunterladen deaktiviert.



3. Wenn Sie Proxyserver in Ihrem Netzwerk haben, geben Sie die Proxyadresse in der Datei *SsRecStorageManager.exe.config* auf Ihrem Sitzungsaufzeichnungsserver ein.

   Die Konfigurationsdatei befindet sich unter `<Session Recording Server installation path>\bin\SsRecStorageManager.exe.config`

   Beispiel: `C:\Program Files\Citrix\SessionRecording\Server\Bin\SsRecStorageMana.exe.config`

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

4. Klicken Sie auf **Datei herunterladen**, um die *SessionRecordingConfigurationFile.json-Datei* herunterzuladen.

   > **Hinweis**
   >
   > Die Datei enthält sensible Informationen. Bewahren Sie die Datei an einem sicheren Speicherort auf.

5. Kopieren Sie die Datei auf den Sitzungsaufzeichnungsserver, den Sie mit Citrix Analytics für Sicherheit verbinden möchten.
6. Wenn Ihre Bereitstellung mehrere Sitzungsaufzeichnungsserver umfasst, müssen Sie die Datei auf jeden Server kopieren, den Sie verbinden möchten, und die Schritte zur Konfiguration jedes Servers ausführen.
7. Führen Sie auf dem Sitzungsaufzeichnungsserver den folgenden Befehl aus, um die Einstellungen zu importieren:

   ```
   <Session Recording Server installation path>\bin\SsRecUtils.exe -
       Import_SRCasConfigurations <configuration file path>
   ```

   Beispiel:

   ```
   C:\Program Files\Citrix\SessionRecording\Server\bin\ SsRecUtils.
   exe -Import_SRCasConfigurations C:\Users\administrator \Downloads
   \SessionRecordingConfigurationFile.json
   ```

8. Starten Sie die folgenden Dienste neu:

   - Analysedienst der Citrix Sitzungsaufzeichnung
   - Citrix Speichermanager der Sitzungsaufzeichnung

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

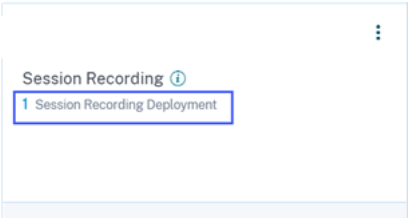
9. Rufen Sie nach erfolgreicher Konfiguration Citrix Analytics für Sicherheit auf, um den verbundenen Sitzungsaufzeichnungsserver anzuzeigen. Klicken Sie **auf Datenverarbeitung einschalten**, damit Citrix Analytics for Security die Daten verarbeiten kann.

> **Hinweis**
>
> Wenn Sie den Sitzungsaufzeichnungsserver der Version 2103 oder 2104 verwenden, müssen Sie zuerst eine Apps- und Desktop-Sitzung starten, um den verbundenen Sitzungsaufzeichnungsserver in Citrix Analytics for Security anzuzeigen. Andernfalls wird der verbundene Sitzungsaufzeichnungsserver nicht angezeigt. Diese Anforderung gilt nicht für den Sitzungsaufzeichnungsserver Version 2106 und höher.

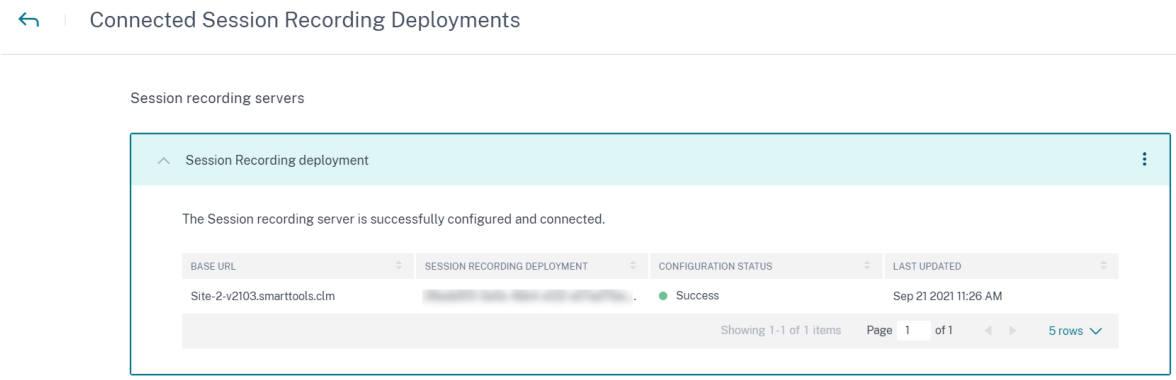
Anzeigen der verbundenen Bereitstellungen

Die Serverbereitstellungen werden nur dann auf der Sitekarte der Sitzungsaufzeichnung angezeigt, wenn die Konfiguration erfolgreich war. Die Sitekarte zeigt die Anzahl der konfigurierten Server an, die Verbindungen mit Citrix Analytics for Security hergestellt haben.

Wenn Sie Ihre Sitzungsaufzeichnungsserver auch nach erfolgreicher Konfiguration nicht sehen, lesen Sie den Artikel zur Fehlerbehebung.



Klicken Sie auf der Sitekarte auf die Anzahl der Bereitstellungen, um die verbundenen Servergruppen mit Citrix Analytics for Security anzuzeigen. Beispiel: Klicken Sie auf **1 Sitzungsaufzeichnungsbereitstellung**, um den verbundenen Server oder die Servergruppen anzuzeigen. Jeder Sitzungsaufzeichnungsserver wird durch eine Basis-URL und eine ServerGroupID dargestellt.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Anzeigen empfangener Ereignisse

Auf der Sitekarte werden die verbundenen Sitzungsaufzeichnungsbereitstellungen und die Ereignisse angezeigt, die in der letzten Stunde von diesen Bereitstellungen empfangen wurden. Dies ist die Standardzeitauswahl. Sie können auch 1 Woche (1 W) auswählen und die Daten anzeigen. Klicken Sie auf die Anzahl der empfangenen Ereignisse, um die Ereignisse auf der Self-Service-Suchseite anzuzeigen.

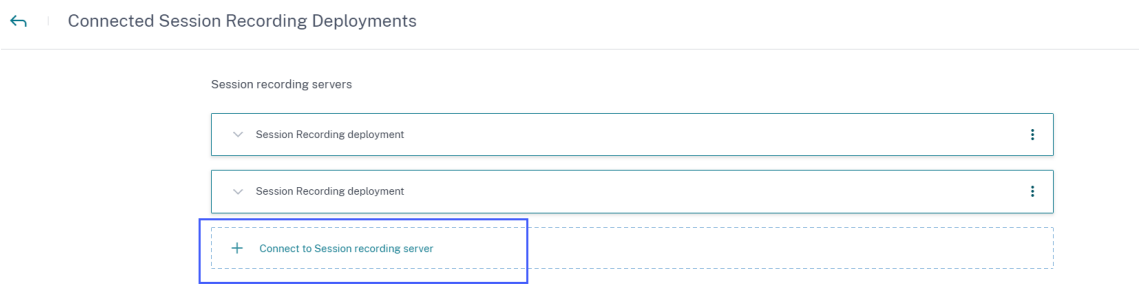
Nachdem Sie die Datenverarbeitung aktiviert haben, wird auf der Sitekarte möglicherweise der Status **No data received** angezeigt. Dieser Status wird aus zwei Gründen angezeigt:

1. Wenn Sie die Datenverarbeitung zum ersten Mal aktiviert haben, dauert es eine gewisse Zeit, bis die Ereignisse den Ereignis-Hub in Citrix Analytics erreichen. Wenn Citrix Analytics die Ereignisse empfängt, ändert sich der Status in **Data processing on**. Wenn sich der Status nach einiger Zeit nicht ändert, aktualisieren Sie die Seite "Data Sources".
2. Citrix Analytics hat in der letzten Stunde keine Ereignisse von der Datenquelle empfangen.

Hinzufügen von Sitzungsaufzeichnungsservern

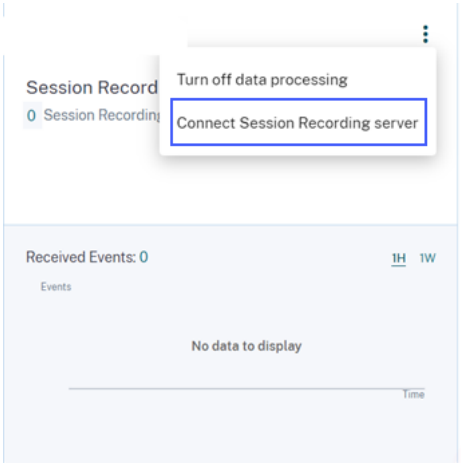
Um einen Sitzungsaufzeichnungsserver hinzuzufügen, führen Sie einen der folgenden Schritte aus:

- Klicken Sie auf der Seite **Connected Session Recording Deployments** auf **Connect to Session recording server**.



- Klicken Sie auf der Sitekarte **Apps und Desktops** —**Sitzungsaufzeichnung** auf die vertikalen Auslassungszeichen (⋮), und wählen Sie dann **Sitzungsaufzeichnungsserver verbinden** aus.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

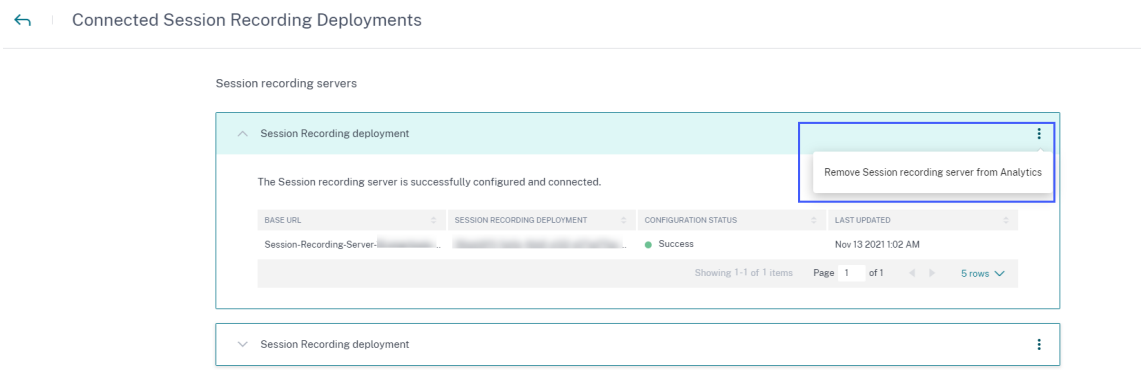


Führen Sie die Schritte zum Herunterladen der Konfigurationsdatei und zum Konfigurieren eines Sitzungsaufzeichnungsservers aus.

Entfernen von Sitzungsaufzeichnungsservern

So entfernen Sie einen Sitzungsaufzeichnungsserver:

1. Navigieren Sie in Citrix Analytics für Sicherheit zur Seite **Connected Session Recording Deployments** und wählen Sie die Serverbereitstellung aus, die Sie entfernen möchten.
2. Klicken Sie auf die vertikalen Auslassungspunkte (⋮) und wählen Sie **Remove Session Recording server from Analytics** aus.



3. Führen Sie auf dem Sitzungsaufzeichnungsserver, den Sie aus Citrix Analytics entfernt haben, den folgenden Befehl aus:

```
<Session Recording Server installation path>\bin\SsRecUtils.exe -
    Remove_SRCasConfigurations
```

Beispiel:

```
C:\Program Files\Citrix\SessionRecording\Server\bin\ SsRecUtils.
exe -Remove_SRCasConfigurations
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Drucktelemetrie für Citrix DaaS aktivieren

Wenn Benutzer Druckaufträge in Citrix DaaS (ehemals Citrix Virtual Apps and Desktops Service) ausführen, können Sie die Protokolle zu diesen Druckaufträgen in Citrix Analytics for Security anzeigen. Diese Druckprotokolle liefern wichtige Informationen über die Druckaktivitäten wie Druckernamen, Druckdateinamen und die Gesamtzahl der gedruckten Exemplare.

> **Hinweis**
>
> Diese Funktion wird nur für Citrix DaaS unterstützt.

In Citrix Analytics for Security können Sie auf der Seite **Suchen** die Datenquelle **Apps and Desktops** auswählen, um die Druckprotokolle anzuzeigen. Als Sicherheitsadministrator können Sie diese Protokolle zur Risikoanalyse und Untersuchung Ihrer Benutzer verwenden.

In der Standardeinstellung ist die Funktion "Drucktelemetrie", bei der diese Druckprotokolle erfasst und übertragen werden, auf den Virtual Delivery Agents (VDAs) deaktiviert.

Um die Drucktelemetrie und die Übertragung von Druckprotokollen an Citrix Analytics for Security zu ermöglichen, müssen Sie Registrierungsschlüssel erstellen und Ihren VDA konfigurieren.

> **Wichtig**
>
> Diese Konfiguration gilt nur für die Windows-VDAs.

Voraussetzungen

- Ihre VDA-Version muss mit der Basisversion für Citrix Virtual Apps and Desktops 7 2203 LTSR oder höher übereinstimmen. Weitere Informationen finden Sie unter Basiskomponenten für Citrix Virtual Apps and Desktops 7 2203.
- Sie benötigen volle Zugriffsberechtigungen, um die Aktualisierungen des Registrierungsschlüssels durchführen zu können.

Drucktelemetrie in energieverwalteten Maschinen aktivieren

Zu den energieverwalteten Maschinen gehören virtuelle Maschinen oder Blade-PCs mit den folgenden Szenarien:

- Bestehendes Masterimage
- Neues Masterimage

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Aktivieren der Drucktelemetrie für ein vorhandenes Masterimage, bei dem die VDA-Version niedriger als die von Citrix Virtual Apps and Desktops 7 2203 LTSR ist

1. Melden Sie sich bei der VDA-Master-Maschine an und erstellen Sie einen Snapshot des aktuellen Status.
2. Aktivieren Sie Druckdienstprotokolle, indem Sie die folgenden Registrierungsschlüssel hinzufügen:

   - Microsoft-Windows-PrintService/Operational
   - ShowJobTitleInEventLogs

   Weitere Informationen zu den Registrierungsschlüsseln finden Sie unter Erstellen von Registrierungsschlüsseln.
3. Aktualisieren Sie den VDA auf eine Basisversion für Citrix Virtual Apps and Desktops 7 2203 LTSR oder höher. Weitere Informationen finden Sie unter Basiskomponenten für Citrix Virtual Apps and Desktops 7 2203.
4. Schalten Sie das Gerät aus und machen Sie eine Momentaufnahme des aktuellen Status.
5. Melden Sie sich bei Citrix Cloud an. Wählen Sie den Maschinenkatalog aus, klicken Sie auf **Maschinen aktualisieren** und folgen Sie den Anweisungen auf dem Bildschirm. Weitere Informationen finden Sie unter Erstellen von Maschinenkatalogen.
6. 24 Stunden warten. Die Konfiguration wird automatisch innerhalb von 24 Stunden übertragen. Wenn die Konfiguration bereits abgeschlossen ist, müssen Sie nicht warten.
7. Starten Sie eine Desktopsitzung mit der Citrix Workspace-App. Alle ausgelösten Druckereignisse, die den Clientdrucker verwenden, sind auf der Seite **Suchen** in Citrix Analytics for Security sichtbar.

Aktivieren Sie die Drucktelemetrie für ein vorhandenes Masterimage, bei dem die VDA-Version mit Citrix Virtual Apps and Desktops 7 2203 LTSR oder höher identisch ist **Option 1**: Fügen Sie die Druckregistrierungsschlüssel im Master-VDA hinzu und aktualisieren Sie virtuelle Desktops.

1. Melden Sie sich bei der VDA-Master-Maschine an und erstellen Sie einen Snapshot des aktuellen Status.
2. Aktivieren Sie Druckdienstprotokolle, indem Sie die folgenden Registrierungsschlüssel hinzufügen:

   - Microsoft-Windows-PrintService/Operational
   - ShowJobTitleInEventLogs

   Weitere Informationen zu den Registrierungsschlüsseln finden Sie unter Erstellen von Registrierungsschlüsseln.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

3. Schalten Sie die VDA-Maschine aus und erstellen Sie einen Snapshot des neuesten Status.
4. Melden Sie sich bei Citrix Cloud an, wählen Sie den Maschinenkatalog aus, klicken Sie auf **Maschinen aktualisieren**und folgen Sie den Anweisungen auf dem Bildschirm.
5. Starten Sie eine Desktopsitzung mit der Citrix Workspace-App. Alle ausgelösten Druckereignisse, die den Clientdrucker verwenden, sind auf der Seite **Suchen** in Citrix Analytics for Security sichtbar.

Option 2: Verschieben des virtuellen Desktops in die Organisationseinheit (OU) und Erstellen von Registrierungsschlüsseln über GPOs

> **Hinweis**
>
> Die Option 2-Methode funktioniert nur für statische Maschinen. Für zufällige Maschinen müssen Sie der Methode Option 1 folgen (wie oben erwähnt).

1. Melden Sie sich bei der Domänencontroller-Maschine an.
2. Aktivieren Sie Druckdienstprotokolle, indem Sie die folgenden Registrierungsschlüssel hinzufügen:

   - Microsoft-Windows-PrintService/Operational
   - ShowJobTitleInEventLogs

   Weitere Informationen zu den Registrierungsschlüsseln finden Sie unter Erstellen von Registrierungsschlüsseln.

> **Hinweis**
>
> In jedem Domänencontroller ist das Erstellen der Registrierungsschlüssel eine einmalige Aufgabe.

1. Starten Sie die VDA-Maschine von Citrix Cloud aus neu.
2. Starten Sie eine Desktopsitzung mit der Citrix Workspace-App. Alle ausgelösten Druckereignisse, die den Clientdrucker verwenden, sind auf der Seite **Suchen** in Citrix Analytics for Security sichtbar.

Drucktelemetrie in einem neuen Masterimage aktivieren

1. Erstellen Sie eine virtuelle Maschine (VM) mithilfe des Verwaltungstools des Hypervisors. Diese VM wird als Master-VDA behandelt.
2. Stellen Sie sicher, dass der Master-VDA zur erforderlichen Domäne hinzugefügt wurde.
3. Melden Sie sich beim Master-VDA an und aktivieren Sie die Druckdienstprotokolle, indem Sie die folgenden Registrierungsschlüssel hinzufügen:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Microsoft-Windows-PrintService/Operational
- ShowJobTitleInEventLogs

Weitere Informationen finden Sie unter Erstellen von Registrierungsschlüsseln.

4. Installieren Sie die VDA-Version für Citrix Virtual Apps and Desktops 7 2203 LTSR oder höher. Wählen Sie bei der Installation des VDA die Option **Master Image**. Weitere Informationen finden Sie unter Basiskomponenten für Citrix Virtual Apps and Desktops 7 2203.
5. Stellen Sie sicher, dass die Hosting-Verbindung zu Citrix Cloud hinzugefügt wurde. Weitere Informationen finden Sie unter Erstellen von Maschinenkatalogen.
6. Erstellen Sie einen Maschinenkatalog mithilfe des Masterimages. Weitere Informationen finden Sie unter Erstellen von Maschinenkatalogen.
7. Erstellen Sie eine Bereitstellungsgruppe und fügen den Maschinenkatalog hinzu. Weitere Informationen finden Sie unter Bereitstellungsgruppen erstellen.
8. 24 Stunden warten. Die Konfiguration wird automatisch innerhalb von 24 Stunden von der Gruppenrichtlinien-Engine übertragen.
9. Starten Sie eine Desktopsitzung mit der Citrix Workspace-App. Alle ausgelösten Druckereignisse, die den Clientdrucker verwenden, sind auf der Seite **Suchen** in Citrix Analytics for Security sichtbar.

Drucktelemetrie auf Maschinen aktivieren, die nicht mit Strom verwaltet werden

Zu den Maschinen ohne Energieverwaltung gehören physische Computer mit den folgenden Szenarien:

- Bestehender physischer VDA
- Neuer physischer VDA

Aktivieren der Drucktelemetrie für einen vorhandenen physischen VDA, bei dem die VDA-Version niedriger als die von Citrix Virtual Apps and Desktops 7 2203 LTSR ist

1. Aktivieren Sie Druckdienstprotokolle, indem Sie die folgenden Registrierungsschlüssel hinzufügen:

   - Microsoft-Windows-PrintService/Operational
   - ShowJobTitleInEventLogs

   Weitere Informationen finden Sie unter Erstellen von Registrierungsschlüsseln.

2. Aktualisieren Sie den VDA auf eine Basisversion für Citrix Virtual Apps and Desktops 7 2203 LTSR oder höher. Weitere Informationen finden Sie unter Basiskomponenten für Citrix Virtual Apps and Desktops 7 2203.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

3. 24 Stunden warten. Die Konfiguration wird automatisch innerhalb von 24 Stunden übertragen. Wenn die Konfiguration bereits abgeschlossen ist, müssen Sie nicht warten.
4. Starten Sie eine Desktopsitzung mit der Citrix Workspace-App. Alle ausgelösten Druckereignisse, die den Clientdrucker verwenden, sind auf der Seite **Suchen** in Citrix Analytics for Security sichtbar.

Drucktelemetrie für einen neuen physischen VDA aktivieren

1. Erstellen Sie eine physische VM und ändern Sie die Domäne in den erforderlichen Domainnamen.
2. Melden Sie sich bei der VM an und aktivieren Sie die Druckdienstprotokolle, indem Sie die folgenden Registrierungsschlüssel hinzufügen:

   - Microsoft-Windows-PrintService/Operational
   - ShowJobTitleInEventLogs

   Weitere Informationen finden Sie unter Erstellen von Registrierungsschlüsseln.
3. Installieren Sie die VDA-Version für Citrix Virtual Apps and Desktops 7 2203 LTSR oder höher. Wählen Sie bei der Installation von VDA die Option Remote-PC-Zugriff aus.
4. Erstellen Sie einen Maschinenkatalog. Weitere Informationen finden Sie unter Erstellen von Maschinenkatalogen.

   > **Hinweis:**
   >
   > Die Maschinenverwaltung muss als **Maschinen ausgewählt werden, die nicht mit Energie verwaltet werden (z. B. physische Maschinen)**.

5. Erstellen Sie eine Bereitstellungsgruppe und fügen den Maschinenkatalog hinzu. Weitere Informationen finden Sie unter Bereitstellungsgruppen erstellen.
6. 24 Stunden warten. Die Konfiguration wird automatisch innerhalb von 24 Stunden von der Gruppenrichtlinien-Engine übertragen.
7. Starten Sie eine Desktopsitzung mit der Citrix Workspace-App. Alle ausgelösten Druckereignisse, die den Clientdrucker verwenden, sind auf der Seite **Suchen** in Citrix Analytics for Security sichtbar.

Erstellen Sie Registrierungsschlüssel

Führen Sie in Ihrem VDA eine der folgenden Optionen aus:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Erstellen Sie Registrierungsschlüssel manuell. Verwenden Sie diese Methode für Master-VDAs und eine geringere Anzahl physischer VDAs in Ihrer Bereitstellung.
- Erstellen Sie Registrierungsschlüssel mithilfe des Gruppenrichtlinienobjekts (GPO). Verwenden Sie diese Methode, wenn Ihre Bereitstellung über eine größere Anzahl physischer VDA-Maschinen verfügt und die Drucktelemetrie auf allen Maschinen aktiviert werden muss.

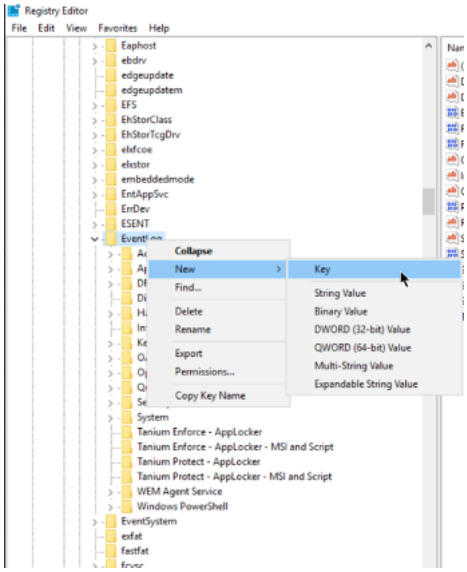
Einzelheiten zu Registrierungsschlüsseln

SL	Name des Registrierungsschlüssels	Zweck des Schlüssels	Einzelheiten zur Registrierung
1	Microsoft-Windows-PrintService/Operational	Aktiviert das Drucken von Dienstprotokollen in der Ereignisanzeige.	**Registrierungspfad**: HKLM:\SYSTEM\CurrentControlSet\
2	ShowJobTitleInEventLogs	Steuert, ob der Druckauftragsname in den Druckereignisprotokollen enthalten ist, berücksichtigt andernfalls den allgemeinen Auftragsnamen “Dokument drucken”.	**Registrierungsstruktur:**HKEY_LOC **Registrierungspfad**: Software\Policies\Microsoft\Windows NT\Printers **Wertname**: ShowJobTitleInEventLogs **Werttyp**: REG_DWORD **Wert**: 1

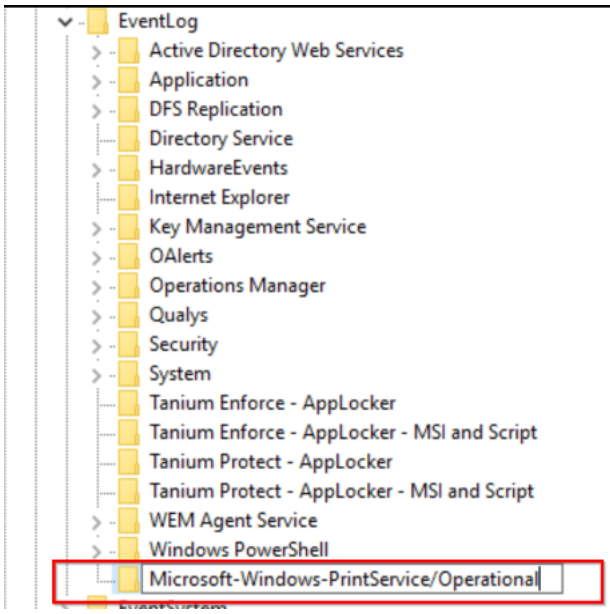
Manuelles Erstellen von Registrierungsschlüsseln in einer VDA-Maschine Verwenden Sie diesen Ansatz, um den Registrierungsschlüssel im VDA-Masterimage zu erstellen. Das Hinzufügen von Schlüsseln zum Masterimage hilft dabei, die Schlüssel für alle Arten von VDAs, die mithilfe des Masterimages erstellt werden, dauerhaft zu halten.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

1. Melden Sie sich bei der VDA-Mastermaschine an.
2. Öffnen Sie Run und geben Sie Regedit ein, um die Windows-Registrierung zu öffnen.
3. Gehen Sie zum Speicherort HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog
4. Rechtsklicken Sie auf **EventLog** und wählen Sie **Neu > Schlüssel**



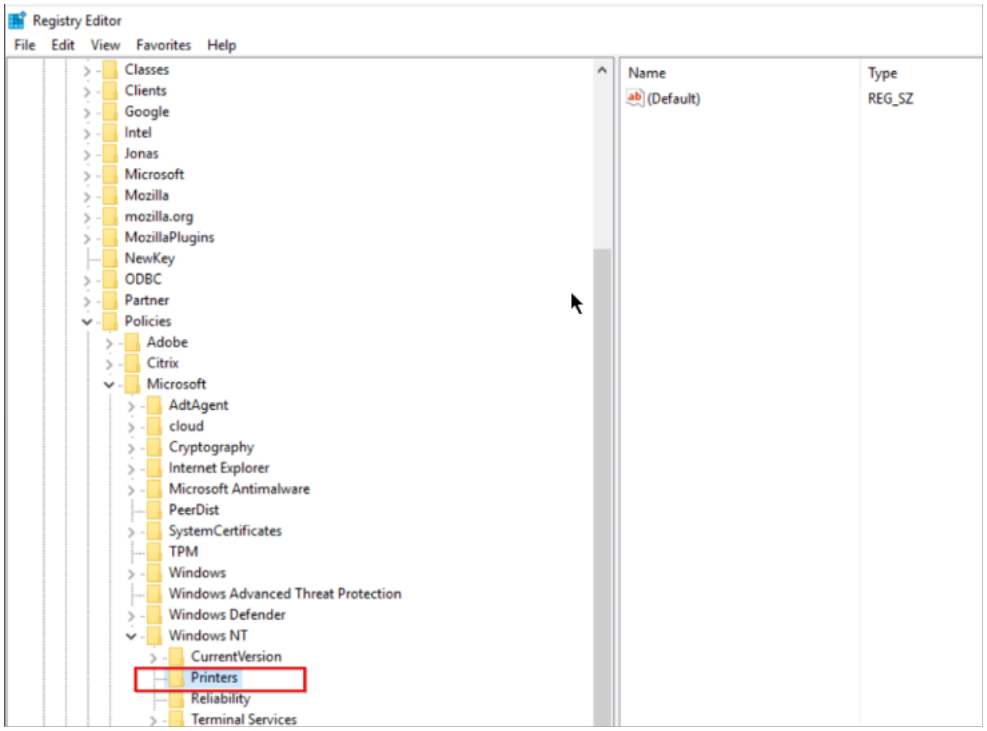
5. Erstellen Sie einen Schlüssel mit dem Namen **Microsoft-Windows-PrintService/Operational**. Dieser Schlüssel aktiviert die Druckdienstprotokolle.



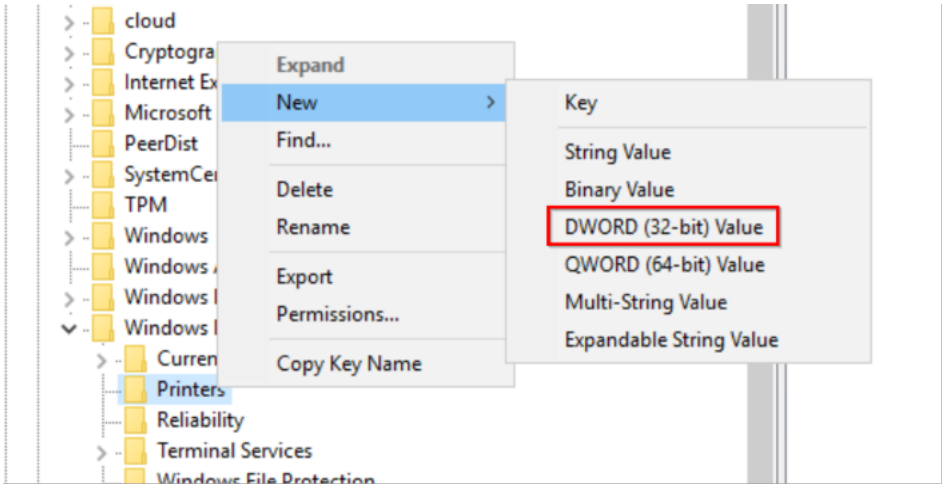
6. Gehen Sie zum Speicherort **HKEY_LOCAL_MACHINE\ Software\ Policies\ Microsoft\ Windows NT\ Printers**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Hinweis:**
>
> Wenn der Ordner Drucker nicht verfügbar ist, erstellen Sie im Windows NT-Ordner einen Schlüssel mit dem Namen Drucker.

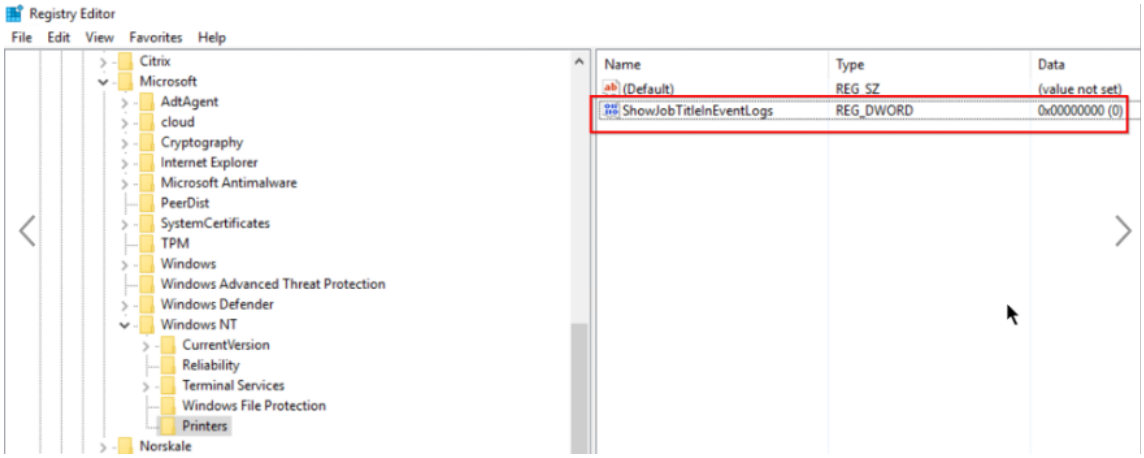


7. Klicken Sie mit der rechten Maustaste auf den Ordner **Drucker** und wählen Sie **Neu > DWORD-Wert (32-Bit)**

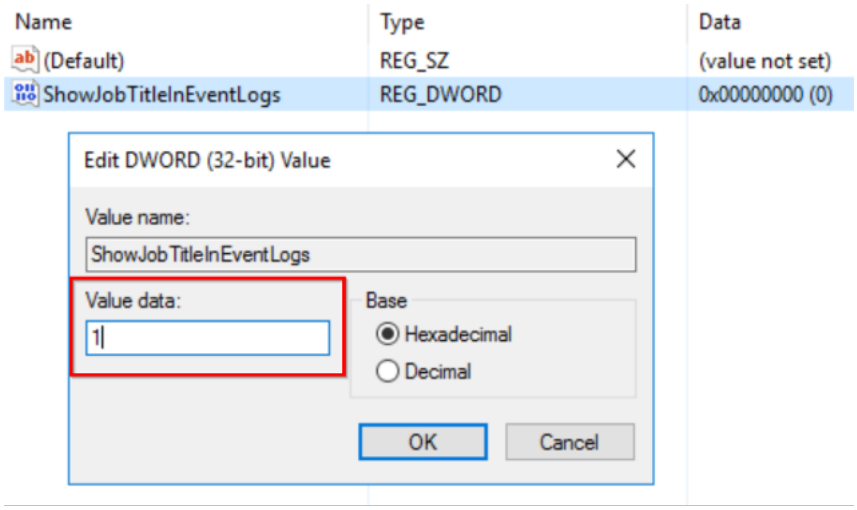


8. Erstellen Sie einen Wert mit dem Namen **ShowJobTitleInEventLogs**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



9. Klicken Sie mit der rechten Maustaste auf **ShowJobTitleInEventLogs** und wählen Sie **Ändern**. Geben Sie die **Wertdaten** als 1 ein und klicken Sie auf **OK**.

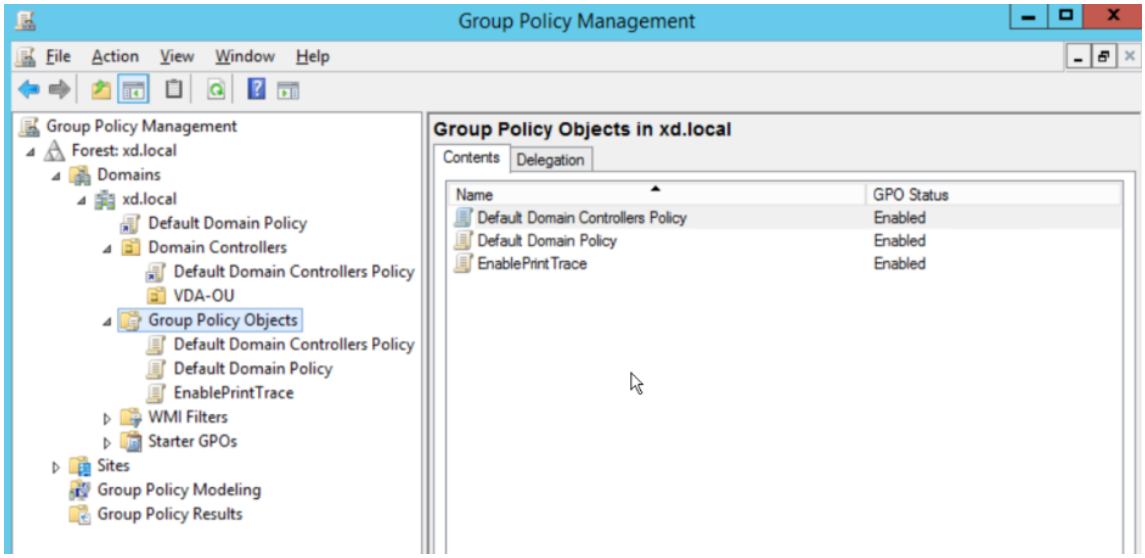


Erstellen von Registrierungsschlüsseln in mehreren VDAs über GPOs Dieser Ansatz funktioniert nur für die persistenten VDAs und erfordert einen Neustart der VDAs nach der Erstellung der Registrierungsschlüssel. Ein persistenter VDA ist eine Maschine, die ihren Status nach einem Neustart beibehält. Die Daten der Benutzer gehen nach dem Neustart nicht verloren.

Erstellen Sie das Registrierungs-GPO mit den Registrierungsschlüsseln

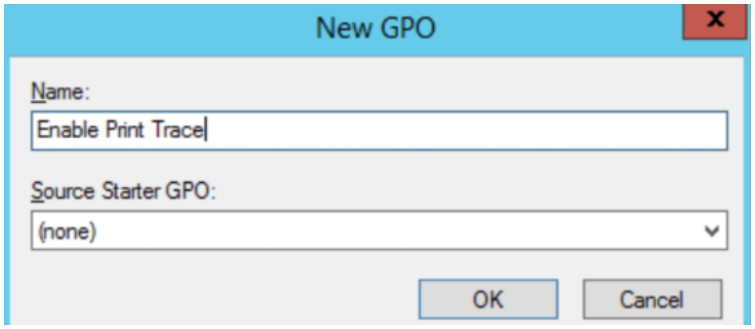
1. Öffnen Sie Gruppenrichtlinienverwaltung, und klicken Sie mit der rechten Maustaste auf **Gruppenrichtlinienobjekt**

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



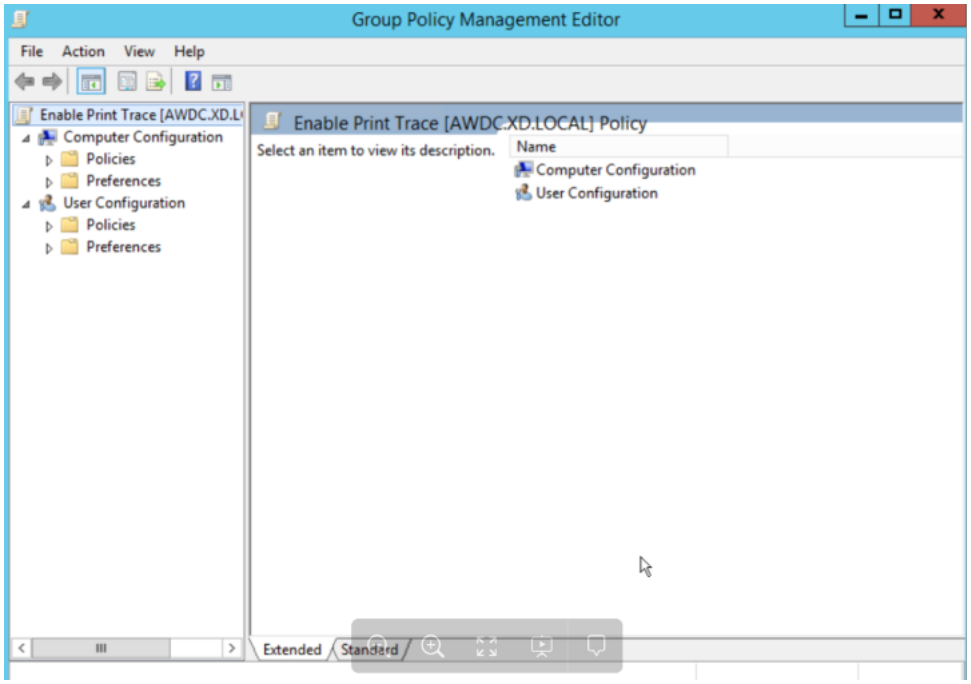
2. Geben Sie im Fenster **Neues GPO** die Werte in die folgenden Felder ein:

   - Name: Print Trace aktivieren
   - Source Starter GPO: (keine)

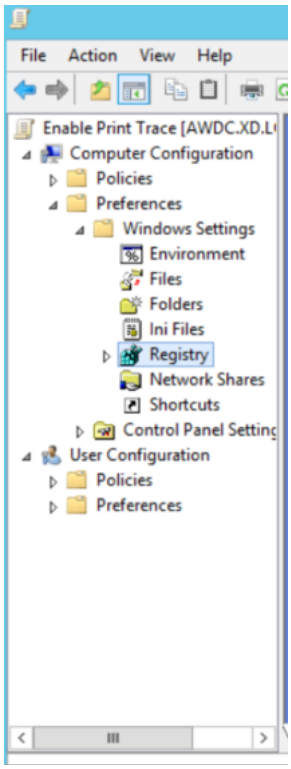


3. Wählen Sie **OK**.
4. Klicken Sie mit der rechten Maustaste auf das von Ihnen erstellte Objekt **Druckverfolgung aktivieren** und wählen Sie **Bearbeiten**

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



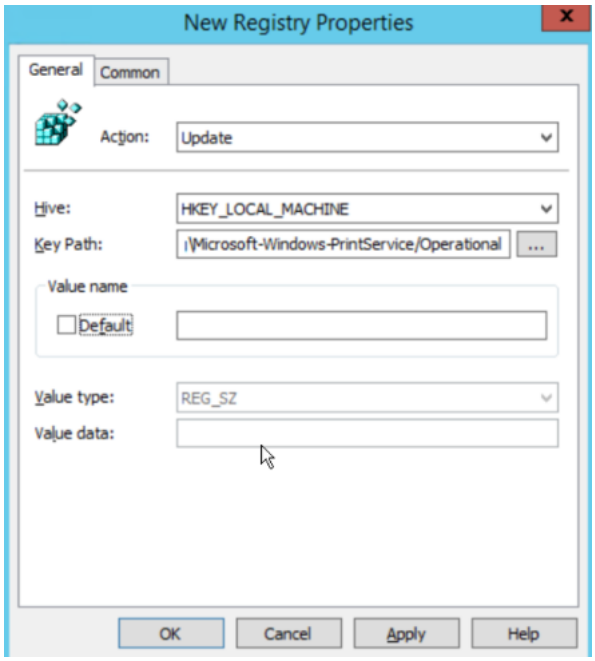
5. Wählen Sie in der Liste **Computerkonfiguration** die Option **Voreinstellungen > Windows-Einstellungen**aus.



6. Rechtsklicken Sie auf **Registrierung**und wählen Sie **Neu > Registrierungselement**. Geben Sie folgende Eigenschaften ein, um Druckprotokolle zu aktivieren:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

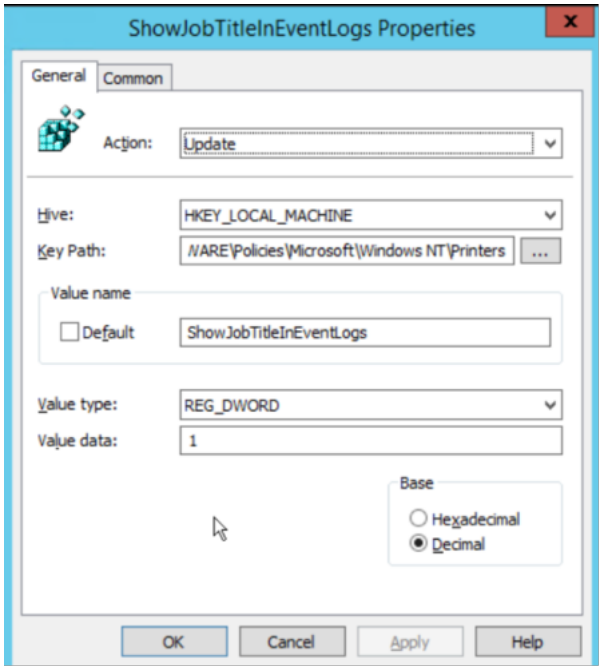
- Aktion: Update
- Hive: HKEY_LOCAL_MACHINE
- Schlüsselpfad: SYSTEM\CurrentControlSet\Services\EventLog\Microsoft-Windows-PrintService/Operational



7. Wählen Sie **Übernehmen** und dann **OK** aus.
8. Klicken Sie noch einmal mit der rechten Maustaste auf **Registrierung** und wählen Sie **Neu > Registrierungselement**. Geben Sie die folgenden Eigenschaften ein, um Druckauftragsnamen zu aktivieren:

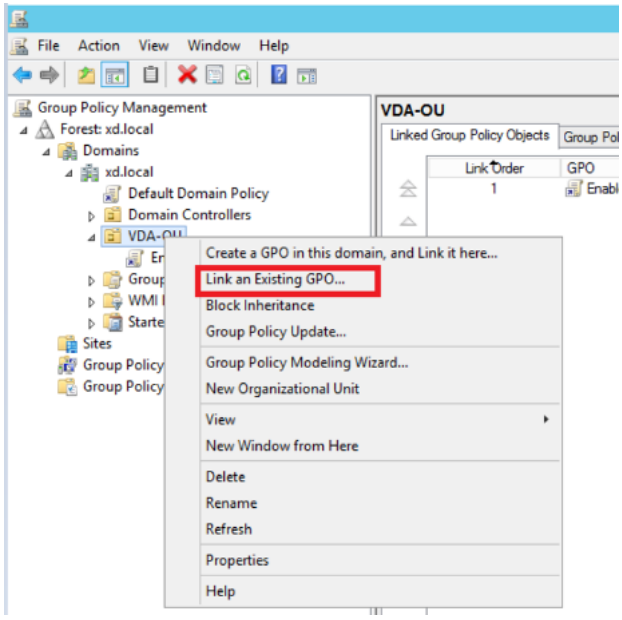
   - Aktion: Update
   - Hive: HKEY_LOCAL_MACHINE
   - Schlüsselpfad: SOFTWARE\Policies\Microsoft\Windows NT\Printers
   - Wertname: ShowJobTitleInEventLogs
   - Werttyp: REG_DWORD
   - Wertdaten: 1
   - Basis: Dezimal

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



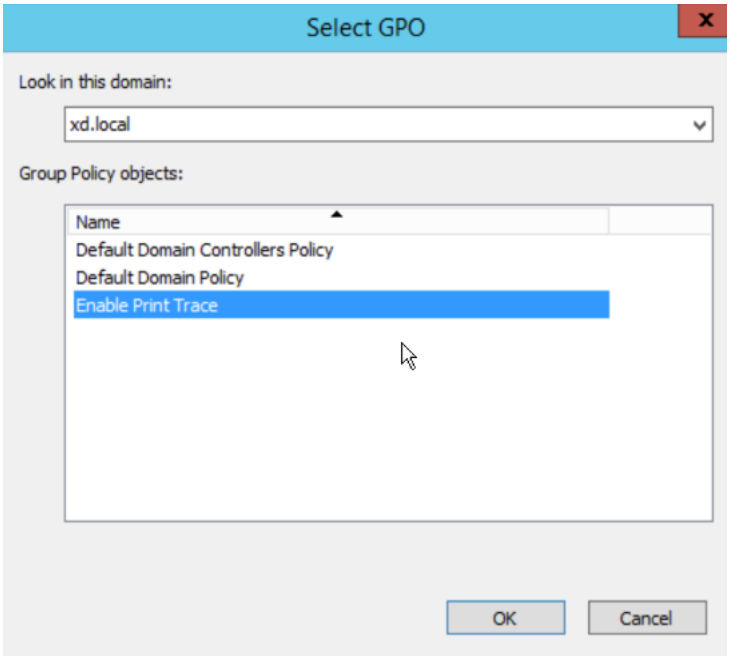
Print Trace für die Organisationseinheit aktivieren

1. Öffnen Sie die **Gruppenrichtlinienverwaltung** und wählen Sie die Domäne (z. B. xd.local) oder die Organisationseinheit aus, falls VDAs Teil davon sind (z. B. —VDA-OU).
2. Klicken Sie mit der rechten Maustaste auf die Domäne (xd.local) oder OU (VDA-OU) und wählen Sie **Vorhandenes Gruppenrichtlinienobjekt verknüpfen**

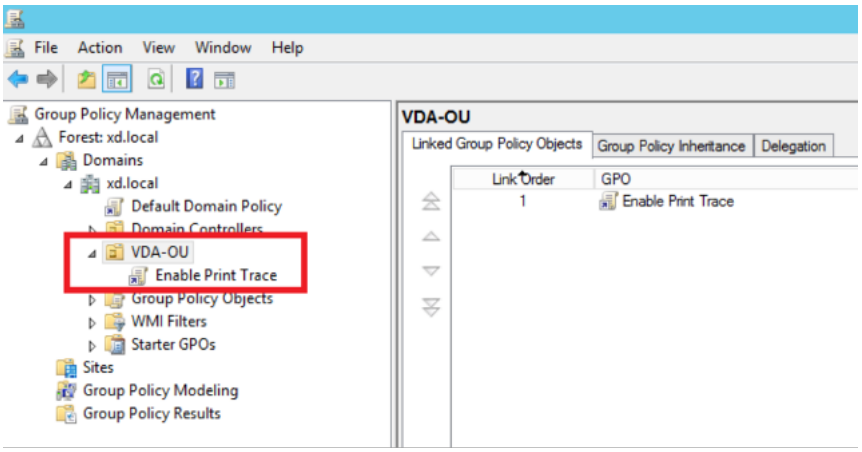


3. Wählen Sie im Dialogfeld **GPO auswählen** die Option “Druckverfolgung aktivieren”und dann **OK**aus.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



4. Stellen Sie sicher, dass das **Gruppenrichtlinienobjekt Druckverfolgung aktivieren** mit der Organisationseinheit verknüpft ist.



Hinweis

- Wenn Sie einen VDA-Neustart durchführen, gehen alle Ereignisse in der Warteschlange verloren und sind in Citrix Analytics nicht verfügbar.
- Dieser Neustart hat nur geringe Auswirkungen auf einen VDA für eine einzelne Sitzung, da nur eine Sitzung gleichzeitig aktiv sein kann. Dementsprechend ist die Anzahl der Ereignisse geringer.
- Dieser Neustart hat große Auswirkungen auf einen VDA mit mehreren Sitzungen, da alle aktiven Sitzungen während des Neustarts beendet werden und die Ereignisse in der Warteschlange verloren gehen.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Telemetrie in der Zwischenablage für Citrix DaaS aktivieren

Mit Citrix DaaS (früher bekannt als Citrix Virtual Apps and Desktops Service) können Benutzer Operationen in der Zwischenablage ausführen, und die zugehörigen Protokolle können in Citrix Analytics for Security eingesehen werden. Diese Zwischenablageprotokolle enthalten wertvolle Informationen wie den VDA-Namen, die Größe der Zwischenablage, den Formattyp der Zwischenablage, die Client-IP, den Vorgang in der Zwischenablage, die Betriebsrichtung der Zwischenablage und ob der Vorgang in der Zwischenablage zulässig war.

Als Sicherheitsadministrator können Sie diese Protokolle für Risikoanalysen und Untersuchungen verwenden, indem Sie auf der **Suchseite** in Citrix Analytics for Security die Datenquelle **Apps and Desktops** auswählen.

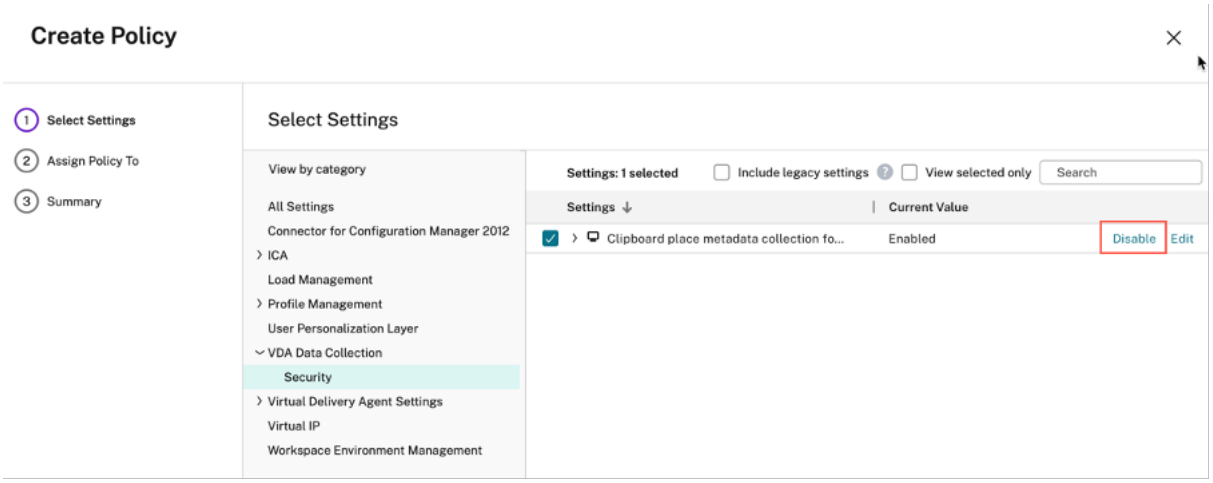
> **Hinweis**
>
> - Standardmäßig ist die Erfassung und Übertragung dieser Zwischenablageprotokolle auf den Virtual Delivery Agents (VDAs) aktiviert.
> - Diese Konfiguration gilt nur für die Windows VDAs.

Voraussetzungen

- Ihre VDA-Version muss mit der Basisversion für Citrix Virtual Apps and Desktops 7 2305 oder höher übereinstimmen. Weitere Informationen finden Sie unter Citrix Virtual Apps and Desktops 7 2305.
- Stellen Sie sicher, dass die Einstellung **Client-Zwischenablage-Umleitung** auf der Seite **Web Studio-Richtlinien** nicht auf den Status Unzulässig konfiguriert ist. Weitere Informationen finden Sie unter Client-Zwischenablage-Umleitung.

Sie können die **Metadatensammlung in der Zwischenablage für die Sicherheitsüberwachungsrichtlinie** verwenden, um die Telemetrie in der Zwischenablage zu aktivieren oder zu deaktivieren. Standardmäßig ist diese Richtlinie aktiviert. Zum Deaktivieren müssen Sie die **Richtlinienseite** aufrufen und unter der **VDA-Datenerfassung** die Option **Sicherheit** auswählen > die Richtlinie überprüfen > auf **Deaktivieren**klicken.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Weitere Informationen finden Sie unter Sammlung von Metadaten in der Zwischenablage für die Sicherheitsüberwachung.

Aktivieren oder Deaktivieren der Datenverarbeitung für die Datenquelle

Sie können die Datenverarbeitung für eine bestimmte Datenquelle- Director- und Workspace-App jederzeit beenden. Klicken Sie auf der Datenquell-Site-Karte auf die **vertikale Auslassungspunkte () > Datenverarbeitung ausschalten**. Citrix Analytics stoppt die Verarbeitung von Daten für diese Datenquelle. Sie können die Datenverarbeitung auch über die Sitekarte Apps and Desktops beenden. Diese Option gilt für beide Datenquellen: Director und Workspace-App.

Um die Datenverarbeitung wieder zu aktivieren, klicken Sie auf **Datenverarbeitung einschalten**.

Microsoft Active Directory und Azure Active Directory Directory-Integration

May 4, 2022

Verbinden Sie Ihr Active Directory oder Ihr Azure Active Directory und importieren Sie die Benutzerdetails und die Benutzergruppen aus der Domäne Ihrer Organisation in Citrix Analytics for Security.

Diese Integration erweitert die Benutzerprofile in Citrix Analytics for Security um Details zur Benutzeridentität wie Berufsbezeichnung, Organisation, Bürostandort, E-Mail und Kontaktdaten. Auf der Benutzerprofilseite können Sie diese Benutzerdetails anzeigen, die Ihnen bei der Risikountersuchung und -analyse helfen.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

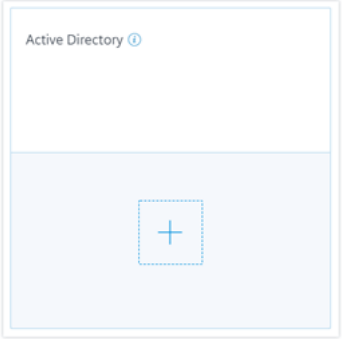
Voraussetzungen

- Wenn Sie Active Directory mit Citrix Analytics for Security verbinden möchten, stellen Sie sicher, dass Ihr Active Directory zuerst mit Ihrem Citrix Cloud Cloud-Konto verbunden ist. Weitere Informationen finden Sie unter Verbinden von Active Directory mit Citrix Cloud.
- Wenn Sie Azure Active Directory mit Citrix Analytics for Security verbinden möchten, stellen Sie sicher, dass Ihr Azure Active Directory zuerst mit Ihrem Citrix Cloud Cloud-Konto verbunden ist. Weitere Informationen finden Sie unter Verbinden von Azure Active Directory mit Citrix Cloud.

Verbinden von Microsoft Active Directory

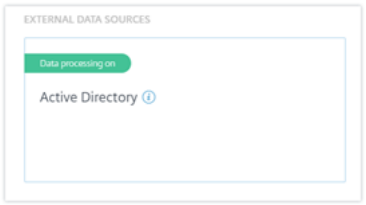
Gehen Sie wie folgt vor, um Ihr Active Directory mit Citrix Analytics for Security zu verbinden:

1. Gehen Sie zu **Einstellungen** > **Datenquellen** > **Sicherheit** und navigieren Sie dann zum Abschnitt **EXTERNE DATENQUELLEN** .
2. Klicken Sie auf der **Active Directory-Standortkarte** auf das Pluszeichen **+** .



3. Citrix Analytics fordert Sie auf, Active Directory mit Ihrem Citrix Cloud-Konto zu verbinden. Weitere Informationen finden Sie unter Voraussetzungen.

Nachdem Sie Ihr Active Directory mit Ihrem Citrix Cloud-Konto verbunden haben, erkennt Citrix Analytics diese neue Datenquelle automatisch. Auf der Seite **Datenquellen** zeigt die Active Directory-Standortkarte **Datenverarbeitung auf an**.



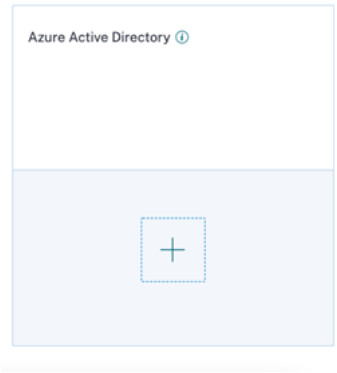
Der Status **Datenverarbeitung im** Status zeigt an, dass das Active Directory erkannt wurde und Benutzerinformationen aus Ihrem Active Directory abgerufen werden.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Verbinden Sie Microsoft Azure Active Directory

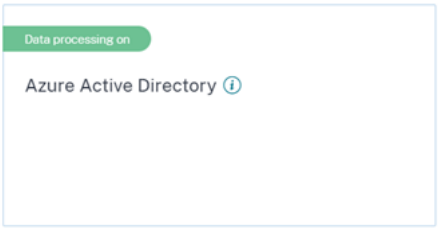
Gehen Sie wie folgt vor, um Ihr Azure Active Directory mit Citrix Analytics zu verbinden:

1. Gehen Sie zu **Einstellungen > Datenquellen > Sicherheit** und navigieren Sie dann zum Abschnitt **EXTERNE DATENQUELLEN** .
2. Klicken Sie auf der **Azure Active Directory Directory-Standortkarte** auf das Pluszeichen +.



3. Citrix Analytics fordert Sie auf, Azure Active Directory mit Ihrem Citrix Cloud Cloud-Konto zu verbinden. Weitere Informationen finden Sie unter Verbinden von Azure Active Directory mit Citrix Cloud.

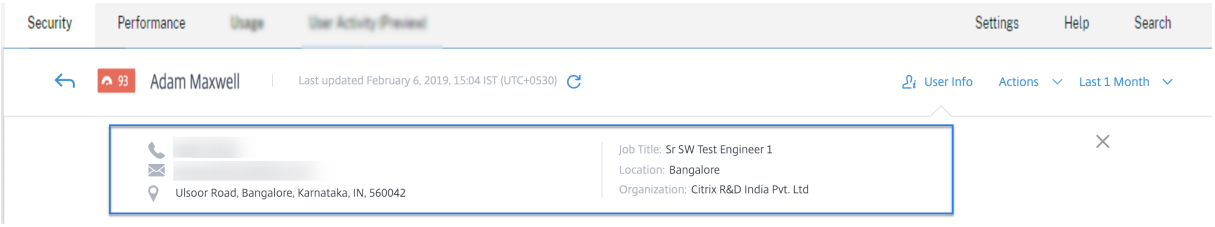
Nachdem Sie Ihr Azure Active Directory mit Ihrem Citrix Cloud Cloud-Konto verbunden haben, erkennt Citrix Analytics diese neue Datenquelle automatisch. Auf der Seite **Datenquellen** zeigt die **Azure Active Directory Directory-StandortkarteDatenverarbeitung auf an**. Dieser Status zeigt an, dass das Azure Active Directory erkannt wurde und die Benutzerinformationen aus Ihrem Azure Active Directory abgerufen werden.



Benutzerinformationen anzeigen

Klicken Sie auf der Registerkarte **Sicherheit** auf einen riskanten Benutzer, um die Benutzerprofilseite anzuzeigen. Wenn der Benutzer in Active Directory oder Azure Active Directory verfügbar ist, können Sie seine Berufsbezeichnung, Organisation, E-Mail-Adresse und Kontaktnummer auf der Benutzerprofilseite anzeigen.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Integration von Microsoft Graph Security

June 17, 2021

Microsoft Graph Security ist eine externe Datenquelle, die Daten von mehreren Sicherheitsanbietern aggregiert. Es bietet auch Zugriff auf die Benutzerinventardaten.

Citrix Analytics unterstützt derzeit die folgenden Sicherheitsanbieter von Microsoft Graph Security:

- Azure AD-Identitätsschutz
- Microsoft Defender für Endpoint

Weitere Informationen zu den Sicherheitsanbietern finden Sie unter den folgenden Links:

- Für **Azure AD Identitätsschutz**:https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/concept-risk-events
- Für **Microsoft Defender für Endpoint**: https://docs.microsoft.com/en-us/mem/configmgr/protect/deploy-use/defender-advanced-threat-protection

Um die Microsoft Graph Security-Datenquelle einbauen zu können, müssen Sie die erforderlichen Berechtigungen für einen Mandanten von der Microsoft-Identitätsplattform abrufen.

Voraussetzungen

Bevor Sie mit dem Onboarding der Microsoft Graph Security-Datenquelle beginnen, müssen Sie Folgendes sicherstellen:

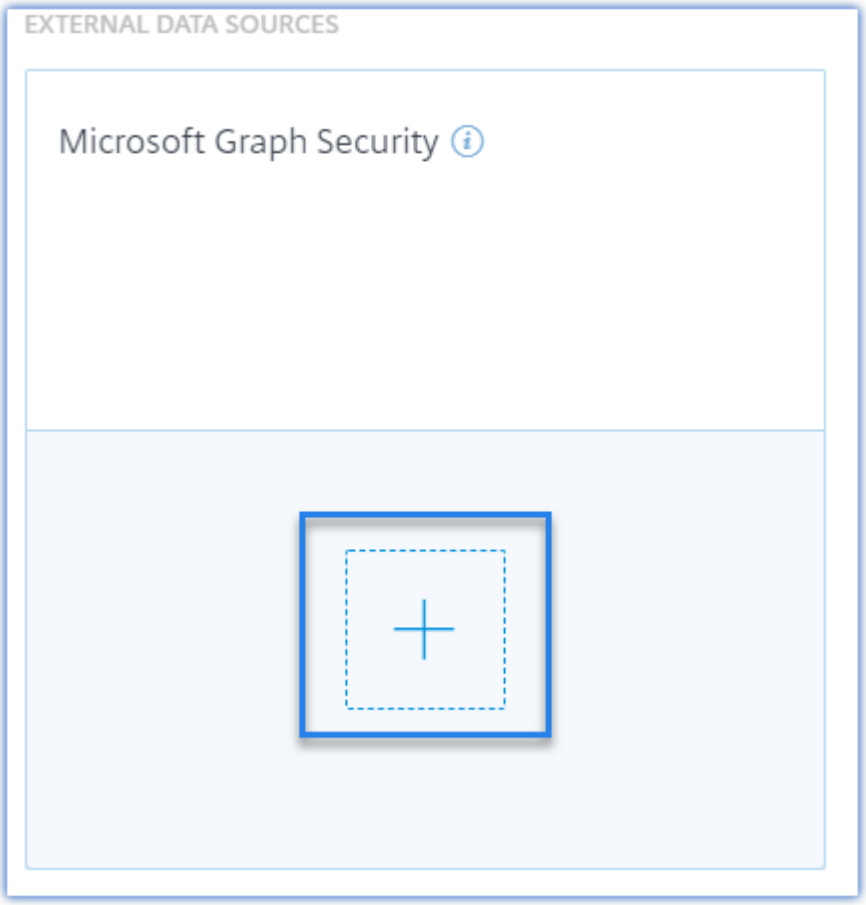
- Der Administrator verwendet den Azure AD Identity Protection (Teil des Azure AD Premium P2) Sicherheitsanbieters.
- Der Endbenutzer ist mit Arbeits- oder Schulkonten im Microsoft Store angemeldet.

Onboarding von Microsoft Graph -Sicherheitsinstanzen

1. Gehen Sie zu **Einstellungen** > **Datenquellen** > **Sicherheit**, und navigieren Sie dann zum Abschnitt **EXTERNE DATAQUELLEN**.

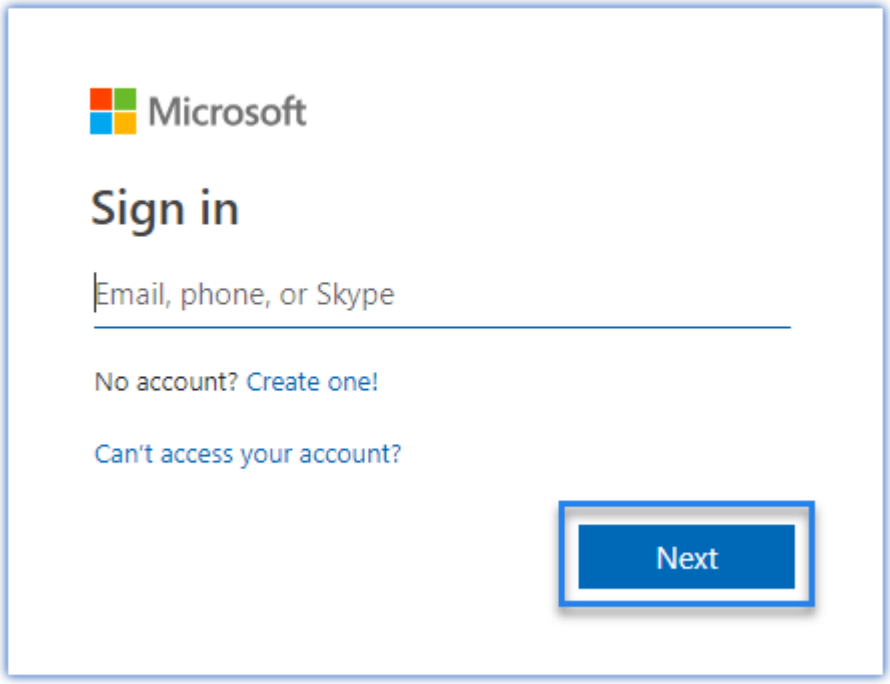
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

2. Klicken Sie auf das Pluszeichen (**+**) auf der Microsoft Graph -Sicherheits-Sitekarte. Sie werden zum Autorisierungsendpunkt umgeleitet.



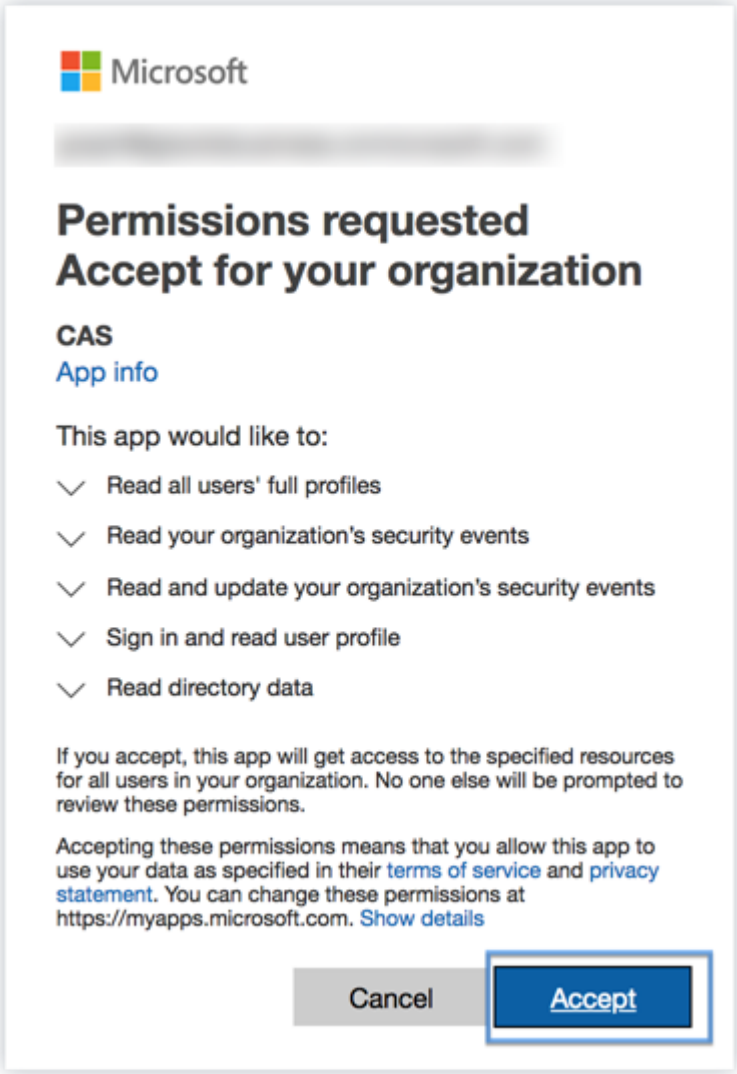
3. Melden Sie sich im **Microsoft-Fenster** mit Ihren Azure-Anmeldeinformationen an, um ein Konto zu registrieren. Oder wählen Sie ein vorhandenes Konto aus.
4. Klicken Sie auf **Weiter**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



5. Klicken Sie auf **Akzeptieren**. Sie werden auf die Seite Datenquellen umgeleitet. Die Microsoft Graph Security-Datenquelle ist jetzt mit Ihrem Citrix Cloud-Konto verknüpft.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

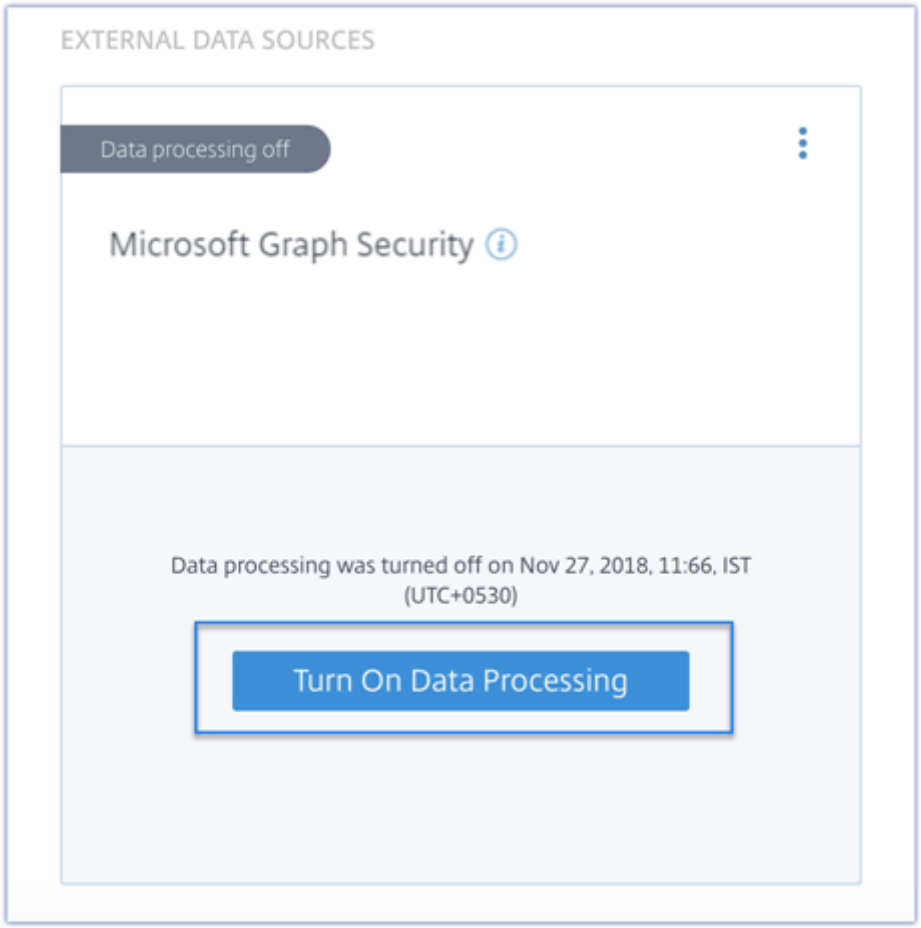


Aktivieren oder Deaktivieren der Datenverarbeitung

Um die Datenverarbeitung zu deaktivieren, klicken Sie auf die vertikale Auslassungspunkte () auf der Sitekarte und wählen Sie **Datenverarbeitung deaktivieren**aus. Dadurch wird verhindert, dass Citrix Analytics Daten für diese Datenquelle verarbeitet.

Sie können die Datenverarbeitung erneut aktivieren, indem Sie **auf der Sitekarte die Option Datenverarbeitung aktivieren** auswählen.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Weitere Informationen zu Microsoft Graph -Sicherheitsrisikoindikatoren finden Sie unter Microsoft Graph -Sicherheitsrisikoindikatoren.

Integration von Sicherheitsinformationen und Ereignismanagement (SIEM)

December 12, 2023

> **Hinweis**
>
> Wenden Sie sich an CAS-PM-Ext@cloud.com, um Unterstützung für die SIEM-Integration, den Export von Daten nach SIEM anzufordern und Feedback zu geben.

Integrieren Sie Citrix Analytics for Security in Ihre SIEM-Dienste und exportieren Sie die Benutzerdaten aus der Citrix IT-Umgebung in Ihr SIEM. Korrelieren Sie die exportierten Daten mit den in Ihrem SIEM verfügbaren Daten, um tiefere Einblicke in die Sicherheitslage Ihres Unternehmens zu erhalten.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Diese Integration erhöht den Wert sowohl Ihres Citrix Analytics for Security als auch Ihres SIEM.

Vorteile

- Ermöglicht es Ihren Security Operations-Teams, Daten aus unterschiedlichen Protokollen zu korrelieren, zu analysieren und zu durchsuchen.
- Hilft Ihren Security Operations-Teams, die Sicherheitsrisiken zu identifizieren und schnell zu beheben.
- Sichtbarkeit von Sicherheitswarnungen an einem zentralen Ort.
- Zentraler Ansatz zur Erkennung potenzieller Sicherheitsbedrohungen für organisatorische Risikoanalysefunktionen wie Risikoindikatoren, Benutzerprofile und Risikobewertungen.
- Möglichkeit, die Citrix Analytics Risk Intelligence-Informationen eines Benutzerkontos mit den externen Datenquellen zu kombinieren und zu korrelieren, die in Ihrem SIEM verbunden sind.

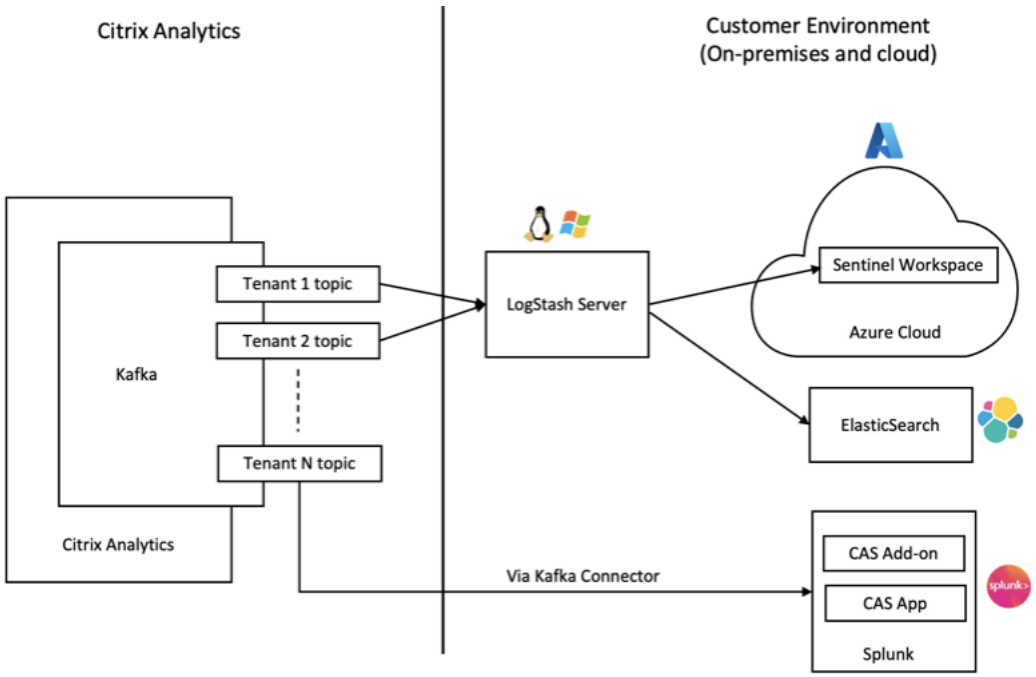
SIEM-Integrationsarchitektur

Ihre SIEM-Integration stellt eine Verbindung zu dem nach Norden führenden Kafka her, das in der Citrix Analytics for Security Cloud bereitgestellt wird. Dies kann auf zwei Arten erreicht werden:

- **Kafka-Endpunkte**: Wenn Ihr SIEM Kafka-Endpunkte unterstützt, verwenden Sie die in der Logstash-Konfigurationsdatei angegebenen Parameter und die Zertifikatsdetails in der JKS-Datei oder der PEM-Datei, um Ihr SIEM in Citrix Analytics for Security zu integrieren. Mit den Kafka-Endpunkten können Sie eine Verbindung herstellen und die Daten zum SIEM Ihrer Wahl abrufen.
- **Logstash-Engine**: Wenn Ihr SIEM keine Kafka-Endpunkte unterstützt, können Sie die Logstash-Datenerfassungs-Engine verwenden. Sie können die Risk Insights-Daten von Citrix Analytics for Security an eines der Ausgabe-Plug-Ins senden, die von Logstash unterstützt werden.

Sehen Sie sich das folgende Architekturdiagramm der SIEM-Lösung an, um zu verstehen, wie Daten von Citrix Analytics for Security zu Ihrem SIEM-Service fließen:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

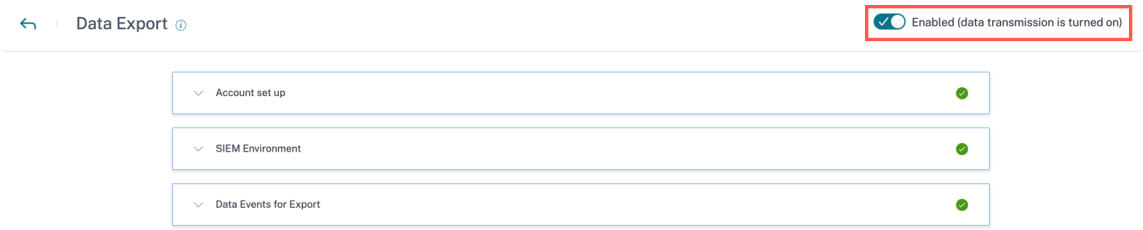


Aktivieren oder Deaktivieren der Datenübertragung

So beenden Sie die Übertragung von Daten aus Citrix Analytics for Security:

1. Gehen Sie zu **Einstellungen > Datenexporte**.
2. Schalten Sie die Umschalttaste aus, um die **Datenübertragung** zu deaktivieren.

> **Hinweis**
> Standardmäßig ist die Datenübertragung für SIEM immer aktiviert/aktiviert.



Um die Datenübertragung wieder zu aktivieren, schalten Sie die Umschalttaste ein.

SIEM-Umgebung einrichten

Um Daten nach SIEM zu exportieren, müssen Sie die folgenden Aktionen ausführen:

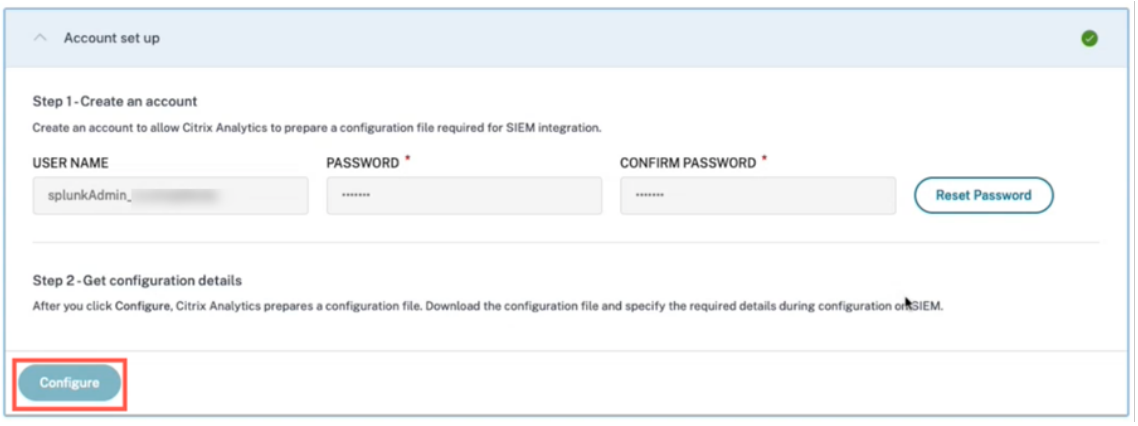
- Richten Sie Ihr Kafka-Konto und Ihre Authentifizierungsdaten ein

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Laden Sie die vorausgefüllte Konfiguration herunter und richten Sie die SIEM-Umgebung ein
- Datenereignisse für den Export

Einrichtung des SIEM-Exportkontos

1. Um Ihr Konto einzurichten, navigieren Sie zu **Einstellungen > Datenexporte > erweitern Sie Kontoeinrichtung**. Erstellen Sie ein Konto, indem Sie den Benutzernamen und das Kennwort angeben. Sobald Sie Ihr Konto eingerichtet haben, werden Ihre Kafka-Daten generiert. Diese Details werden beim Generieren der Konfigurationsdatei automatisch eingebettet.



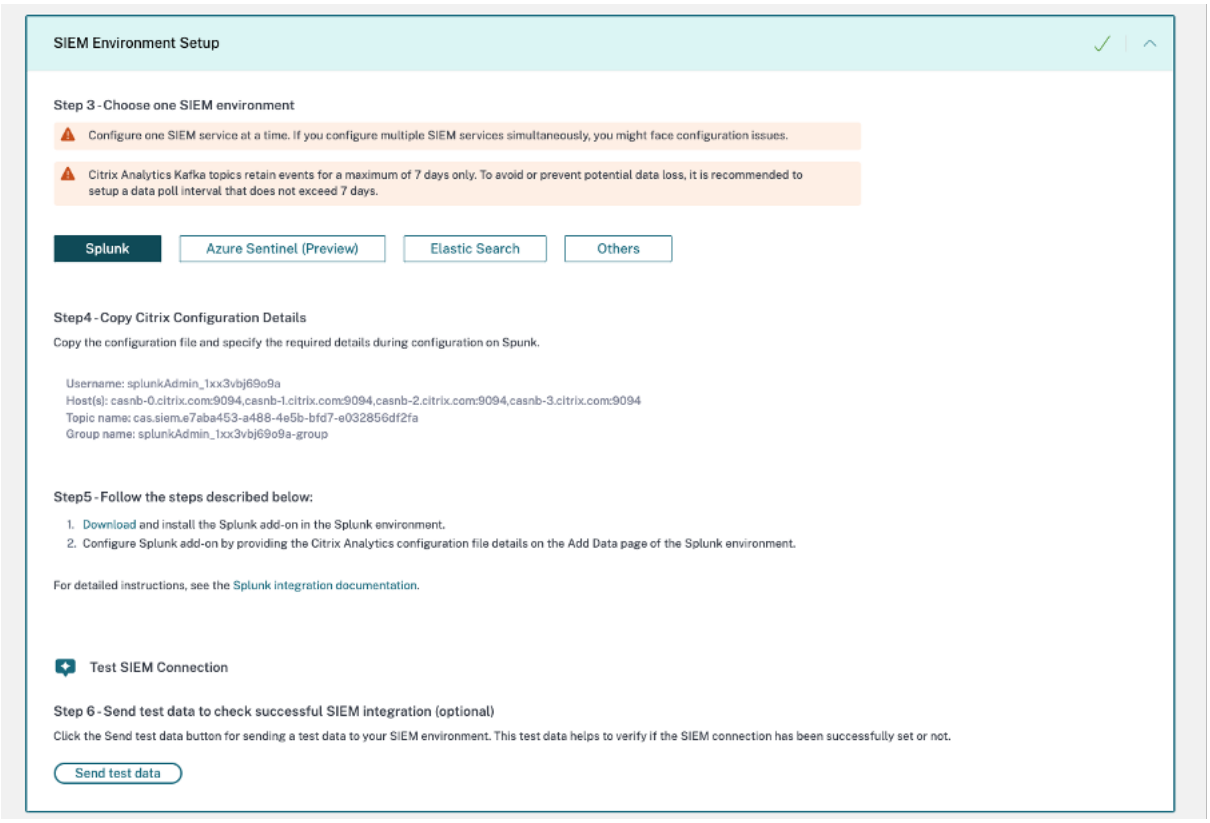
2. Klicken Sie auf **Konfigurieren**, um die Konfigurationsdatei zu generieren. Die Konfigurationsdatei enthält Details wie Kafka-Endpoints, Ihre spezifischen Abonnementthemen und Gruppen-IDs. Außerdem werden die Kafka- und SSL-Attribute vorkonfiguriert, die für den Abschluss der Authentifizierung und des Datenflusses erforderlich sind.

SIEM-Konfiguration und Umgebungs-Setup

Wählen Sie die SIEM-Umgebung nach Bedarf aus. Sie können Citrix Analytics for Security mit den folgenden Diensten integrieren. Unter den folgenden Links erhalten Sie detaillierte Informationen und SIEM-spezifische Konfigurationen:

- Splunk
- Sentinel
- Elasticsearch
- Andere SIEMs verwenden Kafka- oder Logstash-basierten Datenconnector

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Datenereignisse, die aus Citrix Analytics for Security in Ihren SIEM-Dienst exportiert wurden

Im Rahmen von SIEM-Exporten gibt es zwei Arten von Datensätzen:

1. **Risikoeinblicksereignisse (Standardexporte)** —Nachdem Sie die Kontokonfiguration und SIEM-Einrichtung abgeschlossen haben, fließen Standarddaten (Risk Insights-Ereignisse) in Ihre SIEM-Bereitstellung. Risk Insights-Daten enthalten Benutzerrisikobewertungen, Benutzerprofile und Risikoindikatorwarnungen. Diese werden vom Citrix Analytics-Algorithmus für maschinelles Lernen, Benutzerverhaltensanalyse und basierend auf Benutzerereignissen generiert. Informationen zu den verfügbaren Ereignistypen, Metadaten und Schemas finden Sie unter Risk Insights-Daten für SIEM.
2. **Datenquellenereignisse (optionale Exporte)** —Zusätzlich können Sie die Datenexportfunktion so konfigurieren, dass Benutzerereignisse aus den Datenquellen Ihrer Citrix Analytics for Security-fähigen Produkte exportiert werden. Wenn Sie eine Aktivität in der Citrix-Umgebung ausführen, werden die Datenquellenereignisse generiert. Die exportierten Ereignisse sind unverarbeitete Benutzer- und Produktnutzungsdaten in Echtzeit, wie sie in der Self-Service-Ansicht verfügbar sind Die in diesen Ereignissen enthaltenen Metadaten können außerdem für eine tiefere Bedrohungsanalyse, das Erstellen neuer Dashboards und die Zusammenarbeit

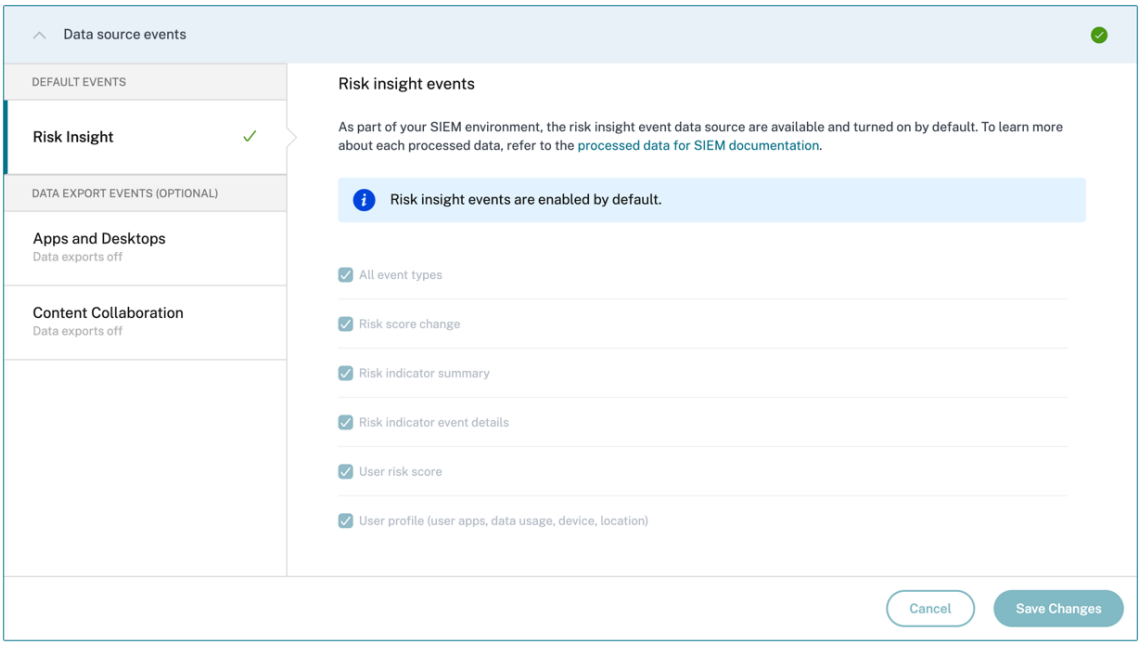
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

mit anderen Nicht-Citrix-Datenquellenereignissen in Ihrer Sicherheits- und IT-Infrastruktur verwendet werden.

Derzeit sendet Citrix Analytics for Security Benutzerereignisse für die Citrix Virtual Apps and Desktops-Datenquelle an Ihr SIEM.

Informationen zu den verfügbaren Ereignistypen, Metadaten und Schemas finden Sie unter Datenquellenereignisse.

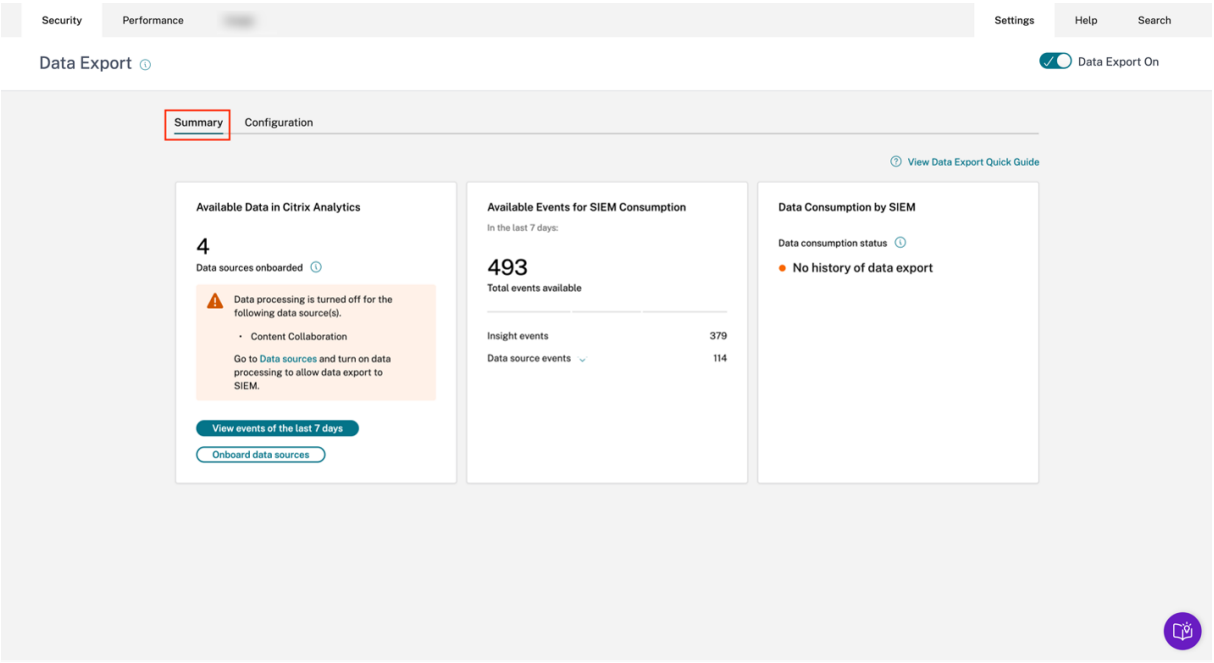
> **Hinweis**
>
> Kunden, die einen Logstash-Datenbroker verwenden, wird empfohlen, die neueste Konfigurationsdatei vom Citrix Analytics for Security-Portal herunterzuladen und im Logstash-Dienstbereitstellung zu aktualisieren. Dadurch wird sichergestellt, dass die richtigen Datenquellen-Ereignistabellen erstellt werden und die Ereignisse nun in SIEM-Indizes verfügbar sind.



Problembehandlung bei der SIEM-Integration

Die Ansicht “Datenexporte für Sicherheit”enthält eine Registerkarte **Zusammenfassung**, die Administratoren bei der Behebung von Problemen bei der SIEM-Integration mit Citrix Analytics unterstützt. Das **Übersichts-Dashboard** bietet einen Überblick über den Zustand und den Datenfluss, indem es die Prüfpunkte durchläuft, die den Fehlerbehebungsprozess unterstützen.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Weitere Informationen zu dieser Funktion finden Sie unter Problembehandlung bei Datenexporten.

Splunk-Integration

November 16, 2023

Integrieren Sie Citrix Analytics for Security in Splunk, um die Benutzerdaten aus Ihrer Citrix IT-Umgebung zu exportieren und zu korrelieren und so tiefere Einblicke in die Sicherheitslage Ihres Unternehmens zu erhalten.

Weitere Informationen zu den Vorteilen der Integration und der Art der verarbeiteten Daten, die an Ihr SIEM gesendet werden, finden Sie unter Integration von Sicherheitsinformationen und Ereignismanagement.

Informationen zu einem umfassenden Verständnis der Splunk-Bereitstellungsmethodik und zur Umsetzung der Strategien für eine effektive Planung finden Sie in der Splunk-Dokumentation zur Splunk-Architektur mit Citrix
Analytics-Anwendungen, die in der Splunk-Dokumentation gehostet werden .

Integrieren Sie Citrix Analytics for Security mit Splunk

Folgen Sie den Anweisungen zur Integration von Citrix Analytics for Security in Splunk:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Datenexport. Citrix Analytics for Security erstellt einen Kafka-Kanal und exportiert Risk Insights und Datenquellenereignisse. Splunk ruft diese Risikointelligenz aus dem Kanal ab.
- Holen Sie sich die Konfiguration auf Citrix Analytics. Erstellen Sie ein Kennwort für Ihr vordefiniertes Konto zur Authentifizierung. Citrix Analytics for Security bereitet eine Konfigurationsdatei vor, die Sie zum Konfigurieren des Citrix Analytics-Add-Ons für Splunk benötigen.
- Laden Sie das Citrix Analytics Add-On für Splunk herunter und installierenSie es. Laden Sie das **Citrix Analytics-Add-on für Splunk** entweder mithilfe von Splunkbase oder Splunk Cloud herunter, um den Installationsvorgang abzuschließen.
- Konfigurieren Sie das Citrix Analytics-Add-On für Splunk. Richten Sie eine Dateneingabe mithilfe der von Citrix Analytics for Security bereitgestellten Konfigurationsdetails ein und konfigurieren Sie das Citrix Analytics-Add-On für Splunk.

Nachdem die Citrix Analytics Konfigurationsdatei vorbereitet wurde, finden Sie unter:

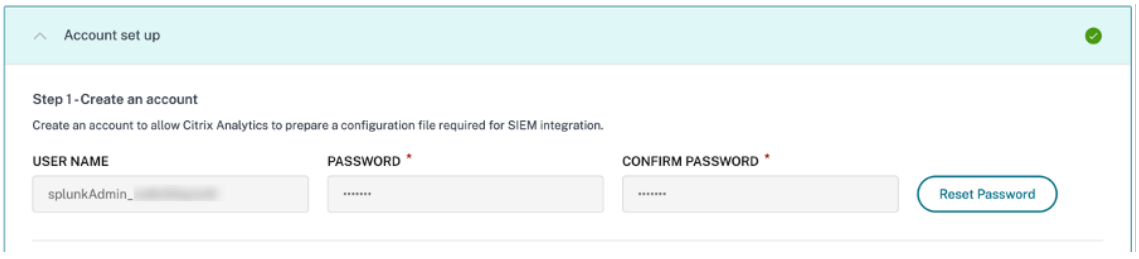
- Funktion zum Zurücksetzen des Kennworts
- Aktivieren oder Deaktivieren der Datenübertragung

Nachdem das Citrix Analytics-Add-On für Splunk konfiguriert wurde, siehe:

- So nutzen Sie Ereignisse in Splunk Environment
- So konfigurieren Sie Citrix Analytics App für Splunk

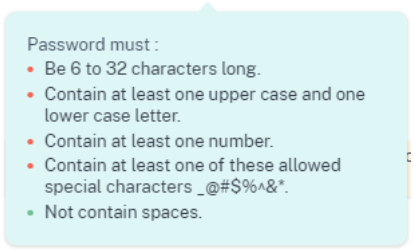
Datenexport

1. Gehen Sie zu **Einstellungen** > **Datenexporte**.
2. Erstellen Sie im Abschnitt **Kontoeinrichtung** ein Konto, indem Sie den Benutzernamen und ein Kennwort angeben. Dieses Konto wird verwendet, um eine Konfigurationsdatei vorzubereiten, die für die Integration erforderlich ist.



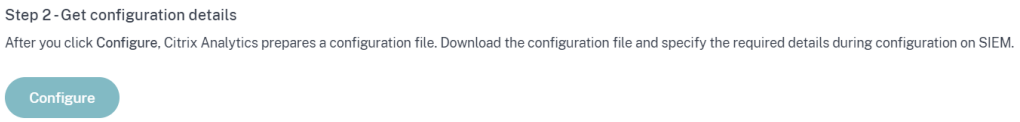
3. Stellen Sie sicher, dass das Kennwort die folgenden Bedingungen erfüllt:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



4. Wählen Sie **Konfigurieren**.

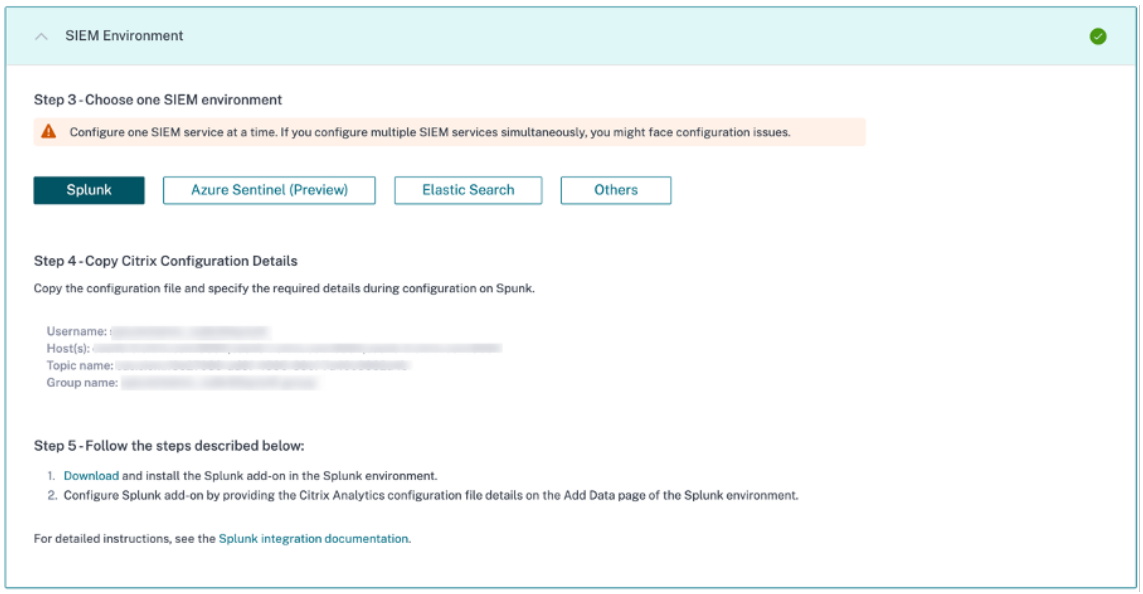
   Citrix Analytics for Security bereitet die für die Splunk-Integration erforderlichen Konfigurationsdetails vor.



5. Wählen Sie **Splunk**aus.
6. Kopieren Sie die Konfigurationsdetails, darunter den Benutzernamen, die Hosts, den Kafka-Themennamen und den Gruppennamen.

   Sie benötigen diese Details, um das Citrix Analytics Add-on für Splunk in den folgenden Schritten zu konfigurieren.

> **WICHTIG**
>
> Diese Daten sind sensibel und Sie müssen sie an einem sicheren Ort aufbewahren.



Um Kandidatendaten für die Splunk-Integration zu generieren, aktivieren Sie entweder die Datenverarbeitung für

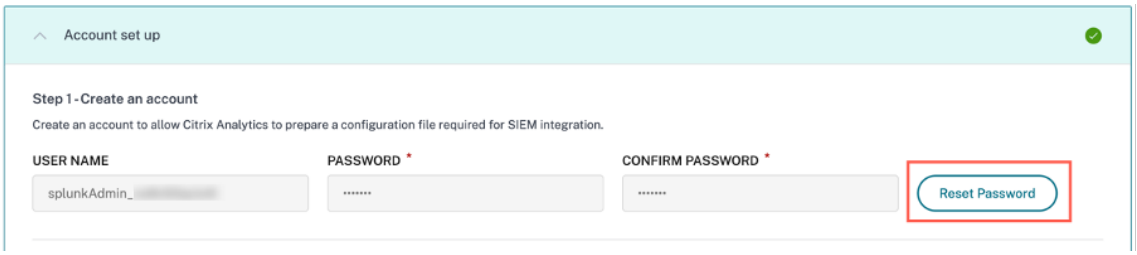
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

mindestens eine Datenquelle oder verwenden Sie die Funktion zur Generierung von Testereignissen. Es hilft Citrix Analytics
for Security, den Splunk-Integrationsprozess zu starten.

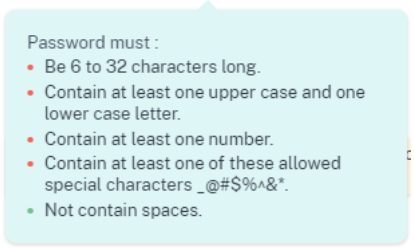
Funktion zum Zurücksetzen des Kennworts

Wenn Sie Ihr Konfigurationskennwort für Citrix Analytics for Security zurücksetzen möchten, führen Sie die folgenden Schritte aus:

1. Klicken Sie auf der Seite **Konto einrichten** auf **Kennwort zurücksetzen**.

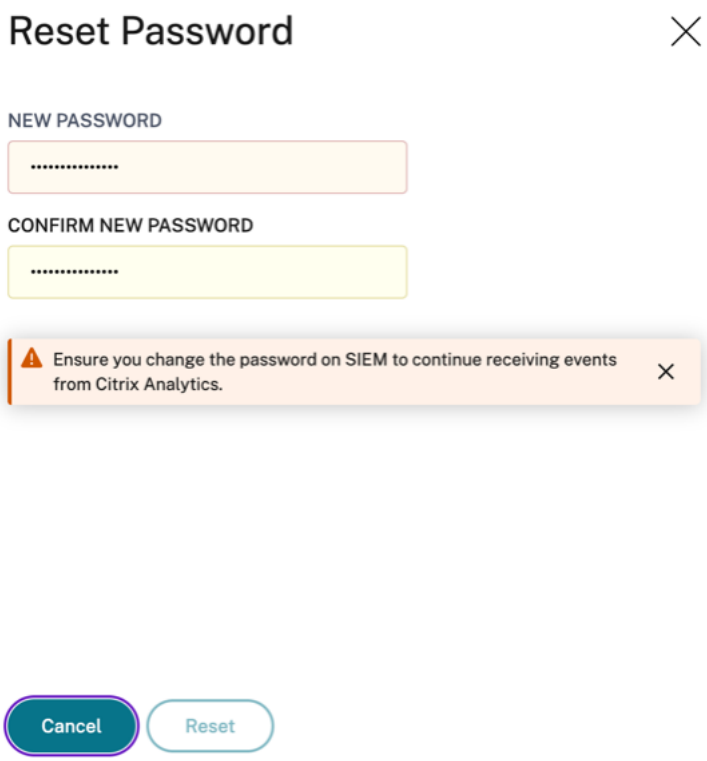


2. Geben Sie im Fenster **Kennwort zurücksetzen** das aktualisierte Kennwort in den Feldern **NEUES KENNWORT** und **NEUES KENNWORT BESTÄTIGEN** an. Folgen Sie den angezeigten Kennwortregeln.



3. Klicken Sie auf **Zurücksetzen**. Die Vorbereitung der Konfigurationsdatei wird eingeleitet.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



> **Hinweis:**
>
> Nachdem Sie das Konfigurationskennwort zurückgesetzt haben, müssen Sie das neue Kennwort aktualisieren, wenn Sie die Dateneingabe auf der Seite **Daten hinzufügen** Ihrer Splunk Umgebung einrichten. Es hilft Citrix Analytics for Security, weiterhin Daten an Splunk zu übertragen.

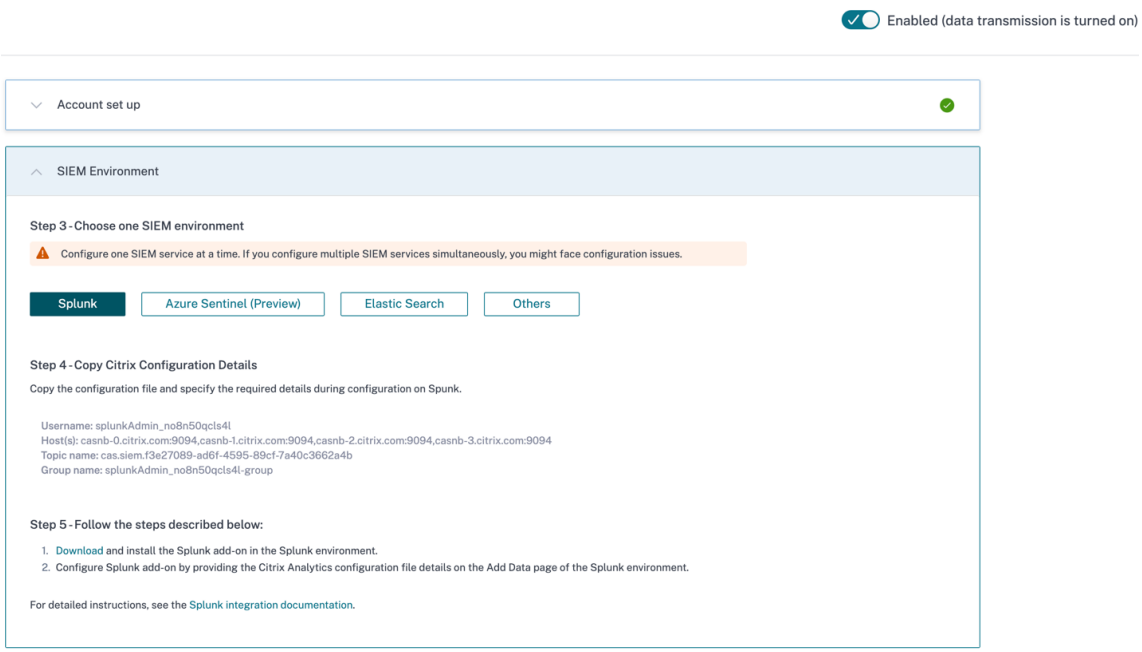
Aktivieren oder Deaktivieren der Datenübertragung

Die Datenübertragung für den Splunk-Datenexport aus Citrix Analytics ist standardmäßig aktiviert.

So beenden Sie die Übertragung von Daten aus Citrix Analytics for Security:

1. Gehen Sie zu **Einstellungen > Datenexporte**.
2. Schalten Sie die Umschalttaste aus, um die **Datenübertragung** zu deaktivieren.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Um die Datenübertragung wieder zu aktivieren, schalten Sie die Umschalttaste ein.

Citrix Analytics-Add-On für Splunk

Sie können wählen, ob Sie die Zusatzanwendung auf einer der folgenden Plattformen installieren möchten:

- Splunk Enterprise (Schwerer Spediteur)
- Splunk-Cloud

Citrix Analytics-Zusatzmodul für Splunk (lokal/unternehmensweit)

Unterstützte Versionen

Citrix Analytics for Security unterstützt die Splunk-Integration auf den folgenden Betriebssystemen:

- CentOS Linux 7 und höher
- Debian GNU/Linux 10.0 und höher
- Red Hat Enterprise Linux Server 7.0 und höher
- Ubuntu 18.04 LTS und höher

> **Hinweis**
>
> - Citrix empfiehlt, die neueste Version der vorherigen Betriebssysteme oder die Versionen zu verwenden, die noch von den jeweiligen Anbietern unterstützt werden.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> - Verwenden Sie für die Linux-Kernel-Betriebssysteme (64-Bit) eine Kernelversion, die von Splunk
> unterstützt wird. Weitere Informationen finden Sie in der Splunk-Dokumentation.

Sie können unsere Splunk-Integration auf der folgenden Splunk-Version konfigurieren: Splunk 8.1 (64-Bit) und höher.

Voraussetzungen

- Das **Citrix Analytics-Add-On für Splunk** stellt eine Verbindung zu den folgenden Endpunkten in Citrix Analytics for Security her. Stellen Sie sicher, dass sich die Endpunkte in der Zulassungsliste Ihres Netzwerks befinden.

Endpunkt	Region der Vereinigten Staaten	Region der Europäischen Union	Asien-Pazifik Süd

Kafka Broker	`casnb-0.citrix.com:9094`
	`casnb-1.citrix.com:9094`
	`casnb-2.citrix.com:9094`
	`casnb-3.citrix.com:9094`
		`casnb-eu-0.citrix.com:9094`
		`casnb-eu-1.citrix.com:9094`
		`casnb-eu-2.citrix.com:9094`
			`casnb-aps-0.citrix.com:9094`
			`casnb-aps-1.citrix.com:9094`
			`casnb-aps-2.citrix.com:9094`

> **Hinweis**
>
> Versuchen Sie, die Endpunktnamen und nicht die IP-Adressen zu verwenden. Die öffentlichen IP-Adressen der Endpunkte können sich ändern.

Citrix Analytics-Add-On für Splunk herunterladen und installieren

Sie können wählen, ob Sie das Add-on mithilfe **von App aus Datei installieren oder aus** der Splunk-Umgebung heraus installieren möchten.

App aus Datei installieren

1. Geh zu Splunkbase.
2. Laden Sie das Citrix Analytics-Add-on für Splunk-Datei herunter.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

3. Klicken Sie auf der Splunk-Web-Homepage neben **Apps**auf das Zahnradsymbol.
4. Klicken Sie auf **App aus Datei installieren**.
5. Suchen Sie die heruntergeladene Datei und klicken Sie auf **Hoch**

   Hinweise

   - Wenn Sie eine ältere Version des Add-Ons haben, wählen Sie **App aktualisieren** aus, um sie zu überschreiben.
   - Wenn Sie das **Citrix Analytics Add-on für Splunk** von einer Version vor 2.0.0 aktualisieren, müssen Sie die folgenden Dateien und Ordner im Ordner */bin* des Add-On-Installationsordners löschen und Ihre Splunk Forwarder- oder Splunk Standalone-Umgebung neu starten:

     ```
     - cd $SPLUNK_HOME$/etc/apps/TA_CTXS_AS/bin
     - rm -rf splunklib
     - rm -rf mac
     - rm -rf linux_x64
     - rm CARoot.pem
     - rm certificate.pem
     ```

6. Stellen Sie sicher, dass die App in der **Apps-Liste** angezeigt wird.

Installieren Sie die App von Splunk aus

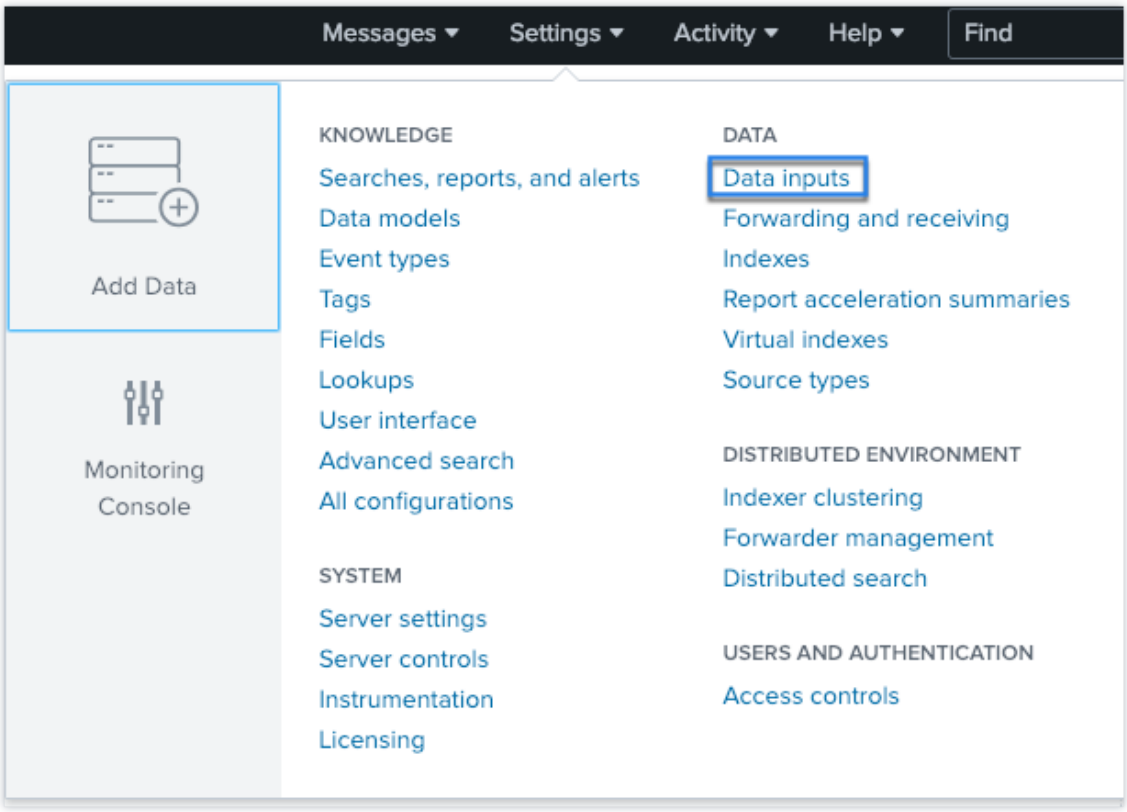
1. Klicken Sie auf der Splunk-Web-Homepage **auf+Weitere Apps suchen**.
2. Suchen Sie auf der Seite “Weitere Apps durchsuchen”im **Citrix Analytics Add-on nach Splunk**.
3. Klicken Sie neben der App auf **Installieren** .
4. Stellen Sie sicher, dass die App in der **Apps-Liste** angezeigt wird.

Konfigurieren des Citrix Analytics Add-Ons für Splunk

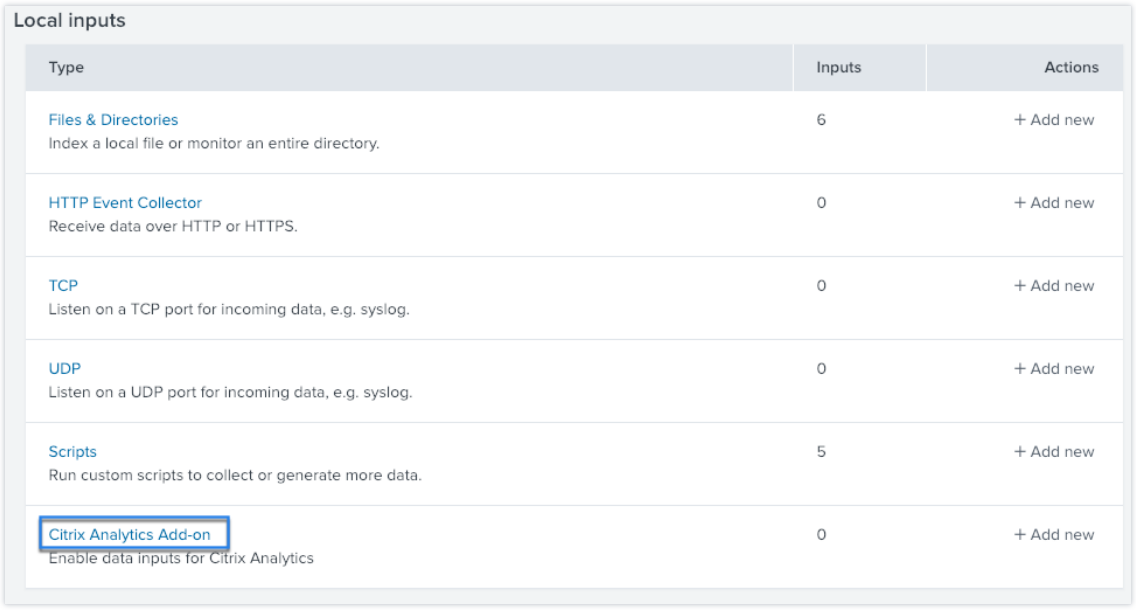
Konfigurieren Sie das Citrix Analytics-Add-On für Splunk mithilfe der Konfigurationsdetails von Citrix Analytics for Security. Nachdem das Add-On erfolgreich konfiguriert wurde, beginnt Splunk mit der Verwendung von Ereignissen von Citrix Analytics for Security.

1. Gehen Sie auf der Splunk Homepage zu **Einstellungen** > **Dateneingaben**.

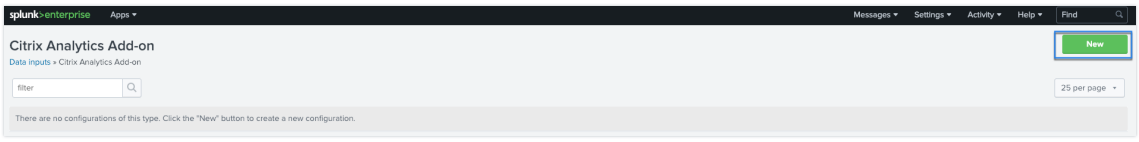
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



2. Klicken Sie im Abschnitt **Lokale Eingaben** auf **Citrix Analytics Add-on**.

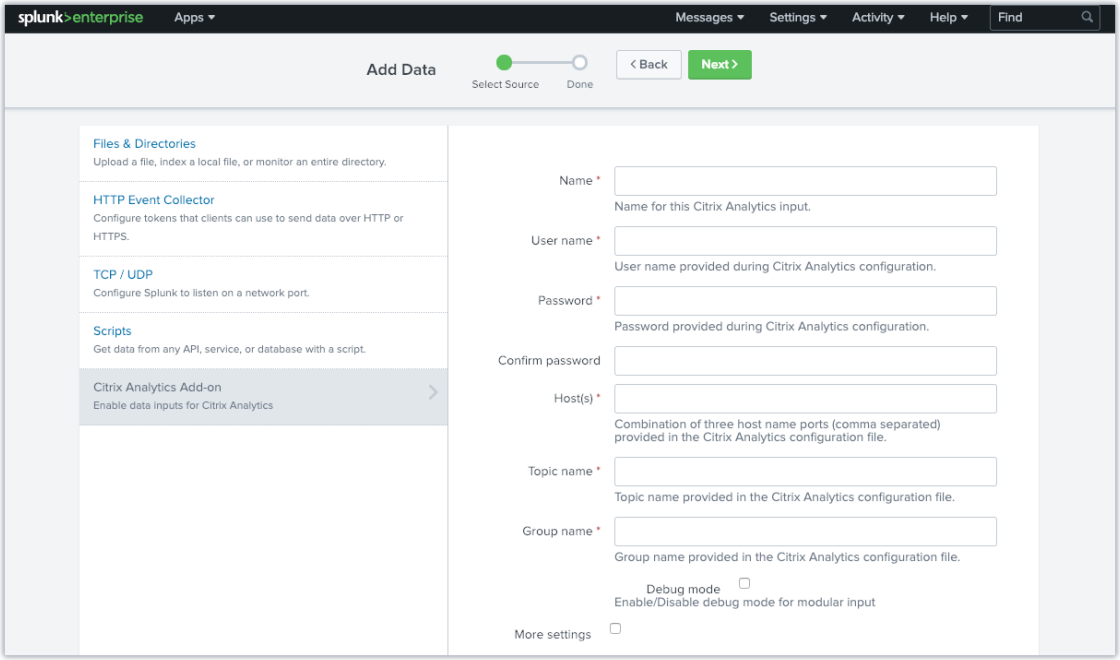


3. Klicken Sie auf **New**.

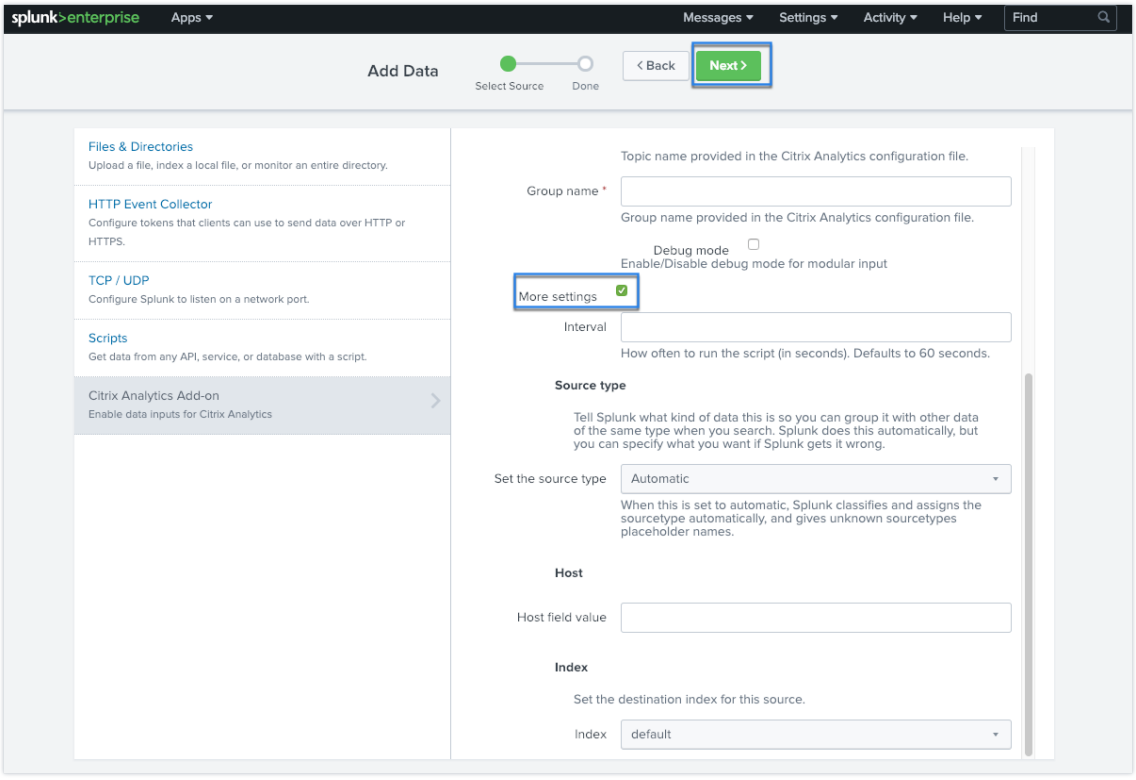


© 1999–2024 Cloud Software Group, Inc. All rights reserved.

4. Geben Sie auf der Seite **Daten hinzufügen** die Details ein, die in der Citrix Analytics-Konfigurationsdatei enthalten sind.



5. Um Ihre Standardeinstellungen anzupassen, klicken Sie auf **Weitere Einstellungen** und richten Sie die Dateneingabe ein. Sie können Ihren eigenen Splunk-Index, Hostnamen und Quelltyp definieren.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

6. Klicken Sie auf **Weiter**. Ihre Citrix Analytics-Dateneingabe wird erstellt und das Citrix Analytics-Add-On für Splunk wurde erfolgreich konfiguriert.

Citrix Analytics-Zusatzmodul für Splunk (Cloud)

Sie können unsere Splunk-Integration auf der folgenden Splunk-Version konfigurieren: Splunk 8.1 und höher.

Voraussetzungen

Das Citrix Analytics-Add-on für Splunk stellt eine Verbindung zu den folgenden IPs und ausgehenden Ports her, um eine Verbindung zu Citrix Analytics for Security herzustellen. Stellen Sie sicher, dass die folgenden IPs und ausgehenden Ports (abhängig von Ihrer Citrix Cloud-Region) in der Zulassungsliste in Ihrem Netzwerk enthalten sind. Informationen zur Konfiguration dieser IPs und ausgehenden Ports finden Sie im Abschnitt **Hinzufügen von Citrix Analytics-IPs und ausgehenden Ports zur Splunk Cloud-Zulassungsliste mithilfe des Admin Configuration Service (** ACS).

Region der Vereinigten Staaten	IP	Ausgehender Port	Region der Europäischen Union	IP	Ausgehender Port	Asien-Pazifik Süd	IP	Ausgehender Port
casnb-0 citrix.com	20.242.21.84	4094	casnb-de-0 citrix.com	20.229.150.91	4094	casnb-aps-0 citrix.com	20.211.0.214	4094
casnb-1.citrix.com	20.98.232.69	4094	casnb-eu-1.citrix.com	20.107.97.59	4094	casnb-aps-1 | citrix.com	20.211.38.102	4094
casnb-2.citrix.com	20.242.21.108	4094	casnb-eu-2.citrix.com	51.124.223.162	4094	casnb-aps-2 citrix.com	20.211.36.180	4094
casnb-3.citrix.com	20.242.57.14	4094						

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

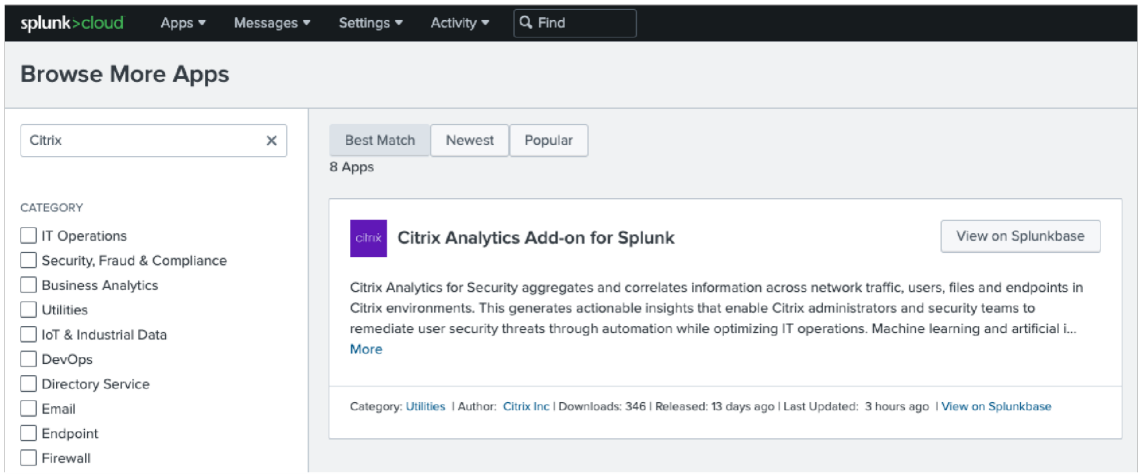
> **Hinweis:**
>
> Diese IPs können rotiert werden. Stellen Sie sicher, dass Ihre Liste der zugelassenen IP-Adressen mit den
> neuesten IPs aktualisiert wird, wie oben gezeigt.

Fügen Sie Citrix Analytics-IPs und ausgehende Ports mithilfe des Admin Configuration Service (ACS) zur Splunk Cloud-Zulassungsliste hinzu

1. Abhängig von Ihrer Citrix Cloud-Region müssen keine IP-Adressen zur Zulassungsliste hinzugefügt werden.
2. Aktivieren Sie den Admin Configuration Service (ACS) auf der Splunk Cloud Platform.
3. Erstellen Sie ein Token für die Zulassungsliste mit einem lokalen Konto mit Administratorrechten.
4. Führen Sie die Befehle cURL GET und POST aus, um Subnetze zur Zulassungsliste der jeweiligen Ports hinzuzufügen und zu überprüfen, ob sie erfolgreich hinzugefügt wurden.
5. Führen Sie die cURL-Befehle GET und POST aus, um ausgehende Ports zur Zulassungsliste hinzuzufügen und zu überprüfen, ob sie erfolgreich hinzugefügt wurden.

Citrix Analytics-Add-On für Splunk herunterladen und installieren

1. Gehen Sie zu **Apps > Weitere Apps finden > Suchen Sie nach dem Citrix Analytics-Add-on für Splunk**.

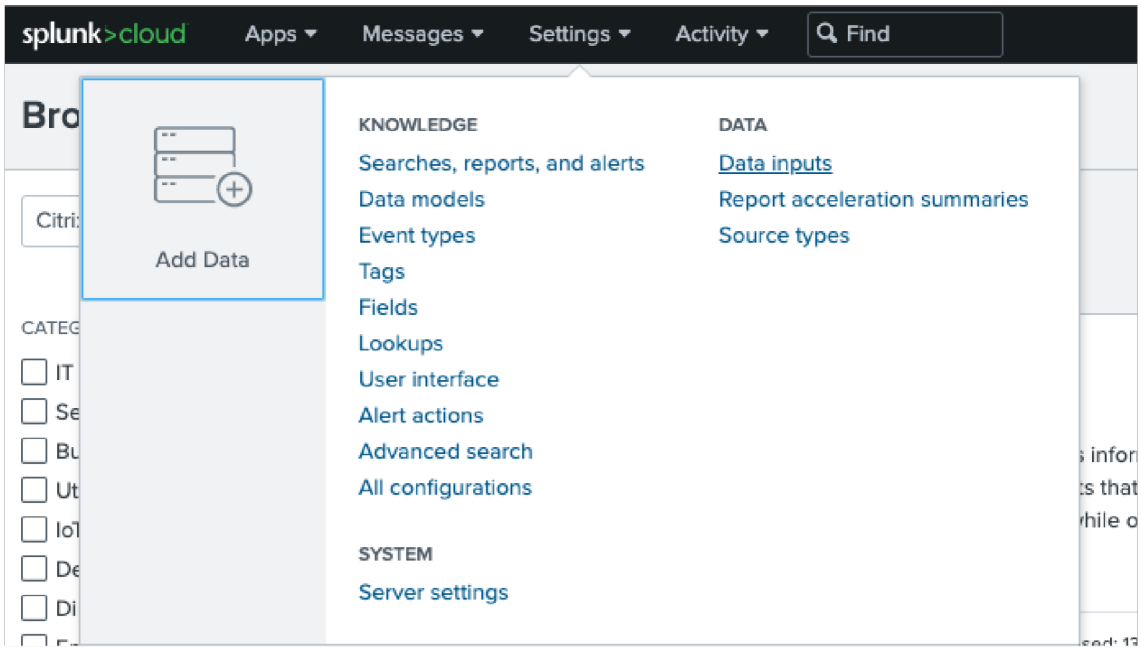


2. Installiere die App.
3. Stellen Sie sicher, dass die App in der Apps-Liste angezeigt wird.

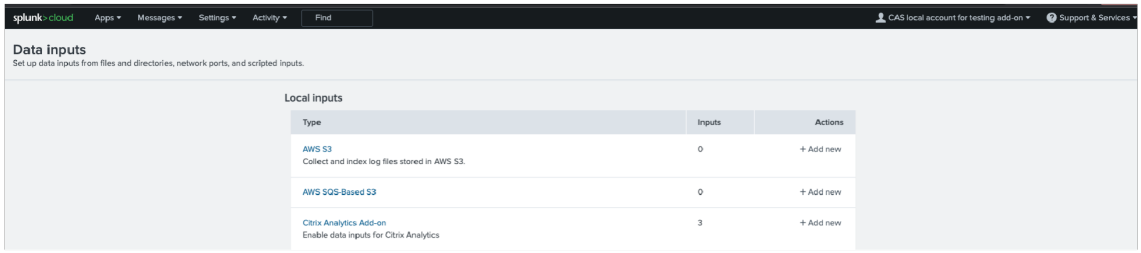
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Konfigurieren des Citrix Analytics Add-Ons für Splunk

1. Gehen Sie zu **Einstellungen > Dateneingaben > Citrix Analytics-Add-on**.

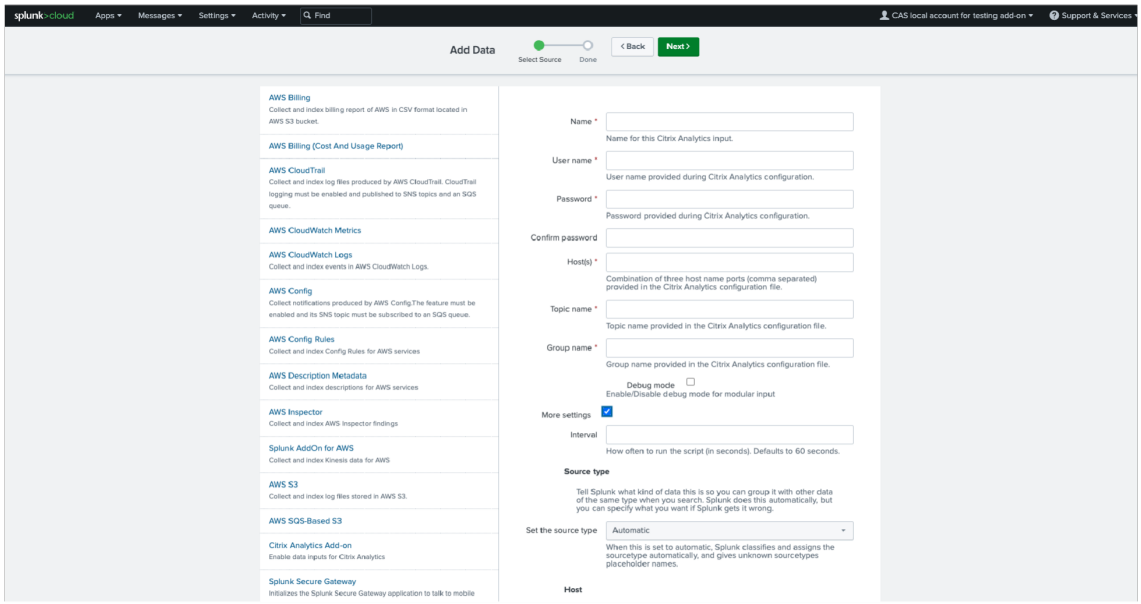


Fügen Sie die Eingabe hinzu: Splunk-Integration	Citrix Analytics für Sicherheit. Klicken Sie auf **Neu hinzufügen**.

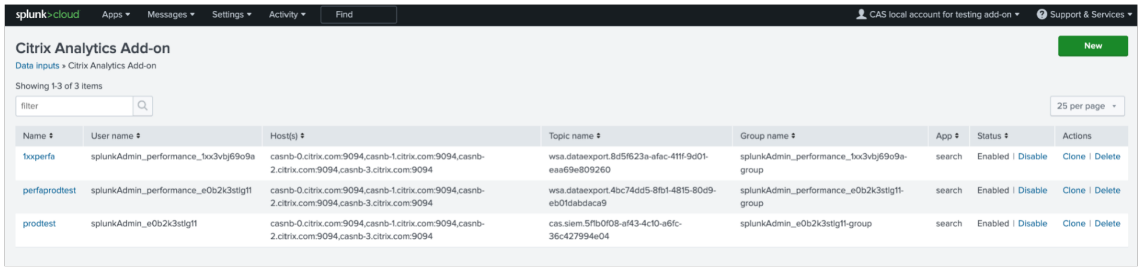
2. 

3. Konfigurieren Sie die Dateneingabe, indem Sie die auf der Seite **Citrix Analytics-Datenexporte** konfigurierten Details eingeben.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



4. Überprüfen Sie, ob Ihre Dateneingabe erfolgreich hinzugefügt wurde.

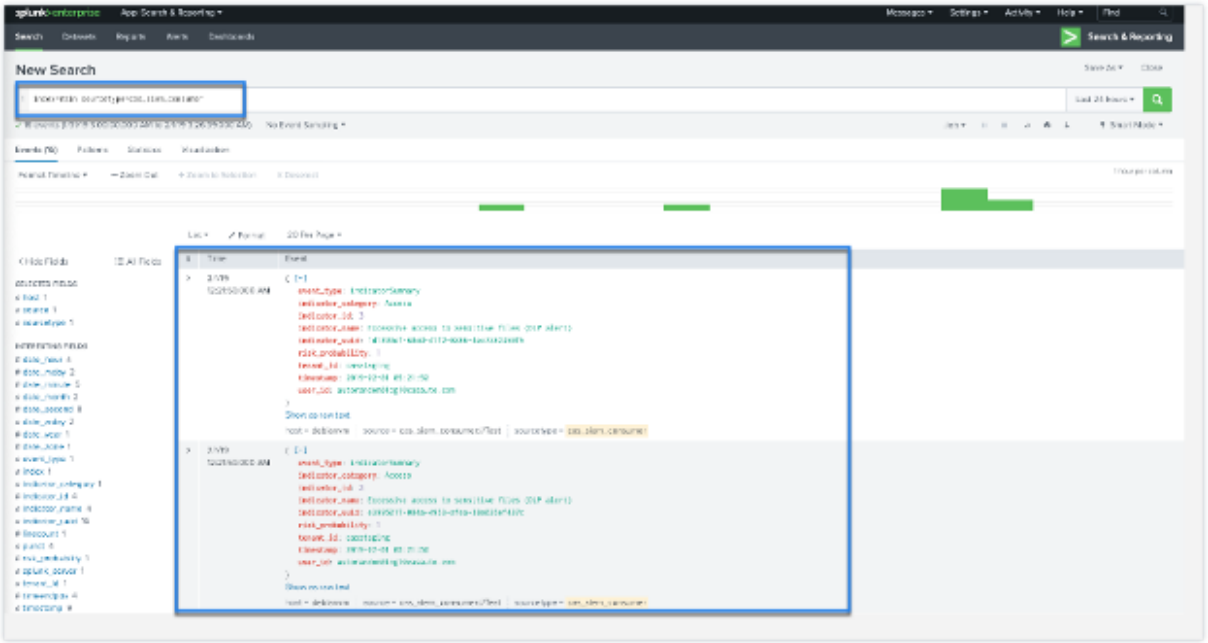


So nutzen Sie Ereignisse in Ihrer Splunk-Umgebung

Nachdem Sie das Add-On konfiguriert haben, ruft Splunk Risk Intelligence von Citrix Analytics for Security ab. Sie können mit der Suche nach den Ereignissen Ihrer Organisation im Splunk -Suchkopf basierend auf der konfigurierten Dateneingabe beginnen.

Die Suchergebnisse werden im folgenden Format angezeigt:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Eine Beispielausgabe:

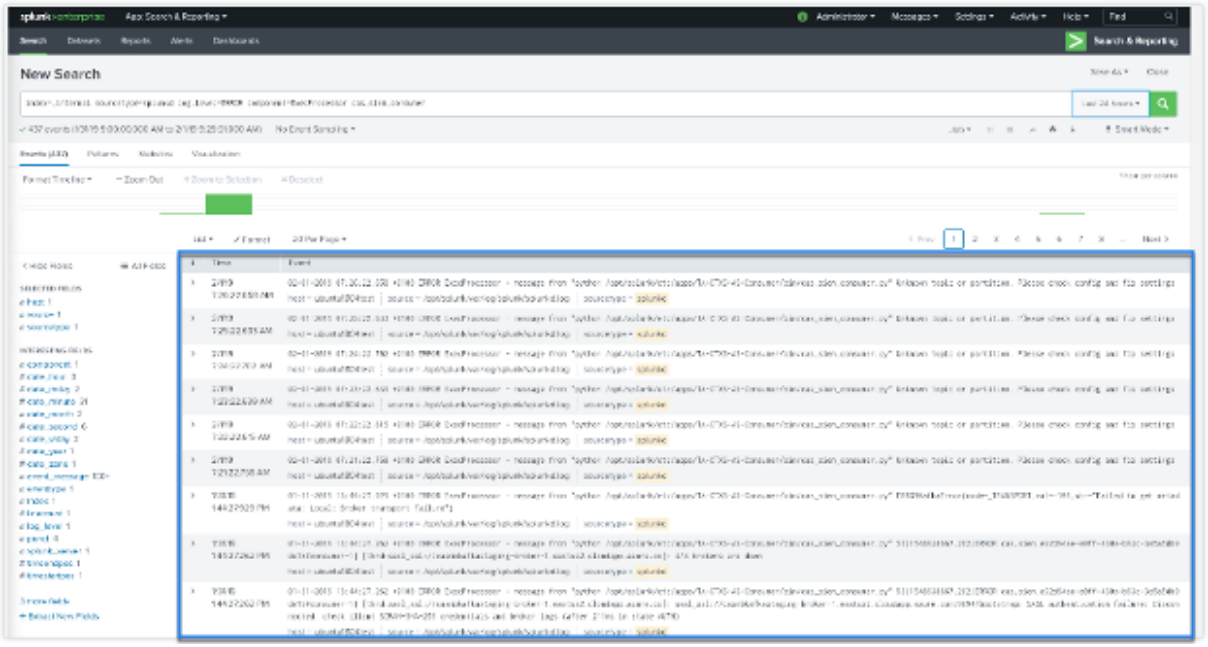
```
{"event_type": "indicatorSummary", "indicator_category": "Access",
"indicator_id": 200, "indicator_name": "Jailbroken / Rooted Device
Detected", "indicator_uuid": "1b97c3be-0000-000-0000-0000000000",
"risk_probability": 1.0, "tenant_id": "notcloud", "timestamp": "2017-11-16
23:59:59", "user_id": "testuser00001"}
```

Verwenden Sie die folgende Suchanfrage, um Probleme mit dem Add-On zu suchen und zu beheben:

```
index=_internal sourcetype=splunkd log_level=ERROR component=ExecProcessor
cas_siem_consumer
```

Die Ergebnisse werden im folgenden Format angezeigt:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Weitere Informationen zum Datenformat finden Sie unter Citrix Analytics-Datenformat für SIEM.

Problembehandlung beim Citrix Analytics-Add-On für Splunk

Wenn Sie keine Daten in Ihren Splunk-Dashboards sehen oder beim Konfigurieren des Citrix Analytics-Add-ons für Splunk Probleme auftreten, führen Sie die Debugging-Schritte aus, um das Problem zu beheben. Weitere Informationen finden Sie unter Konfigurationsprobleme mit dem Citrix Analytics-Add-on für Splunk.

> **Hinweis**
>
> Wenden Sie sich an CAS-PM-Ext@cloud.com, um Unterstützung für die Splunk-Integration, den Export von Daten nach Splunk anzufordern oder Feedback zu geben.

Citrix Analytics App für Splunk

> **Hinweis**
>
> Diese App befindet sich in der Vorschau.

Citrix Analytics App für Splunk ermöglicht es Splunk Enterprise-Administratoren, die von Citrix Analytics for Security gesammelten Benutzerdaten in Form von aufschlussreichen und umsetzbaren Dashboards auf Splunk anzuzeigen. Mithilfe dieser Dashboards erhalten Sie einen detaillierten Überblick über das riskante Verhalten der Benutzer in Ihrem Unternehmen und können rechtzeitig Maßnahmen ergreifen, um Insider-Bedrohungen abzuwehren. Sie können die von Citrix Analytics for Security gesammelten Daten auch mit anderen auf Ihrem Splunk konfigurierten Datenquellen

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

korrelieren. Diese Korrelation gibt Ihnen Einblick in die riskanten Aktivitäten der Benutzer aus verschiedenen Quellen und ergreift Maßnahmen zum Schutz Ihrer IT-Umgebung.

Unterstützte Splunk-Version

Die Citrix Analytics App für Splunk läuft auf den folgenden Splunk-Versionen:

- Splunk 9.0 64-Bit
- Splunk 8.2 64-Bit
- Splunk 8.1 64-Bit

Voraussetzungen für Citrix Analytics App für Splunk

- Installieren Sie das Citrix Analytics-Add-On für Splunk.
- Stellen Sie sicher, dass die für das Citrix Analytics-Add-On für Splunk genannten Voraussetzungen bereits erfüllt sind.
- Stellen Sie sicher, dass die Daten von Citrix Analytics for Security zu Splunk fließen.

Installation und Konfiguration

Wo installiere ich die App? Splunk Suchkopf

Wie installiere und konfiguriere ich die App? Sie können die Citrix Analytics App für Splunk installieren, indem Sie sie von Splunkbase herunterladen oder von Splunk aus installieren.

App aus Datei installieren

1. Geh zu Splunkbase.
2. Laden Sie die Datei Citrix Analytics App für Splunk herunter.
3. Klicken Sie auf der Splunk-Web-Homepage neben **Apps**auf das Zahnradsymbol.
4. Klicken Sie auf **App aus Datei installieren**.
5. Suchen Sie die heruntergeladene Datei und klicken Sie auf **Hoch**

   > **Hinweis**
   >
   > Wenn Sie eine ältere Version der App haben, wählen Sie **App aktualisieren** aus, um sie zu überschreiben.

6. Stellen Sie sicher, dass die App in der **Apps-Liste** angezeigt wird.

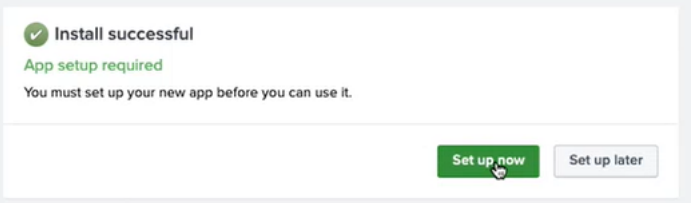
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Installieren Sie die App von Splunk aus

1. Klicken Sie auf der Splunk-Web-Homepage **auf+Weitere Apps suchen**.
2. Suchen Sie auf der Seite Weitere Apps durchsuchen die **Citrix Analytics App nach Splunk**.
3. Klicken Sie neben der App auf **Installieren** .

Konfigurieren Sie Ihren Index und Ihren Quelltyp, um Daten zu korrelieren

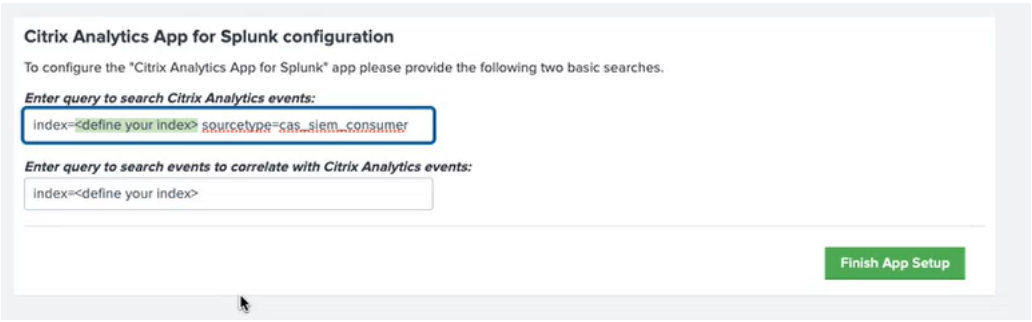
1. Nachdem Sie die App installiert haben, klicken Sie auf **Jetzt einrichten**.



2. Geben Sie die folgenden Abfragen ein:
   - Index und Quelltyp, in dem die Daten von Citrix Analytics for Security gespeichert werden.

     > **Hinweis**
     >
     > Diese Abfragewerte müssen mit den im Citrix Analytics-Add-On für Splunk angegebenen übereinstimmen. Weitere Informationen finden Sie unter Konfigurieren des Citrix Analytics-Add-ons für Splunk.

   - Index, von dem aus Sie Ihre Daten mit Citrix Analytics for Security korrelieren möchten.



3. Klicken Sie auf **App-Setup beenden**, um die Konfiguration abzuschließen.

Nachdem Sie die Citrix Analytics App für Splunk konfiguriert und eingerichtet haben, verwenden Sie die Citrix Analytics-Dashboards, um die Benutzerereignisse auf Ihrem Splunk anzuzeigen.

Weitere Informationen zur Splunk-Integration finden Sie unter den folgenden Links:

- Citrix Analytics-Integration mit Splunk
- Die Citrix Analytics-App für Splunk, jetzt in Splunkbase

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Splunk-Architektur mit Citrix Analytics als Add-On

February 14, 2023

Splunk folgt einer Architektur, die die folgenden drei Ebenen enthält:

- Sammlung
- Indizierung
- Suchen

Splunk unterstützt eine Vielzahl von Datenerfassungsmechanismen, mit denen Daten einfach in Splunk aufgenommen werden können, sodass sie indexiert und für die Suche verfügbar gemacht werden können. Diese Stufe ist nichts anderes als Ihr Heavy Forwarder oder Universal Forwarder.

Sie müssen die Zusatzanwendung auf der Heavy-Forwarder-Ebene statt auf der universellen Forwarder-Ebene installieren. Denn mit wenigen Ausnahmen für gut strukturierte Daten (wie json, csv, tsv) analysiert der Universal Forwarder Protokollquellen nicht in Ereignisse und kann daher keine Aktion ausführen, für die ein Verständnis des Protokollformats erforderlich ist.

Es wird auch mit einer abgespeckten Version von Python geliefert, wodurch es nicht mit modularen Eingabeanwendungen kompatibel ist, für deren Funktion ein vollständiger Splunk-Stack erforderlich ist. Der Heavy Forwarder nichts anderes als deine Sammelstufe.

Der Hauptunterschied zwischen einem Universal Forwarder und einem Heavy Forwarder besteht darin, dass der Heavy Forwarder die vollständige Parsing-Pipeline enthält und dieselben Funktionen ausführt, die ein Indexer ausführt, ohne Ereignisse tatsächlich auf den Datenträger zu schreiben und zu indizieren. Dies ermöglicht es dem Heavy Forwarder, einzelne Ereignisse wie das Maskieren von Daten, das Filtern und Routing auf der Grundlage von Ereignisdaten zu verstehen und darauf zu reagieren. Da die Zusatzanwendung über eine vollständige Splunk Enterprise-Installation verfügt, kann sie modulare Eingaben hosten, die einen vollständigen Python-Stack für eine korrekte Datenerfassung benötigen, oder als Endpunkt für den Splunk HTTP Event Collector (HEC) fungieren.

Sobald die Daten gesammelt sind, werden sie indexiert oder verarbeitet und so gespeichert, dass sie durchsuchbar sind.

Die wichtigste Methode für Kunden, ihre Daten zu erkunden, ist die Suche. Eine Suche kann als Bericht gespeichert und zur Stromversorgung von Dashboard-Panels verwendet werden. Suchen sind das Extrahieren von Informationen aus Ihren Daten.

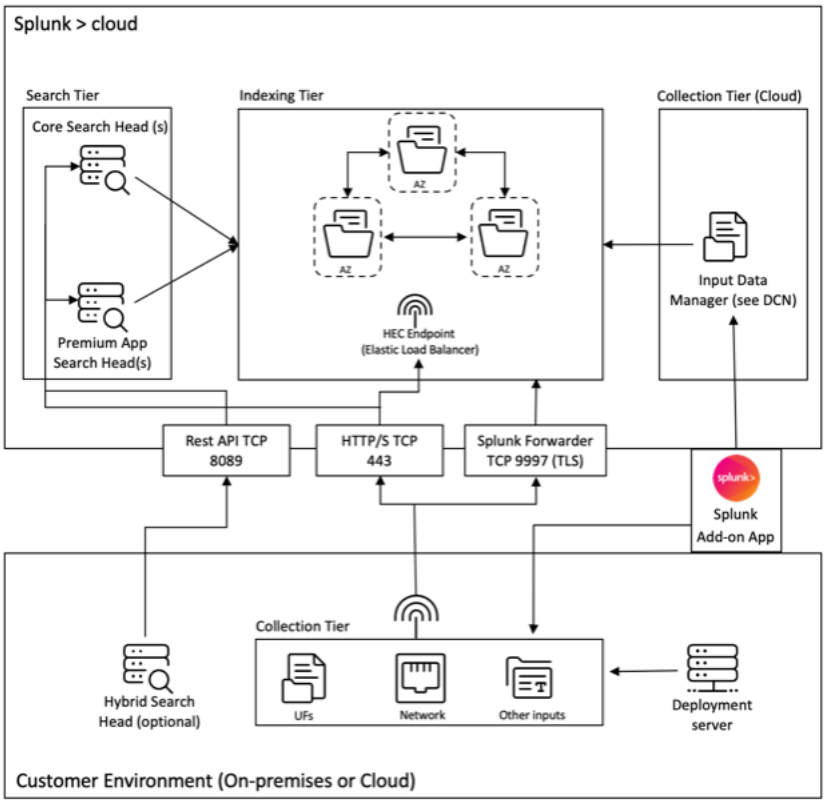
Im Allgemeinen wird die Splunk-Add-On-Anwendung auf der Collection-Ebene (auf Splunk-Unternehmensebene) bereitgestellt, wohingegen unsere Dashboarding-Anwendung auf der Suchebene (auf Splunk Cloud-Ebene) bereitgestellt wird. Bei einem einfachen lokalen Setup können Sie all diese drei Ebenen auf einem einzigen Splunk-Host haben (bekannt als Single Server

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Deployment).

Die Sammlungsstufe ist eine viel bessere Möglichkeit, die Zusatzanwendung für Splunk zu verwenden. Es gibt zwei Möglichkeiten, die Zusatzanwendung zu installieren. Entweder können Sie es auf der Erfassungsebene in der Kundenumgebung oder im Eingabedatenmanager unter der **Splunk Cloud-Instanz**installieren.

Sehen Sie sich das folgende Diagramm an, um die Splunk-Bereitstellungsarchitektur mit unserer Zusatzanwendung zu verstehen:



Der im oben genannten Diagramm gezeigte Inputs Data Manager (IDM) ist die von Splunk Cloud verwaltete Implementierung eines Data Collection Node (DCN), der nur skriptbasierte und modulare Eingaben unterstützt. Für darüber hinausgehende Datenerfassungsanforderungen können Sie mithilfe eines Splunk Heavy Forwarders ein DCN in Ihrer Umgebung bereitstellen und verwalten.

Splunk ermöglicht das Sammeln, Indexieren und Suchen von Daten aus verschiedenen Quellen. Eine Möglichkeit, Daten zu sammeln, sind APIs, die es Splunk ermöglichen, auf Daten zuzugreifen, die in anderen Systemen oder Anwendungen gespeichert sind. Diese APIs können REST, Webdienste, JMS und/oder JDBC als Abfragemechanismus enthalten. Splunk und alle Drittanbieter-Entwickler bieten eine Reihe von Anwendungen an, die API-Interaktionen über das modulare Splunk-Eingabeframework ermöglichen. Diese Anwendungen erfordern in der Regel eine vollständige Installation der Splunk-Unternehmenssoftware, um ordnungsgemäß zu funktionieren.

Um die Erfassung von Daten über APIs zu erleichtern, ist es üblich, einen Heavy Forwarder als DCN

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

einzusetzen. Heavy Forwarders sind mächtigere Agenten als Universal Forwarders, da sie die gesamte Parsing-Pipeline enthalten und einzelne Ereignisse verstehen und darauf reagieren können. Auf diese Weise können sie Daten über APIs sammeln und verarbeiten, bevor sie zur Indizierung an eine Splunk-Instanz weitergeleitet werden.

Weitere Informationen zur übergeordneten Architektur einer Splunk Cloud-Bereitstellung finden Sie unter Splunk Validated Architectures.

Citrix Analytics-Dashboards für Splunk

December 12, 2023

> **Hinweis**
>
> **Achtung**: Citrix Content Collaboration und ShareFile haben das Ende ihrer Lebensdauer erreicht und stehen Benutzern nicht mehr zur Verfügung.
>
> Dieses Feature ist als Preview verfügbar.

Voraussetzung

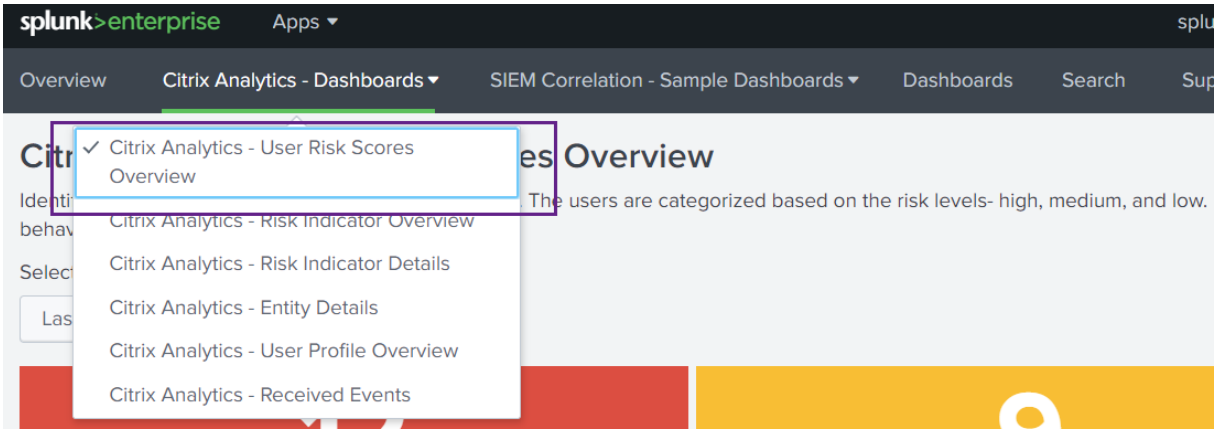
Um die folgenden Citrix Analytics Dashboards zu verwenden, stellen Sie sicher, dass Sie die Citrix Analytics App für Splunkbereits konfiguriert und eingerichtet haben.

Überblick über den Risiko-Score

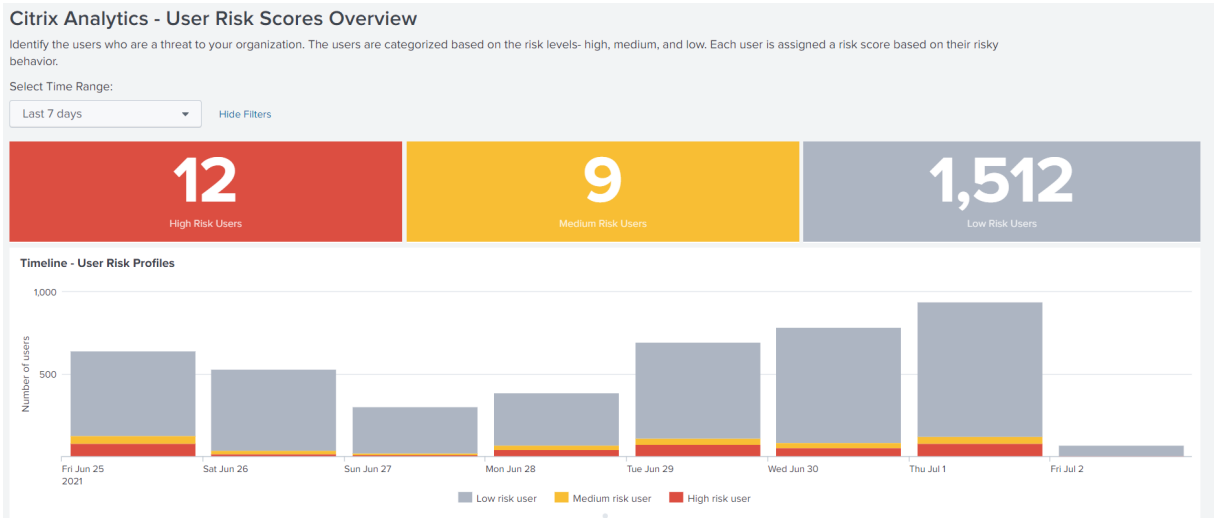
Dieses Dashboard bietet eine konsolidierte Ansicht der riskanten Benutzer in Ihrem Unternehmen. Die Benutzer werden nach den Risikoniveaus kategorisiert - hoch, mittel und niedrig. Die Risikostufen basieren auf den Anomalien in den Benutzeraktivitäten und dementsprechend wird ein Risiko-Score zugewiesen. Weitere Informationen zu den Arten riskanter Benutzer finden Sie im Benutzer-Dashboard.

Um dieses Dashboard anzuzeigen, klicken Sie auf **Citrix Analytics- Dashboards > Citrix Analytics-Übersicht über Benutzerrisikobewertungen**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Wählen Sie einen voreingestellten Zeitraum oder einen benutzerdefinierten Zeitraum aus, um die Zeitleiste der riskanten Benutzer und ihre Details anzuzeigen.



Die Tabelle Riskante Benutzer enthält die folgenden Informationen:

- **Benutzer**: Zeigt den Benutzernamen an. Klicken Sie auf einen Benutzernamen, um die Details zum riskanten Verhalten des Benutzers im Dashboard Citrix Analytics - Entitätsdetails anzuzeigen.
- **Gefundene Risiken für gefährdete Endpunkte**: Gibt die Anzahl der vom Benutzer ausgelösten Risikoindikatoren an, die zur Risikokategorie kompromittierter Endpunkte gehören.
- **Gefundene Risiken für gefährdete Benutzer**: Gibt die Anzahl der vom Benutzer ausgelösten Risikoindikatoren an, die zur Risikokategorie kompromittierter Benutzer gehören.
- **Gefundene Datenexfiltrationsrisiken**: Gibt die Anzahl der vom Benutzer ausgelösten Risikoindikatoren an, die zur Risikokategorie der Datenexfiltration gehören.
- **Gefundene Risiken für Insider-Bedrohungen**: Gibt die Anzahl der vom Benutzer ausgelösten Risikoindikatoren an, die zur Risikokategorie für Insider-Bedrohungen gehören.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Risiko-Score**: Zeigt den Risiko-Score des Benutzers an.

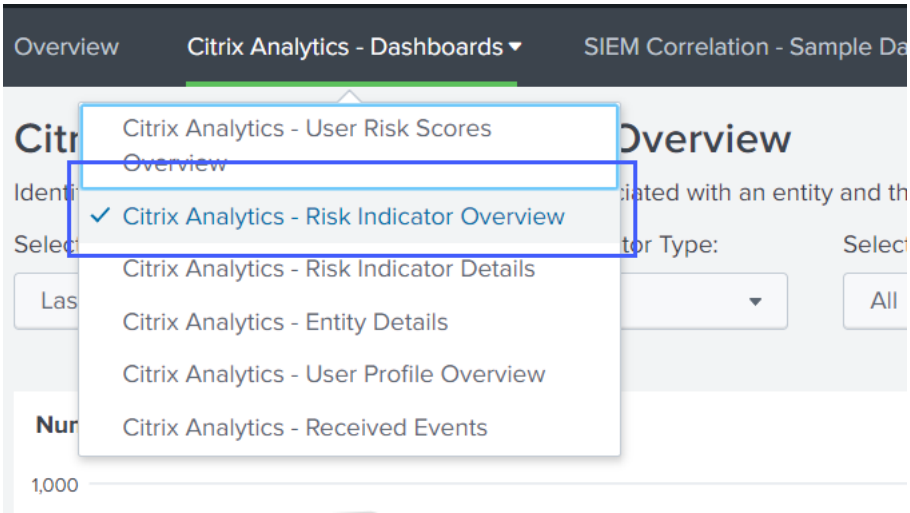
Sie können einen Benutzer auch nach dem Benutzernamen suchen und die erforderlichen Details abrufen.

Weitere Informationen finden Sie unter Risikokategorien.

Überblick über Risikoindikatoren

Das Dashboard bietet eine konsolidierte Ansicht der von den Benutzern in Ihrem Unternehmen ausgelösten Risikoindikatoren.

Um das Dashboard anzuzeigen, klicken Sie auf **Citrix Analytics- Dashboards > Citrix Analytics-Risikoindikatorübersicht**.



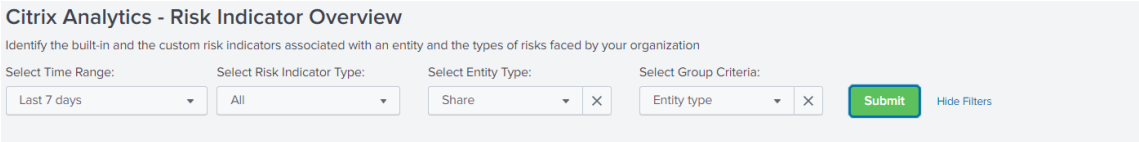
Wählen Sie eine Kategorie, um den Bericht anzuzeigen

Suchen Sie die Risikoindikatoren, indem Sie eine oder mehrere Kategorien auswählen:

- **Zeitraum**: Wählen Sie einen voreingestellten Zeitraum oder einen benutzerdefinierten Zeitraum aus, um die ausgelösten Risikoindikatoren für diesen Zeitraum anzuzeigen.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Risikoindikatortyp**: Wählen Sie die Art des Risikoindikators: eingebaut oder benutzerdefiniert.
- **Entitätstyp**: Wählen Sie einen Benutzer aus, um die zugehörigen Risikoindikatoren anzuzeigen.
- **Gruppe**: Wählen Sie ein Kriterium aus, um die Benutzerereignisse nach Datenquelle, Indikatorkategorie, Indikatorname, Indikatortyp oder Entity-Art zu gruppieren und die zugehörigen Risikoindikatoren anzuzeigen.

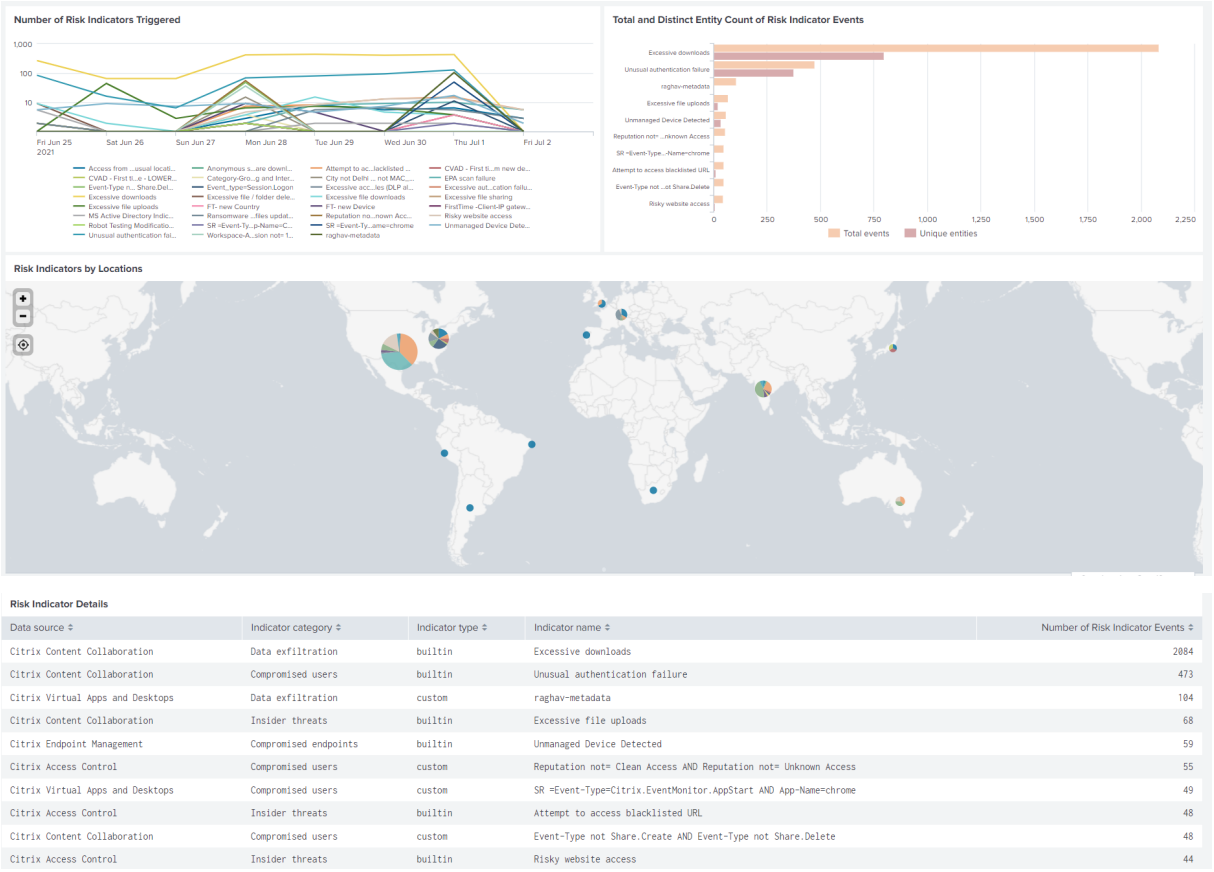


Bericht ansehen

Verwenden Sie die folgenden Berichte, um Details zu den Risikoindikatoren anzuzeigen, indem Sie eine oder mehrere Kategorien auswählen:

- **Anzahl der ausgelösten Risikoindikatoren**: Zeigt die Anzahl der für den ausgewählten Zeitraum ausgelösten Risikoindikatoren an. Verwenden Sie diesen Bericht, um das Muster und die Bereiche riskanter Aktivitäten zu identifizieren. Identifizieren Sie außerdem die riskanten Aktivitäten in Ihrem Unternehmen.
- **Gesamtzahl und eindeutige Anzahl von Risikoindikatorereignissen**: Zeigt die Gesamtereignisse und die eindeutigen Ereignisse an, die einem Risikoindikator entsprechen. Verwenden Sie diesen Bericht, um das Auftreten der einzelnen Risikoindikatoren und der wichtigsten Risikoindikatoren in Ihrer Organisation zu ermitteln. Sie können auch ermitteln, wie viele einzelne Benutzer einen bestimmten Risikoindikator ausgelöst haben, und überprüfen, ob der Risikoindikator von einer größeren oder einer kleineren Benutzergruppe ausgelöst wird.
- **Risikoindikatoren nach Standorten**: Zeigt die Anzahl der Risikoindikatoren an, die von den Benutzern standortübergreifend ausgelöst werden. Verwenden Sie diesen Bericht, um die Standorte zu identifizieren, die riskantere Aktivitäten zeigen, und um zu überprüfen, ob sich die Standorte außerhalb des Betriebsbereichs Ihrer Organisation befinden.
- **Risikoindikatordetails**: Zeigt die Details zum Risikoindikator an, z. B. die zugehörige Datenquelle, die Indikatorkategorie, den Indikatortyp und die Anzahl der Vorkommnisse.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



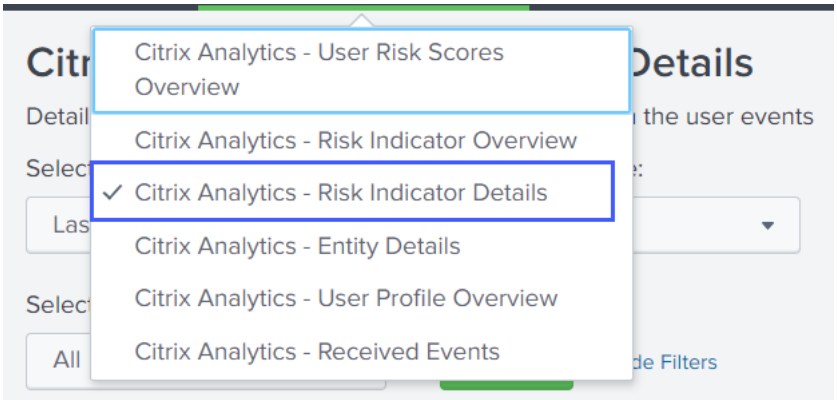
Risk Indicator Details

Data source	Indicator category	Indicator type	Indicator name	Number of Risk Indicator Events
Citrix Content Collaboration	Data exfiltration	builtin	Excessive downloads	2084
Citrix Content Collaboration	Compromised users	builtin	Unusual authentication failure	473
Citrix Virtual Apps and Desktops	Data exfiltration	custom	raghav-metadata	104
Citrix Content Collaboration	Insider threats	builtin	Excessive file uploads	68
Citrix Endpoint Management	Compromised endpoints	builtin	Unmanaged Device Detected	59
Citrix Access Control	Compromised users	custom	Reputation not= Clean Access AND Reputation not= Unknown Access	55
Citrix Virtual Apps and Desktops	Compromised users	custom	SR =Event-Type=Citrix.EventMonitor.AppStart AND App-Name=chrome	49
Citrix Access Control	Insider threats	builtin	Attempt to access blacklisted URL	48
Citrix Content Collaboration	Compromised users	custom	Event-Type not Share.Create AND Event-Type not Share.Delete	48
Citrix Access Control	Insider threats	builtin	Risky website access	44

Angaben zu Risikoindikatoren

Das Dashboard bietet detaillierte Informationen zu den integrierten und benutzerdefinierten Risikoindikatoren, die von den Benutzern ausgelöst werden. Weitere Informationen finden Sie unter Citrix Benutzerrisikoindikatoren und Benutzerdefinierte Risikoindikatoren.

Um das Dashboard anzuzeigen, klicken Sie auf **Citrix Analytics** —**Dashboards > Citrix Analytics** — **Risikoindikator-Details**.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Wählen Sie eine Kategorie aus, um die Berichte anzuzeigen

Zeigen Sie die Details der Risikoindikatoren an, indem Sie eine oder mehrere Kategorien auswählen:

- **Zeitraum**: Wählen Sie einen voreingestellten Zeitraum oder einen benutzerdefinierten Zeitraum aus, um die Details der ausgelösten Risikoindikatoren für diesen Zeitraum anzuzeigen.
- **Entitätstyp**: Wählen Sie einen Benutzer aus, um die Details der zugehörigen Risikoindikatoren anzuzeigen.
- **Risikoindikatortyp**- Wählen Sie die Art des integrierten oder benutzerdefinierten Risikoindikators aus, um deren Details anzuzeigen.
- **Datenquelle**- Wählen Sie die Datenquelle aus, um die Details der zugehörigen Risikoindikatoren anzuzeigen.
- **Risikoindikatorkategorie**- Wählen Sie die Risikokategorie aus, um die Details der zugehörigen Risikoindikatoren anzuzeigen.
- **Risikoindikator**- Wählen Sie den Risikoindikator aus, um seine Details anzuzeigen

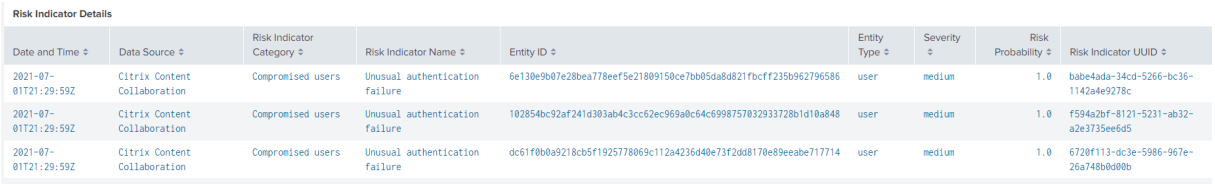
Sehen Sie sich die Berichte an

Wählen Sie beispielsweise aus der Liste Risikoindikator auswählen die Option **Ungewöhnlicher Authentifizierungsfehler (Citrix Content Collaboration)**aus, klicken Sie auf **Senden**, und zeigen Sie die folgenden Informationen an:

- Die 10 wichtigsten Benutzer, die mit dem Risikoindikator in Verbindung stehen
- Details zum Risikoindikator wie
  - Datum und Uhrzeit des Triggers
  - Zugehörige Datenquelle
  - Zugehörige Risiko
  - Zugeordnete Entitäts-ID und Benutzerentitstyp
  - Schweregrad des Risikos —hoch, mittel oder niedrig
  - Risikowahrscheinlichkeit des Benutzerereignisses
  - Eindeutige Identität des Risikoindikators (UUID)

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Klicken Sie **unter Top 10 Entitäten nach Risikoindikatoren**auf eine Entität, um deren Details im **Citrix Analytics-Dashboard "Entitätsdetails** "anzuzeigen.



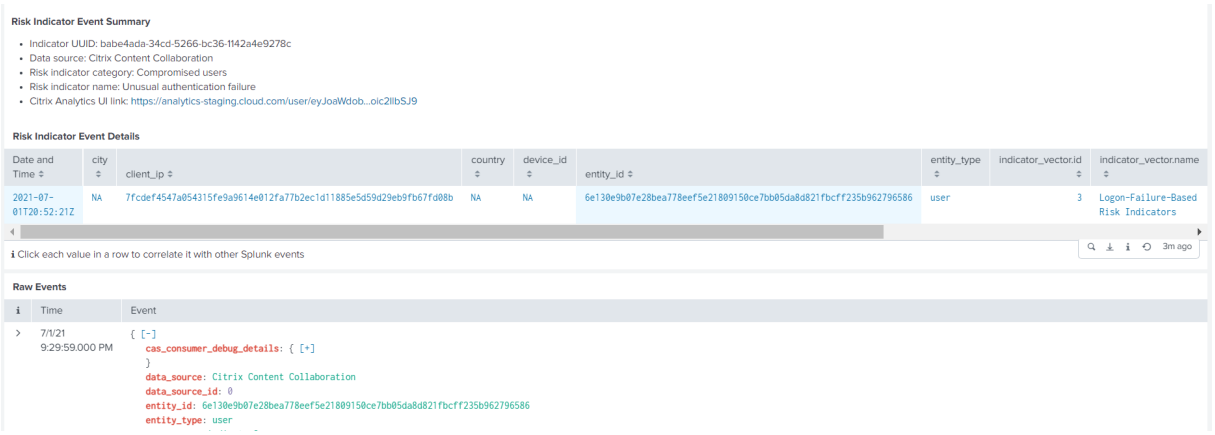
Risk Indicator Details

Date and Time	Data Source	Risk Indicator Category	Risk Indicator Name	Entity ID	Entity Type	Severity	Risk Probability	Risk Indicator UUID
2021-07-01T21:29:59Z	Citrix Content Collaboration	Compromised users	Unusual authentication failure	6e130e9b07e28bea778eef5e21809150ce7bb05da8d821fbcff235b962796586	user	medium	1.0	babe4ada-34cd-5266-bc36-1142a4e9278c
2021-07-01T21:29:59Z	Citrix Content Collaboration	Compromised users	Unusual authentication failure	102854bc92af241d303ab4c3cc62ec969a0c64c69985757032933728b1d10a848	user	medium	1.0	f594a2bf-8121-5231-ab32-a2e3735ee6d5
2021-07-01T21:29:59Z	Citrix Content Collaboration	Compromised users	Unusual authentication failure	dc61f0b0a9218cb5f1925778069c112a4236d40e73f2dd8170e89eeabe717714	user	medium	1.0	6720f113-dc3e-5986-967e-26a748b0d00b

Klicken Sie auf jede Zeile der Tabelle mit den **Risikoindikatordetails**, um die Ereigniszusammenfassung, die Ereignisdetails und die Rohereignisse des ausgewählten Risikoindikators anzuzeigen.

Klicken Sie im Abschnitt **Risikoindikator-Ereignisübersicht** auf den **Link Citrix Analytics UI**, um von Ihrem Splunk aus direkt zur Benutzerzeitleiste in Citrix Analytics for Security zu gelangen. Zeigen Sie auf der Benutzerzeitleiste den Risikoindikator, die zugehörigen Ereignisse und alle angewendeten Aktionen für den Benutzer an.

Weitere Informationen zur Ereigniszusammenfassung und Ereignisdetails finden Sie unter Citrix Analytics data format for SIEM.



Risk Indicator Event Summary

- Indicator UUID: babe4ada-34cd-5266-bc36-1142a4e9278c
- Data source: Citrix Content Collaboration
- Risk indicator category: Compromised users
- Risk indicator name: Unusual authentication failure
- Citrix Analytics UI link: https://analytics-staging.cloud.com/user/eyJoaWdob...oic2libSJ9

Risk Indicator Event Details

Date and Time	city	client_ip	country	device_id	entity_id	entity_type	indicator_vector.id	indicator_vector.name
2021-07-01T20:52:21Z	NA	7fcdef4547a054315fe9a9614e012fa77b2ec1d11885e5d59d29eb9fb67fd08b	NA	NA	6e130e9b07e28bea778eef5e21809150ce7bb05da8d821fbcff235b962796586	user	3	Logon-Failure-Based Risk Indicators

Click each value in a row to correlate it with other Splunk events

3m ago

Raw Events

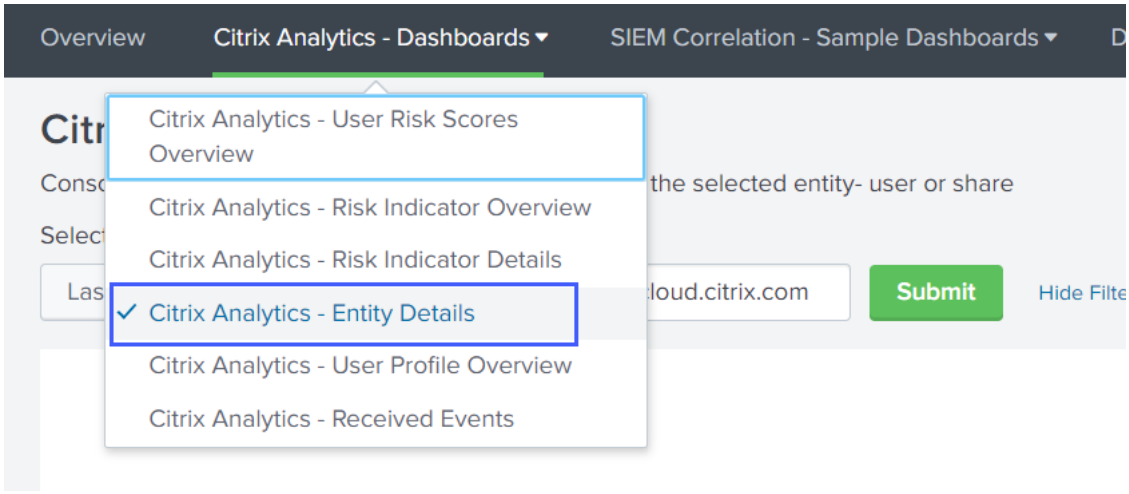
Time	Event
7/1/21 9:29:59.000 PM	{ [-] cas_consumer_debug_details: { [+] } data_source: Citrix Content Collaboration data_source_id: 0 entity_id: 6e130e9b07e28bea778eef5e21809150ce7bb05da8d821fbcff235b962796586 entity_type: user

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Angaben zum Unternehmen

Verwenden Sie das Dashboard, um die Details zu einem Benutzer einer Benutzerentität und seinem riskanten Verhalten anzuzeigen.

Um das Dashboard anzuzeigen, klicken Sie auf **Citrix Analytics- Dashboards > Citrix Analytics- Entitätsdetails**.

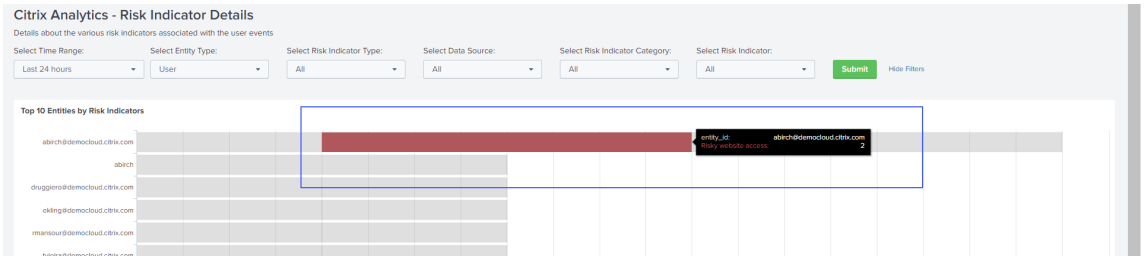


Sehen Sie sich den Bericht an

Geben Sie einen Zeitraum und die Entität (Benutzername) ein und klicken Sie auf **Senden**, um die detaillierten Informationen anzuzeigen.

Alternativ können Sie die detaillierten Informationen zu einer Entität auch in den folgenden Dashboards anzeigen:

- Wechseln Sie in **Citrix Analytics - Risikoindikatordetails**zu **Top 10 Entitäten nach Risikoindikatoren**, und klicken Sie auf eine Entität.

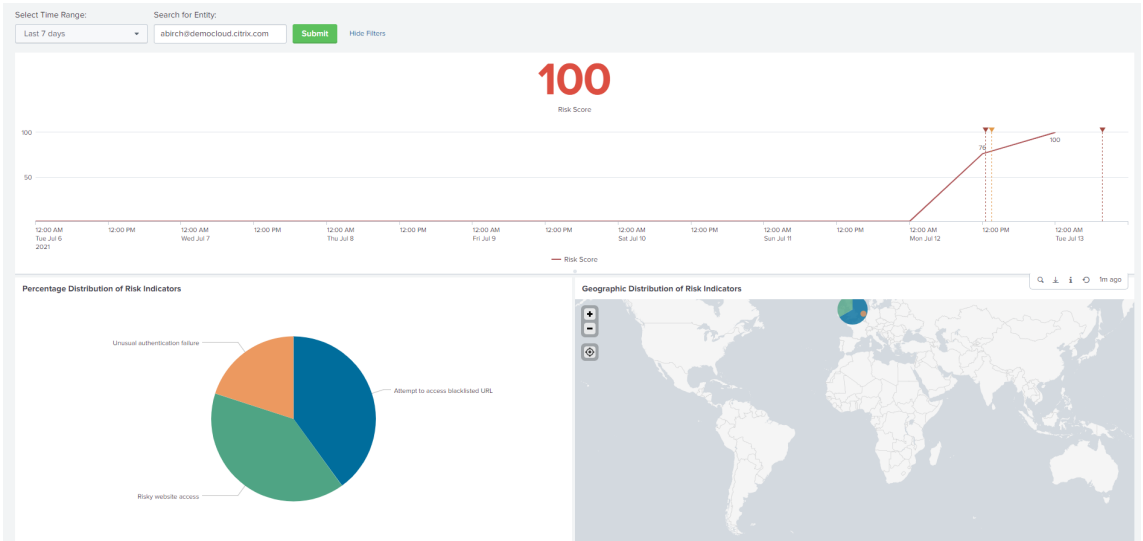


- Wechseln Sie in **Citrix Analytics - Risk Score Overview**zu **Risky Users**, und klicken Sie auf einen Benutzernamen.

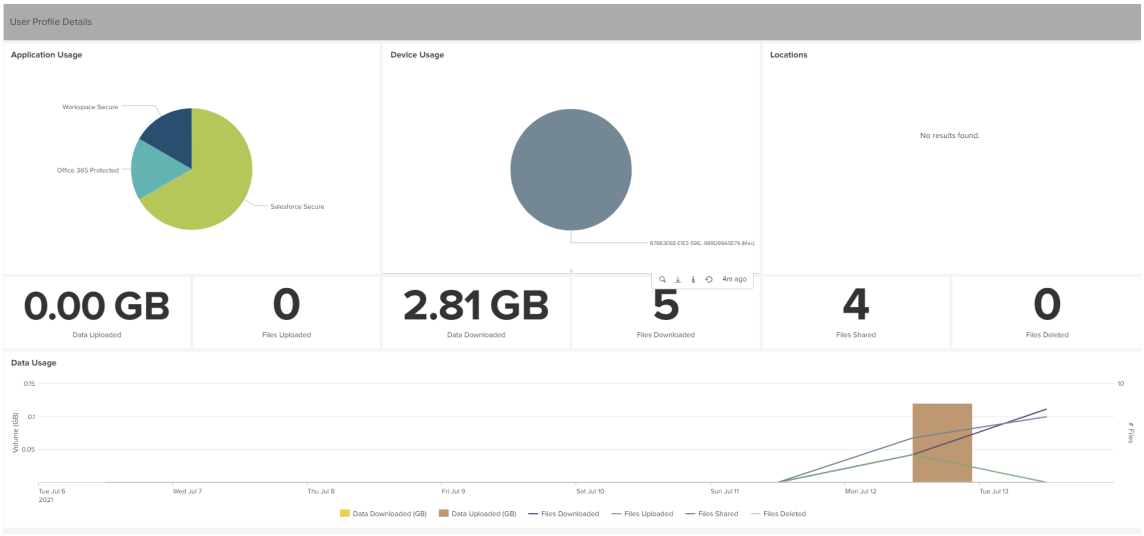
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Die folgenden detaillierten Informationen werden angezeigt:

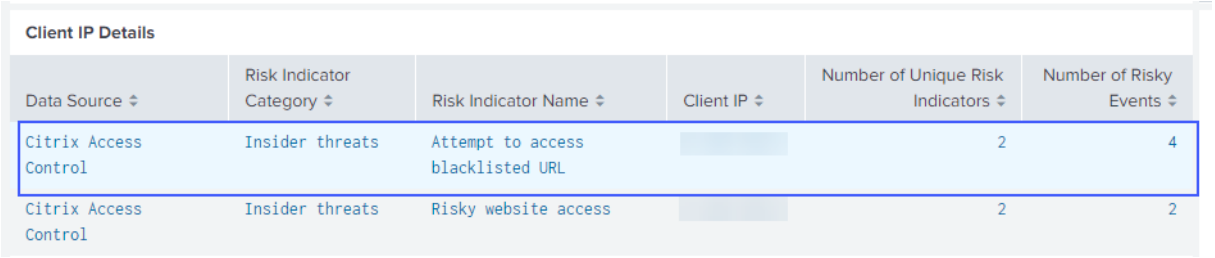
- Aktueller Risiko-Score und der Zeitplan für die Risikobewertung für den ausgewählten Zeitraum.
- Prozentuale Verteilung der Risikoindikatoren. Hilft Ihnen, das Muster riskanter Aktivitäten des Unternehmens zu analysieren.
- Geografische Verteilung der Risikoindikatoren. Hilft Ihnen, ungewöhnliche und risikoreiche Standorte zu identifizieren.
- Kunden-IP-Details im Zusammenhang mit den riskanten Aktivitäten.
- Benutzergerätedetails, die mit den riskanten Aktivitäten verbunden sind.
- Details zu Risikoindikatoren wie zugehörige Datenquelle, Risikokategorie, Risikoschweregrad usw.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.



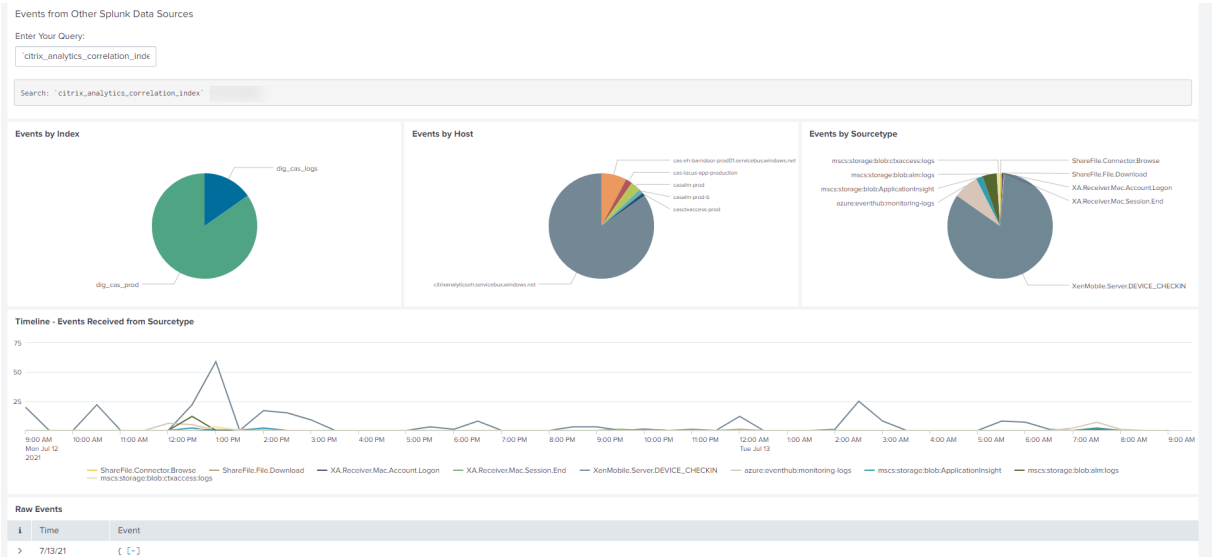
Korrelieren Sie die Client-IPs und Benutzergeräte, die mit riskanten Aktivitäten verknüpft sind, mit den Ereignissen, die von anderen Sicherheitsquellen erfasst wurden, die mit Ihrem Splunk verbunden sind. Klicken Sie beispielsweise in der Tabelle **Client-IP-Details** auf eine Zeile.



Client IP Details

Data Source	Risk Indicator Category	Risk Indicator Name	Client IP	Number of Unique Risk Indicators	Number of Risky Events
Citrix Access Control	Insider threats	Attempt to access blacklisted URL		2	4
Citrix Access Control	Insider threats	Risky website access		2	2

Im **Citrix Analytics Ereigniskorrelation-Dashboard** können Sie die Ereignisse anzeigen, die mit der ausgewählten Client-IP verknüpft sind und mit Ihren anderen Sicherheitsdatenquellen korreliert sind (basierend auf Index und Quelltyp). Diese Ereignisse bieten tiefere Einblicke in die böswilligen Aktivitäten, die mit der Client-IP verbunden sind.

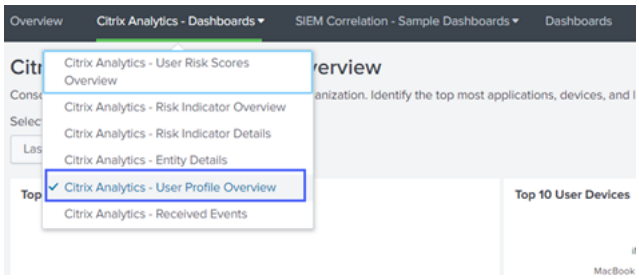


© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Benutzerprofil-Übersicht

Verwenden Sie das Dashboard, um die Ereignismetriken anzuzeigen, die mit den Benutzern in Ihrer Organisation verknüpft sind.

Um das Dashboard anzuzeigen, klicken Sie auf **Citrix Analytics- Dashboards > Citrix Analytics- Benutzerprofilübersicht**.



Ereignisse anzeigen

Wählen Sie einen Zeitraum aus und sehen Sie sich die folgenden Metriken an:

- Top 10 Anwendungen, die von den Benutzern verwendet werden
- Top 10 Geräte, die von den Benutzern verwendet werden
- Top 10 Standorte, die von den Benutzern genutzt werden
- Anzahl der verwendeten Web- und SaaS-Anwendungen
- Anzahl der verwendeten Geräte
- Anzahl der Benutzer, die standortübergreifend zugegriffen haben
- Datennutzungskennzahlen wie hochgeladene, heruntergeladene, freigegebene Dateien

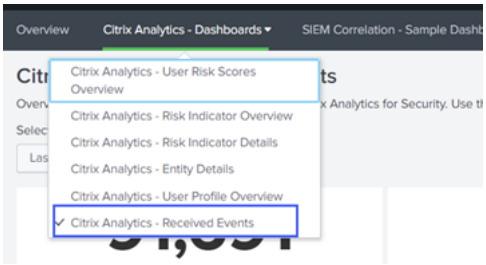
Diese Metriken geben Ihnen Einblicke in die Benutzeraktivitäten in Ihrem Unternehmen. Sie können die wichtigsten Anwendungen und Geräte, Nutzungsmuster, nicht konforme Geräte und Anwendungen, ungewöhnliche Standorte, riskanten Zugriff und ungewöhnliche Dateiaktivitäten identifizieren.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Erhaltene Ereignisse

Verwenden Sie das Dashboard, um die von Citrix Analytics for Security empfangenen Ereignisse anzuzeigen. Ein Ereignis weist auf eine Art von Benutzeraktivität hin.

Um das Dashboard anzuzeigen, klicken Sie auf **Citrix Analytics- Dashboards > Citrix Analytics-Empfangene Ereignisse**.



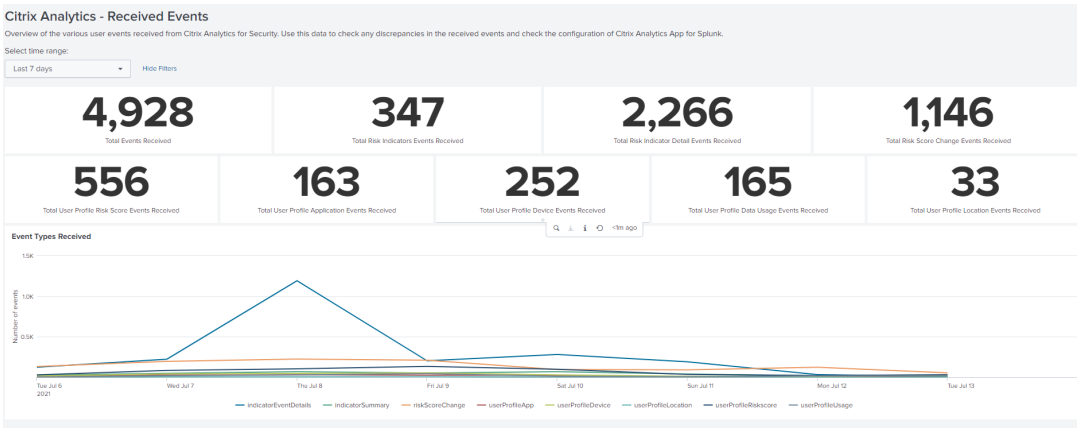
Sehen Sie sich die Berichte an

Wählen Sie einen Zeitraum aus, um die verschiedenen Arten von empfangenen Ereignissen anzuzeigen und zu vergleichen. Das Dashboard bietet die folgenden Informationen:

- Gesamtzahl der empfangenen Ereignisse: Dies ist die Summe aller von Citrix Analytics for Security empfangenen Ereignisse, einschließlich der folgenden:
  - Gesamtrisikoindikatorereignisse: Zeigt die Ereignisse an, die mit den von den Benutzern ausgelösten Risikoindikatoren verbunden sind.
  - Gesamtrisikoindikator-Detail-Ereignisse: Zeigt die Ereignisse an, die mit den Details der ausgelösten Risikoindikatoren verbunden sind.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Ereignisse zur Änderung der Risikobewertung insgesamt: Gibt die Ereignisse an, die mit der Änderung der Risikobewertung des Benutzers verbunden sind.
- Gesamtzahl der Ereignisse des Benutzerprofil-Risiko-Scores: Zeigt die Ereignisse an, die mit den Risikobewertungen der Benutzer
- Gesamtzahl der Anwendungsereignisse für Benutzerprofile: Zeigt die Ereignisse an, die mit den von den Benutzern verwendeten Anwendungen verknüpft sind.
- Gesamtzahl der Geräteereignisse des Benutzerprofils: Zeigt die Ereignisse an, die mit den von den Benutzern verwendeten Geräten verknüpft sind.
- Gesamtzahl der Benutzerprofildatennutzungsereignisse: Zeigt die Ereignisse an, die mit der Datennutzung der Benutzer verbunden sind.
- Gesamtzahl der Standortereignisse des Benutzerprofils: Zeigt die Ereignisse an, auf die die Benutzer zugreifen.

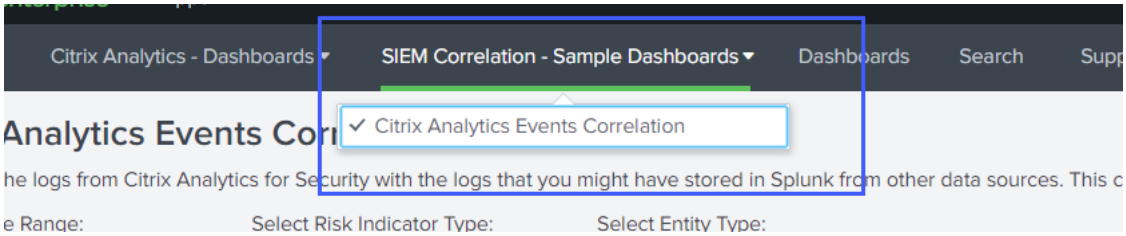


Beispiel für Ereigniskorrelation

Verwenden Sie das Dashboard, um von Citrix Analytics for Security empfangene Ereignisse mit den Ereignissen zu korrelieren, die von anderen in Ihrem Splunk konfigurierten Sicherheitsdatenquellen gesammelt wurden. Sie erhalten tiefere Einblicke in die riskanten Aktivitäten des Benutzers, die aus mehreren Datenquellen gesammelt wurden, finden Zusammenhänge zwischen den Ereignissen und identifizieren etwaige Bedrohungen.

Um das Dashboard anzuzeigen, klicken Sie auf **SIEM-Korrelation - Beispiel-Dashboards > Citrix Analytics Ereigniskorrelation**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Voraussetzungen

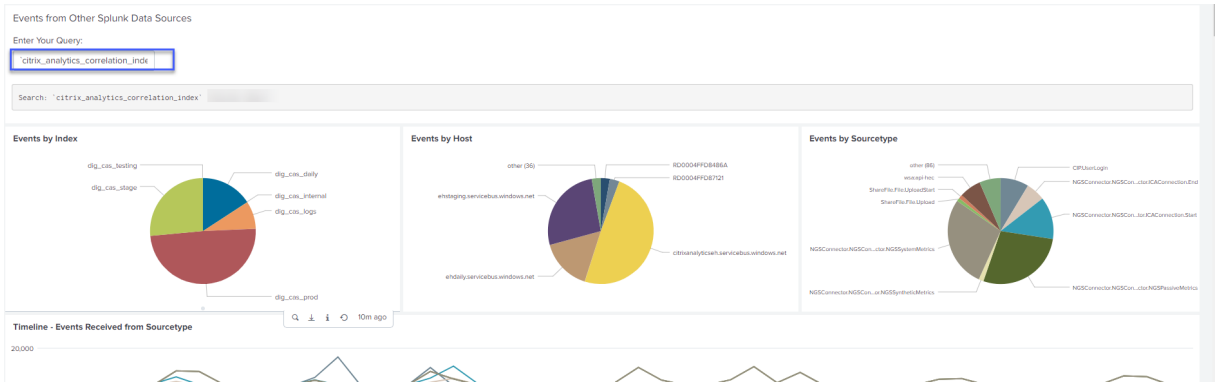
Stellen Sie Folgendes sicher, um eine Korrelation durchzuführen:

- Sie müssen Ereignisse aus Ihren anderen Sicherheitsdatenquellen haben, um korrelieren zu können. Beispielsweise Ereignisse, die mit Benutzern, Geräten und Client-IP-Adressen verknüpft sind, die von anderen in Ihrem Splunk konfigurierten Datenquellen empfangen wurden.
- Sie müssen bereits während der Konfiguration einen Korrelationsindex definiert haben.

Korrelieren Sie die Ereignisse

Sie können die riskanten Entitäten und die riskantesten IP-Adressen anzeigen, die von Citrix Analytics for Security erkannt wurden. Um diese Ereignisse mit anderen Datenquellen (definiert im Index und im Quelltyp) zu korrelieren, klicken Sie auf eine Entität oder eine IP-Adresse aus den Tabellen.

Der im Abfragefeld angezeigte Indexwert wird während der Konfiguration der App definiert. Sie können den Indexwert je nach Ihren Anforderungen in eine andere Sicherheitsdatenquelle ändern.



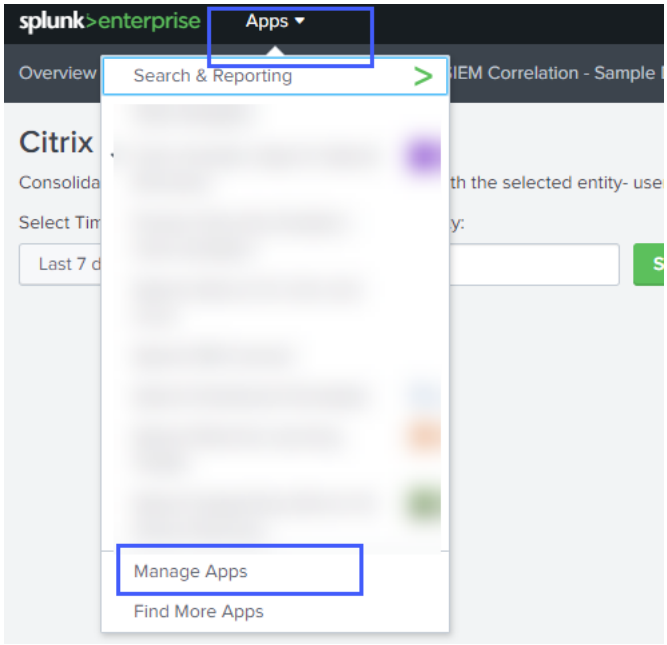
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Fehlerbehebung für keine Ereignisse

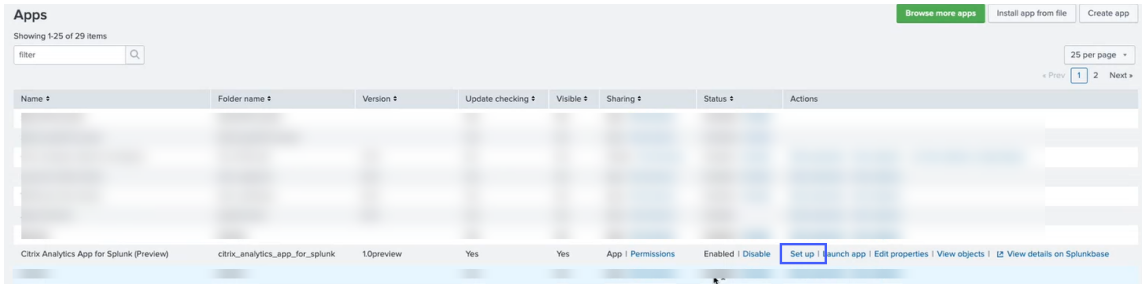
Wenn Sie in allen Dashboards keine Ereignisse finden, liegt dies möglicherweise an den Konfigurationsproblemen in der Citrix Analytics App für Splunk und dem Citrix Analytics-Add-On für Splunk. Überprüfen Sie in einem solchen Szenario den Indexwert und den Wert des Quelltyps. Stellen Sie sicher, dass die Werte des Index- und Quelltyps sowohl in der App als auch im Add-On identisch sind.

So zeigen Sie die Konfigurationseinstellungen der Citrix Analytics App für Splunk an:

1. Klicken Sie auf **Apps > Apps verwalten**.

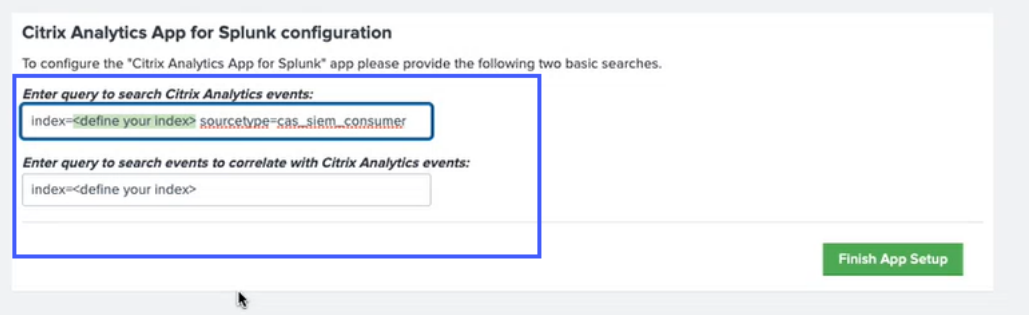


2. Suchen Sie Citrix Analytics App für Splunk aus der Liste. Klicken Sie auf **Einrichten**.



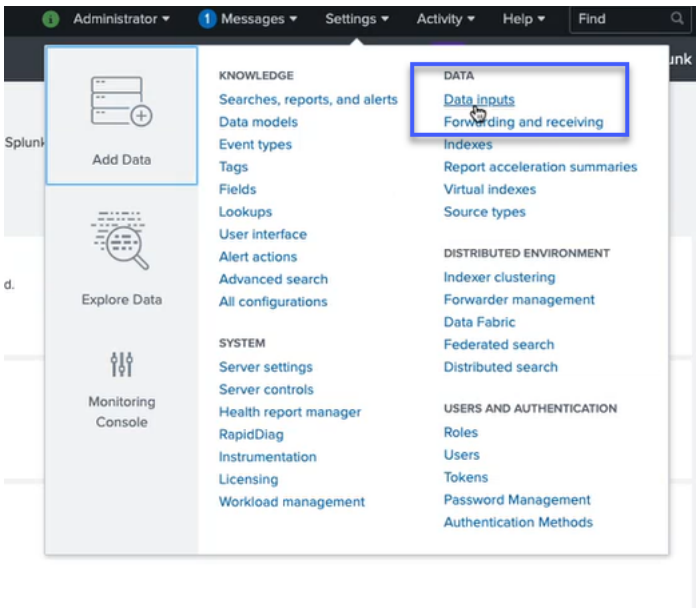
3. Prüfen Sie den Quelltyp und den Index.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



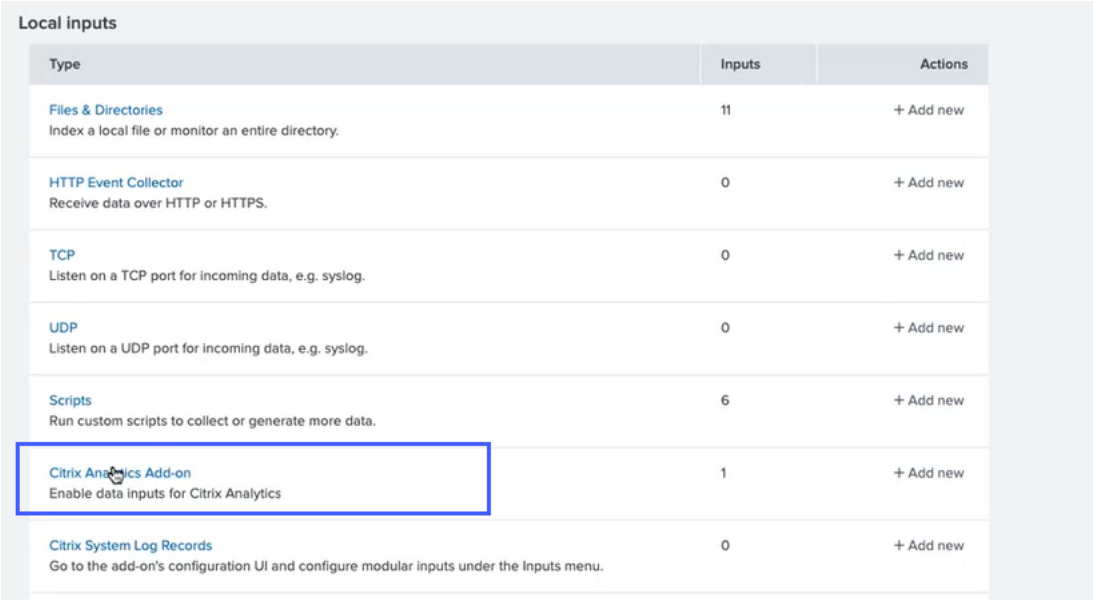
So zeigen Sie die Konfigurationseinstellungen des Citrix Analytics-Add-Ons für Splunk an:

1. Klicken Sie auf **Einstellungen > Dateneingaben**.

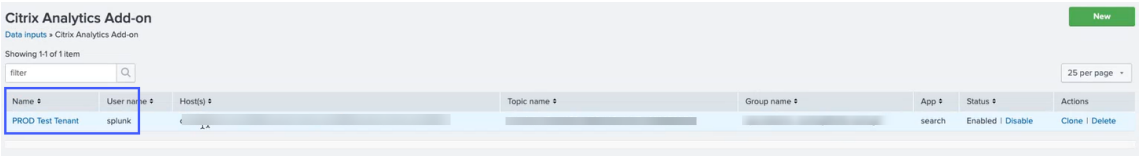


2. Klicken Sie auf **Citrix Analytics Add-on**.

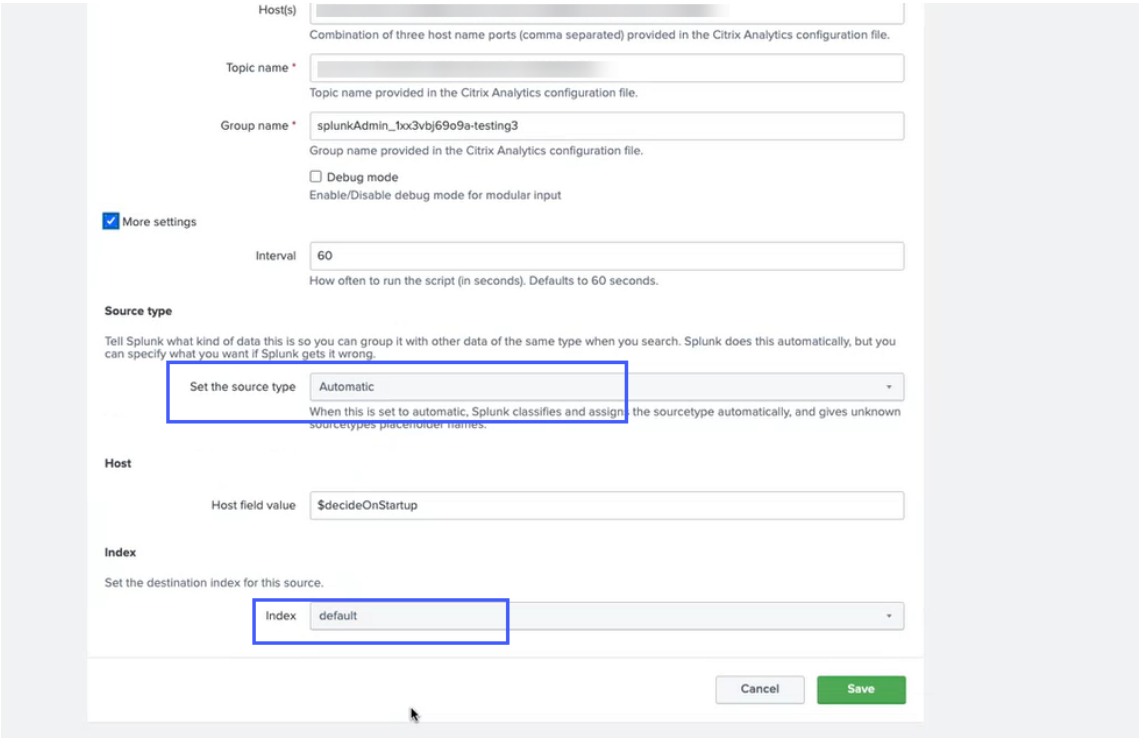
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



3. Klicken Sie auf den Mandanten, von dem Sie die Ereignisse erhalten.
4. Wähle **Weitere Einstellungen**aus.



5. Prüfen Sie den Quelltyp und den Index.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Weitere Informationen zur Konfiguration finden Sie unter Konfigurieren des Citrix Analytics-Add-ons für Splunk.

Konfigurationsprobleme mit dem Citrix Analytics-Add-On für Splunk

July 12, 2022

Citrix Analytics-Zusatzeinstellungen sind nicht verfügbar

Nachdem Sie das Citrix Analytics Add-on für Splunk in Ihrer Splunk Forwarder- oder Splunk Standalone-Umgebung installiert haben, werden die **Citrix Analytics-Add-on-Einstellungen** unter **Einstellungen > Dateneingaben**nicht angezeigt.

Grund

Dieses Problem tritt auf, wenn Sie das Citrix Analytics Add-on für Splunk in einer nicht unterstützten Splunk-Umgebung installieren.

Fixes

Installieren Sie das Citrix Analytics-Add-on für Splunk in einer unterstützten Splunk-Umgebung. Informationen zu den unterstützten Versionen finden Sie unter Splunk-Integration.

Keine Daten in Splunk-Dashboards verfügbar

Nach der Installation und Konfiguration des Citrix Analytics Add-ons für Splunk in Ihrer Splunk Forwarder- oder Splunk Standalone-Umgebung werden in Ihren Splunk-Dashboards keine Daten von Citrix Analytics angezeigt.

Schecks

Um das Problem zu beheben, überprüfen Sie Folgendes in Ihrer Splunk Forwarder- oder Splunk Standalone-Umgebung:

1. Stellen Sie sicher, dass die Voraussetzungen für die Splunk-Integration erfüllt sind.
2. Gehen Sie zu **Einstellungen > Dateneingaben > Citrix Analytics Add-on**. Stellen Sie sicher, dass die Citrix Analytics-Konfigurationsdetails verfügbar sind.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

3. Wenn die Konfigurationsdetails verfügbar sind, führen Sie die folgende Abfrage aus, um die Protokolle auf Fehler im Zusammenhang mit dem Citrix Analytics-Add-on für Splunk zu überprüfen:

```
index=_internal sourcetype=splunkd log_level=ERROR component=
    ExecProcessor cas_siem_consumer
```

4. Wenn Sie keine Fehler finden, funktioniert das Citrix Analytics-Add-On für Splunk wie erwartet. Wenn Sie Fehler in den Protokollen finden, kann dies an einem der folgenden Gründe liegen:

   - Es konnte keine Verbindung zwischen Ihrer Splunk-Umgebung und Citrix Analytics Kafka-Endpunkten hergestellt werden. Dieses Problem könnte auf die Firewall-Einstellungen zurückzuführen sein.

     Korrekturen: Wenden Sie sich an Ihren Netzwerkadministrator, um dieses Problem zu beheben.

   - Falsche Konfigurationsdetails unter **Einstellungen > Dateneingaben > Citrix Analytics Add-on**.

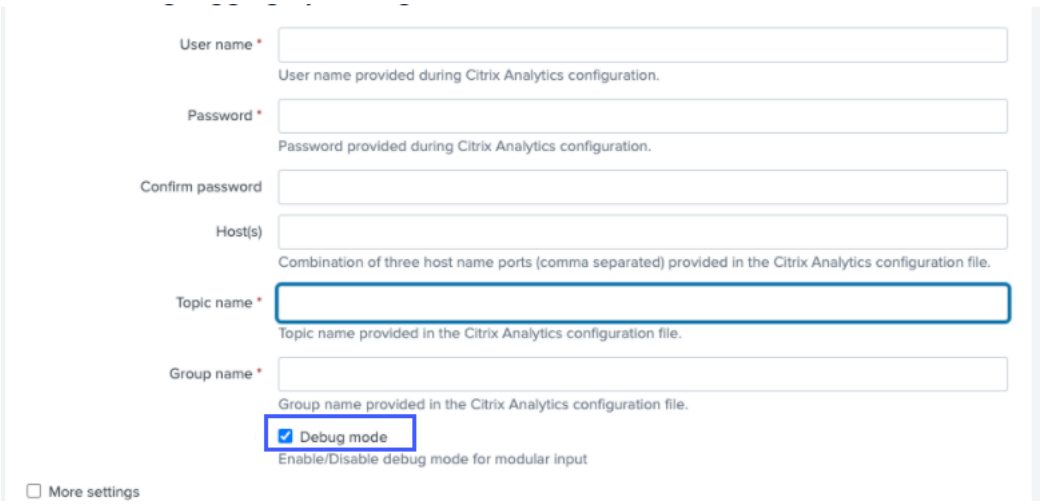
     Korrekturen: Stellen Sie sicher, dass die Citrix Analytics-Konfigurationsdetails wie Benutzername, Kennwort, Host-Endpunkte, Thema und Benutzergruppe gemäß der Citrix Analytics-Konfigurationsdatei korrekt eingegeben werden. Weitere Informationen finden Sie unter Konfigurieren des Citrix Analytics-Add-ons für Splunk.

5. Wenn Sie die Ursache des Problems in den vorhergehenden Protokollen nicht finden können und weitere Untersuchungen durchführen möchten:

   a) Aktivieren Sie den **Debug-Modusunter Einstellungen > Dateneingaben > Citrix Analytics Add-on**.

   > Hinweis
   >
   > Standardmäßig ist der **Debug-Modus** deaktiviert. Durch die Aktivierung dieses Modus werden zu viele Protokolle generiert. Verwenden Sie diese Option also nur bei Bedarf und deaktivieren Sie sie, nachdem Sie Ihre Debugging-Aufgabe abgeschlossen haben.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



b) Suchen Sie die generierten Debug-Protokolle an folgendem Ort und überprüfen Sie, ob Fehler auftreten:

```
$SPLUNK_HOME$/var/log/splunk.Filename
    splunk_citrix_analytics_add_on_debug_connection.log
```

c) (Optional) Verwenden Sie das Debug-Skript `splunk cmd python cas_siem_consumer_debug.py`, das mit dem Citrix Analytics-Add-on für Splunk verfügbar ist. Dieses Skript generiert eine Protokolldatei, die die Details Ihrer Splunk-Umgebung und die Konnektivitätsprüfungen enthält. Sie können die Details verwenden, um das Problem zu debuggen. Führen Sie das Script mit dem folgenden Befehl aus:

```
cd $SPLUNK_HOME$/etc/apps/TA_CTXS_AS/bin/; /opt/splunk/bin/
    splunk cmd python cas_siem_consumer_debug.py
```

Fehlermeldung

In den Protokollen im Zusammenhang mit dem Citrix Analytics-Add-on für Splunk wird möglicherweise der folgende Fehler angezeigt:

```
ERRORKafkaError{ code=_TRANSPORT,val=-195,str="Failed to get metadata
: Local: Broker transport failure"}
```

Dieser Fehler ist entweder auf ein Problem mit der Netzwerkkonnektivität oder auf ein Authentifizierungsproblem zurückzuführen.

Um das Problem zu debuggen:

1. Aktivieren Sie in Ihrer Splunk Forwarder- oder Splunk Standalone-Umgebung den **Debug-Modus**, um die Debug-Protokolle abzurufen. Beziehen Sie sich auf den vorherigen Schritt 5.a.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

2. Führen Sie die folgende Abfrage aus, um Authentifizierungsprobleme in den Debug-Protokollen zu finden:

```
index=_internal source="*
    splunk_citrix_analytics_add_on_debug_connection.log*" "
    Authentication failure"
```

3. Wenn Sie in den Debug-Protokollen keine Authentifizierungsprobleme finden, ist der Fehler auf ein Problem mit der Netzwerkkonnektivität zurückzuführen.
4. Suchen und beheben Sie das Problem, indem Sie Telnet oder das im vorherigen Schritt 5.c erwähnte Debug-Skript verwenden.

Das Add-on-Upgrade schlägt von einer Version vor 2.0.0 fehl

Wenn Sie in Ihrer Splunk Forwarder- oder Splunk Standalone-Umgebung das Citrix Analytics-Add-On für Splunk von einer Version vor 2.0.0 auf die neueste Version aktualisieren, schlägt das Upgrade fehl.

Fixes

1. Löschen Sie die folgenden Dateien und Ordner im Ordner /`bin` des Citrix Analytics-Add-ons für Splunk-Installationsordner:
    - `cd $SPLUNK_HOME$/etc/apps/TA_CTXS_AS/bin`
    - `rm -rf splunklib`
    - `rm -rf mac`
    - `rm -rf linux_x64`
    - `rm CARoot.pem`
    - `rm certificate.pem`
2. Starten Sie Ihre Splunk Forwarder- oder Splunk Standalone-Umgebung neu.

Microsoft Sentinel-Integration

November 16, 2023

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Hinweise

- Wenden Sie sich an CAS-PM-Ext@cloud.com, um Unterstützung für die Microsoft Sentinel-Integration, den Export von Daten nach Microsoft Sentinel anzufordern oder Feedback zu geben.
- Der Datenexport nach Microsoft Sentinel mithilfe der Logstash-Engine befindet sich in der Vorschau. Diese Funktion wird ohne Service Level Agreement bereitgestellt und wird nicht für Produktionsarbeitslasten empfohlen. Weitere Informationen finden Sie in der Microsoft Sentinel-Dokumentation .

Integrieren Sie Citrix Analytics for Security mithilfe der Logstash-Engine in Ihren Microsoft Sentinel.

Diese Integration ermöglicht es Ihnen, die Benutzerdaten aus Ihrer Citrix IT-Umgebung zu Microsoft Sentinel zu exportieren und zu korrelieren und so tiefere Einblicke in die Sicherheitslage Ihres Unternehmens zu erhalten. Zeigen Sie in Ihrer Splunk-Umgebung die aufschlussreichen Dashboards an, die nur für Citrix Analytics for Security gelten. Sie können auch benutzerdefinierte Ansichten basierend auf Ihren Sicherheitsanforderungen erstellen.

Weitere Informationen zu den Vorteilen der Integration und der Art der verarbeiteten Daten, die an Ihr SIEM gesendet werden, finden Sie unter Integration von Sicherheitsinformationen und Ereignismanagement.

Voraussetzungen

- Aktivieren Sie die Datenverarbeitung für mindestens eine Datenquelle. Es hilft Citrix Analytics for Security, den Microsoft Sentinel-Integrationsprozess zu beginnen.
- Stellen Sie sicher, dass der folgende Endpunkt in der Zulassen Liste in Ihrem Netzwerk enthalten ist.

Endpunkt	Region der Vereinigten Staaten	Region der Europäischen Union	Asien-Pazifik Süd

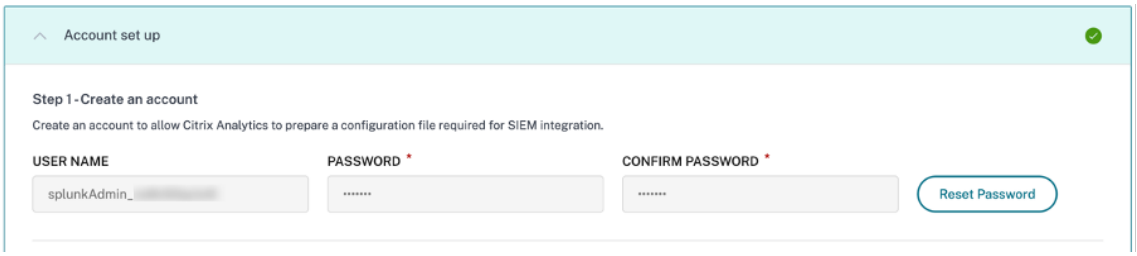
Kafka Broker	`casnb-0.citrix.com:9094`
	`casnb-1.citrix.com:9094`
	`casnb-2.citrix.com:9094`
	`casnb-3.citrix.com:9094`
		`casnb-eu-0.citrix.com:9094`
		`casnb-eu-1.citrix.com:9094`
		`casnb-eu-2.citrix.com:9094`
			`casnb-aps-0.citrix.com:9094`
			`casnb-aps-1.citrix.com:9094`
			`casnb-aps-2.citrix.com:9094`

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

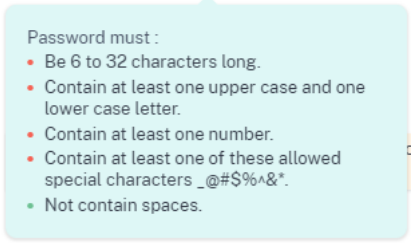
- Stellen Sie sicher, dass Sie die Logstash-Versionen 7.17.7 oder höher (getestete Versionen auf Kompatibilität mit Citrix Analytics for Security: v7.17.7 und v8.5.3) mit dem Microsoft Sentinel-Ausgabe-Plug-In für Logstash verwenden.

Integrieren Sie mit Microsoft Sentinel

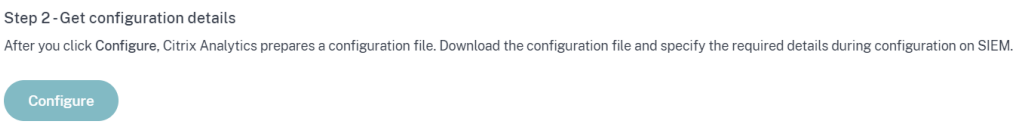
1. Gehen Sie zu **Einstellungen > Datenexporte**.
2. Erstellen Sie im Abschnitt **Kontoeinrichtung** ein Konto, indem Sie den Benutzernamen und ein Kennwort angeben. Dieses Konto wird verwendet, um eine Konfigurationsdatei vorzubereiten, die für die Integration erforderlich ist.



3. Stellen Sie sicher, dass das Kennwort die folgenden Bedingungen erfüllt:



4. Klicken Sie auf **Konfigurieren**, um die Logstash-Konfigurationsdatei zu erstellen



5. Wählen Sie die Registerkarte Azure Sentinel (Vorschau), um die Konfigurationsdateien herunterzuladen:

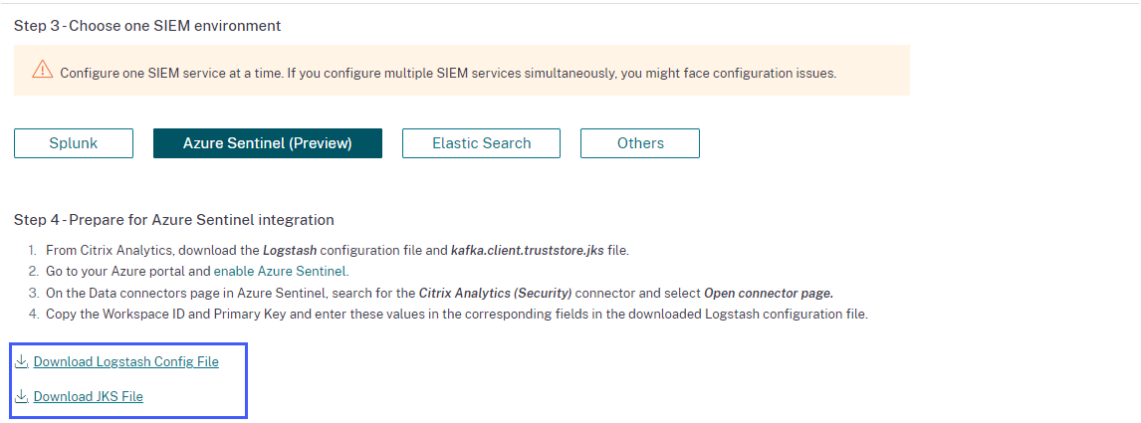
   - **Logstash-Konfigurationsdatei**: Enthält die Konfigurationsdaten (Eingabe-, Filter- und Ausgabeabschnitte) zum Senden von Ereignissen von Citrix Analytics for Security an Microsoft Sentinel mithilfe des Logstash-Datenerfassungsmoduls.

     Informationen zur Struktur der Logstash-Konfigurationsdatei finden Sie in der Logstash-Dokumentation .

   - **JKS-Datei**: Enthält die für die SSL-Verbindung erforderlichen Zertifikate.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Hinweis**
>
> Diese Dateien enthalten sensible Informationen. Bewahren Sie sie an einem sicheren Ort auf.



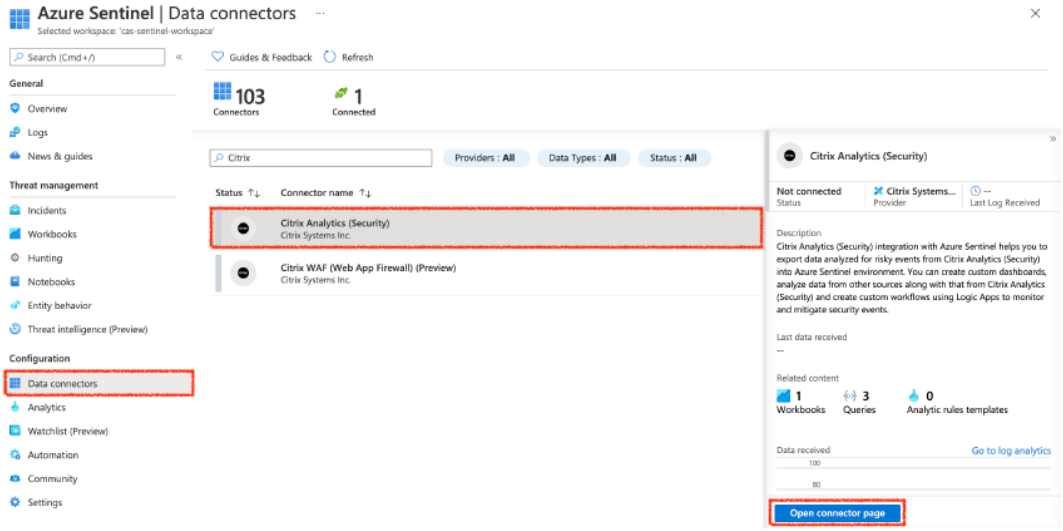
6. Bereiten Sie Ihre Azure Sentinel-Integration vor:

   a) Aktivieren Sie auf Ihrem Azure-Portal Microsoft Sentinel. Sie können einen Workspace erstellen oder Ihren vorhandenen Workspace verwenden, um Microsoft Sentinel auszuführen.

   b) Wählen Sie im Hauptmenü DatenConnectoren aus, um die **DatenConnectoren-Galerie** zu öffnen.

   c) Suchen Sie nach **Citrix Analytics (Sicherheit)**.

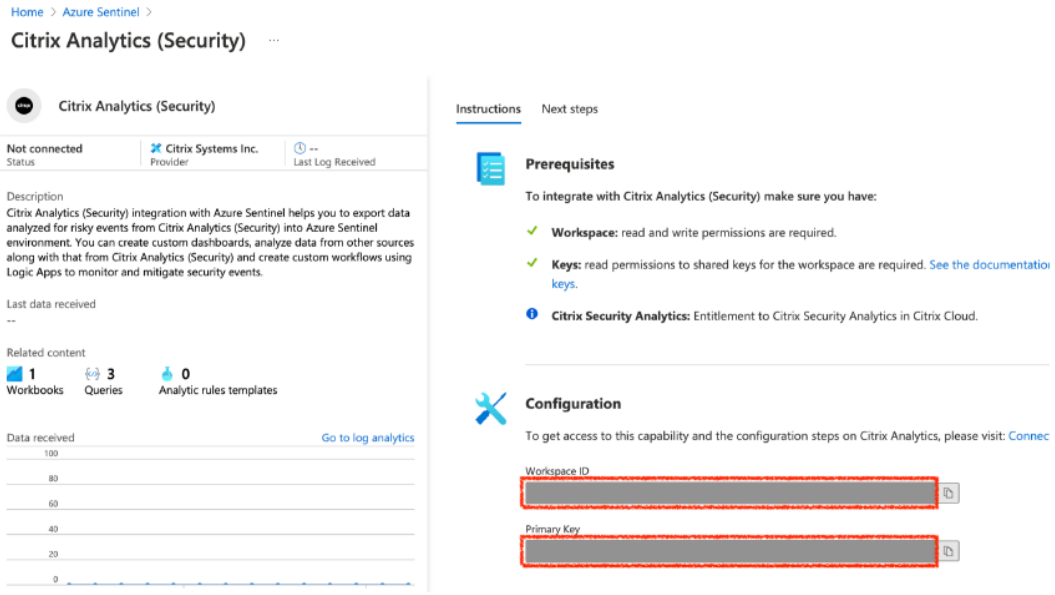
   d) Wählen Sie **Citrix Analytics (Sicherheit)** und wählen Sie **Connector-Seite öffnen**.



   e) Kopieren Sie auf der Seite **Citrix Analytics (Sicherheit)** die **Workspace-ID** und den

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Primärschlüssel. Sie müssen diese Informationen in den nachfolgenden Schritten in die Logstash-Konfigurationsdatei eingeben.



f) Konfiguriere Logstash auf deinem Host-Computer:

i. Installieren Sie auf Ihrem Linux- oder Windows-Host-Computer Logstash und das Microsoft Sentinel-Ausgabe-Plug-in für Logstash.

ii. Platzieren Sie auf dem Host-Computer, auf dem Sie Logstash installiert haben, die folgenden Dateien in das angegebene Verzeichnis:

Host-Maschinentyp	Dateiname	Pfad für das Verzeichnis
Linux	CAS_AzureSentinel_LogStash_Config.conf	Für Debian- und RPM-Pakete: `/etc/logstash/conf.d/` Für .zip- und .tar.gz-Archive: `{ extract.path } / config`
	kafka.client.truststore.jks	Für Debian- und RPM-Pakete: `/etc/logstash/ssl/` Für .zip- und .tar.gz-Archive: `{ extract.path } /ssl`
Windows	CAS_AzureSentinel_LogStash_Config.conf	`C:\Logstash-7.xx.x\config`
	kafka.client.truststore.jks	

Informationen zur Standardverzeichnisstruktur der Logstash-Installationspakete

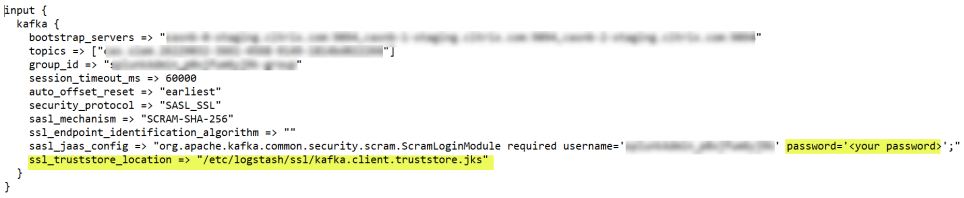
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

finden Sie in der Logstash-Dokumentation.

iii. Öffnen Sie die Logstash-Konfigurationsdatei und gehen Sie wie folgt vor:

A. Geben Sie im Eingabebereich der Datei Folgendes ein:

- **Kennwort**: Das Kennwort des Kontos, das Sie in Citrix Analytics for Security zur Vorbereitung der Konfigurationsdatei erstellt haben.
- **SSL-Truststore-Standort**: Der Speicherort Ihres SSL-Clientzertifikats. Dies ist der Speicherort der Datei kafka.client.truststore.jks auf Ihrem Host-Computer.



B. Geben Sie im Ausgabeabschnitt der Datei die **Workspace-ID** und den **Primärschlüssel** (den Sie von Microsoft Sentinel kopiert haben) im Ausgabeabschnitt der Datei ein.

```
output {
  if [event_type] == "indicatorSummary" {
    microsoft-logstash-output-azure-loganalytics {
          workspace_id => "<your Azure Log analytics Workspace ID>"
          workspace_key => "<your Shared Key>"
          custom_log_table_name => "CitrixAnalytics_indicatorSummary"
          time_generated_field => "timestamp"
    }
  } else if [event_type] == "indicatorEventDetails" {
    microsoft-logstash-output-azure-loganalytics {
          workspace_id => "<your Azure Log analytics Workspace ID>"
          workspace_key => "<your Shared Key>"
          custom_log_table_name => "CitrixAnalytics_indicatorEventDetails"
          time_generated_field => "timestamp"
    }
  }else if [event_type] == "riskScoreChange" {
    microsoft-logstash-output-azure-loganalytics {
          workspace_id => "<your Azure Log analytics Workspace ID>"
          workspace_key => "<your Shared Key>"
          custom_log_table_name => "CitrixAnalytics_riskScoreChange"
          time_generated_field => "timestamp"
    }
  } else if [event_type] =~ "userProfile.+" {
    microsoft-logstash-output-azure-loganalytics {
          workspace_id => "<your Azure Log analytics Workspace ID>"
          workspace_key => "<your Shared Key>"
          custom_log_table_name => "CitrixAnalytics_userProfile"
          time_generated_field => "timestamp"
    }
  } else {
    microsoft-logstash-output-azure-loganalytics {
          workspace_id => "<your Azure Log analytics Workspace ID>"
          workspace_key => "<your Shared Key>"
          custom_log_table_name => "CitrixAnalytics_misc"
          time_generated_field => "timestamp"
```

iv. Starten Sie den Logstash-Hostcomputer neu, um die verarbeiteten Daten von Citrix Analytics for Security an Microsoft Sentinel zu senden.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

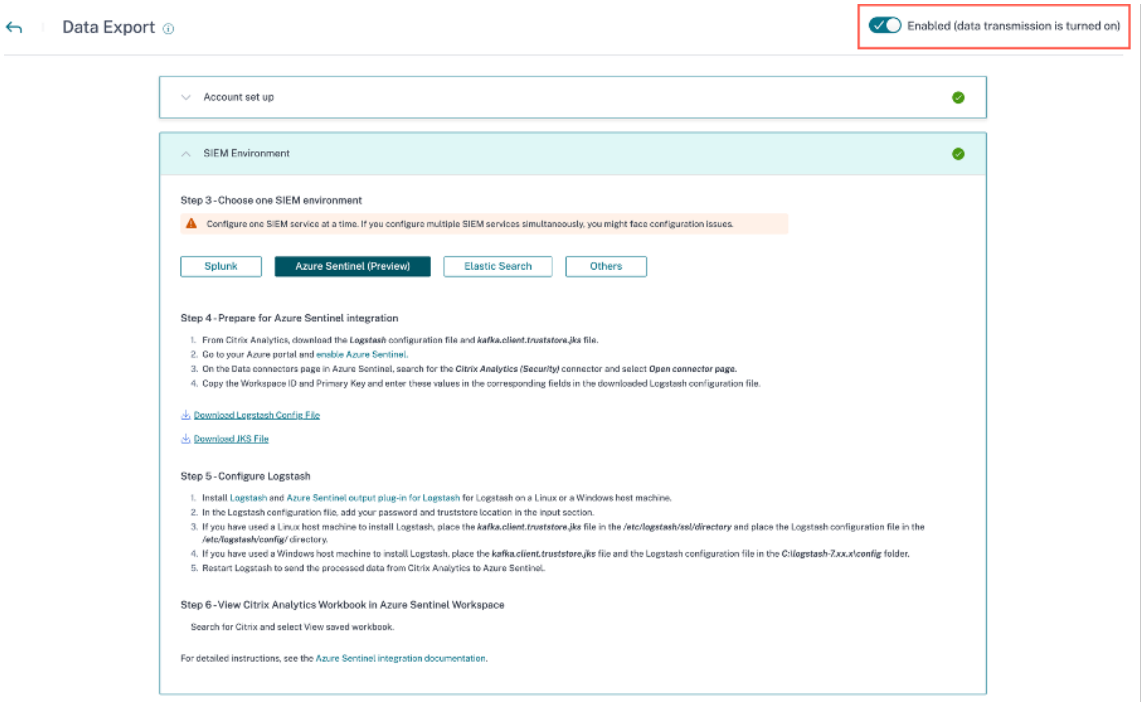
g) Gehen Sie zu Ihrem Microsoft Sentinel Workspace und zeigen Sie die Daten in der Citrix Analytics-Arbeitsmappean.

Aktivieren oder Deaktivieren der Datenübertragung

Nachdem Citrix Analytics for Security die Konfigurationsdatei vorbereitet hat, ist die Datenübertragung für Microsoft Sentinel aktiviert.

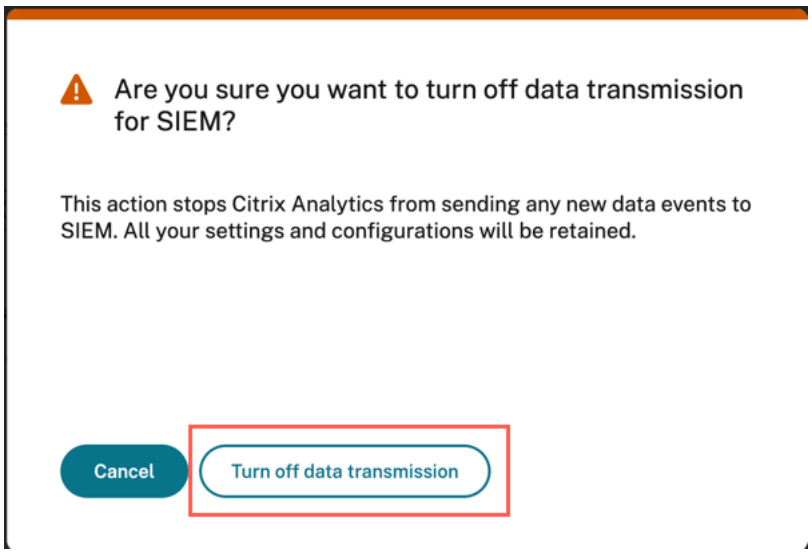
So beenden Sie die Übertragung von Daten aus Citrix Analytics for Security:

1. Gehen Sie zu **Einstellungen > Datenexporte**.
2. Schalten Sie die Umschalttaste aus, um die **Datenübertragung** zu deaktivieren. Standardmäßig ist die Datenübertragung immer aktiviert..



Zur Bestätigung wird ein Warnfenster angezeigt. Klicken Sie auf die Schaltfläche **Datenübertragung ausschalten**, um die Übertragungsaktivität zu beenden.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Um die Datenübertragung wieder zu aktivieren, schalten Sie die Umschalttaste ein.

Weitere Informationen zur Microsoft Sentinel-Integration finden Sie unter den folgenden Links:

- Integration von Citrix Analytics mit Microsoft Sentinel
- Verbessern Sie Ihre Bedrohungssuche mit Citrix Analytics for Security und Microsoft Sentinel

Citrix Analytics-Arbeitsmappe für Microsoft Sentinel

December 12, 2023

> **Hinweis**
>
> Dieses Feature ist als Preview verfügbar.

In diesem Artikel wird die Citrix Analytics-Arbeitsmappe beschrieben, die in Ihrem Microsoft Sentinel-Arbeitsbereich verfügbar ist.

Voraussetzung

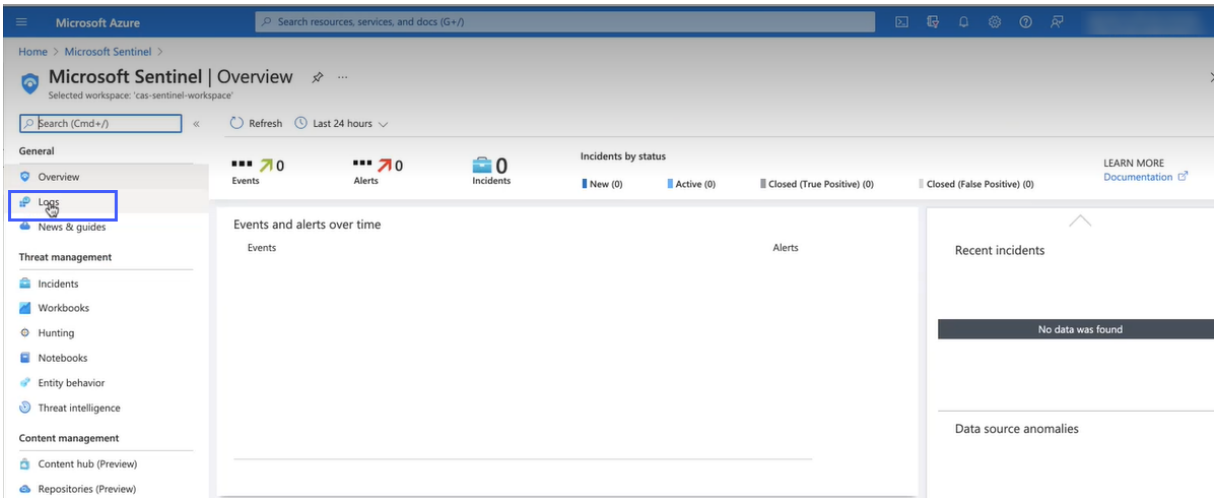
Um die Citrix Analytics-Arbeitsmappe zu verwenden, stellen Sie sicher, dass Sie Microsoft Sentinel bereits in Citrix Analytics for Security integriert haben. Weitere Informationen finden Sie unter Microsoft Sentinel-Integration.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Anzeigen der Citrix Analytics-Ereignisse

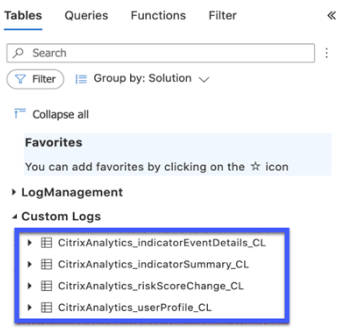
Nach der Integration von Citrix Analytics for Security mit Microsoft Sentinel beginnt der Logstash-Connector, Ereignisse von Citrix Analytics for Security in den Microsoft Sentinel-Arbeitsbereich zu übertragen. Öffnen Sie in Ihrem **Azure-Portal**den Microsoft Sentinel-Arbeitsbereich, den Sie für die Integration verwendet haben.

Um zu überprüfen, ob Microsoft Sentinel die Ereignisse von Citrix Analytics for Security empfängt, wählen Sie **Protokolle > Benutzerdefinierte Protokolle**aus.



Im Abschnitt **Benutzerdefinierte Protokolle** können Sie die Protokolltabellen anzeigen, die automatisch erstellt werden, um die von Citrix Analytics for Security empfangenen Ereignisse zu speichern. Diese Protokolltabellen dienen als Quelle für die Dashboards in der Citrix Analytics-Arbeitsmappe.

> **Hinweis**
>
> Es kann einige Stunden dauern, bis die von Citrix Analytics for Security gesendeten Ereignisse im Microsoft Sentinel-Arbeitsbereich angezeigt werden. Daher kann es zu einer Verzögerung bei der Erstellung der Protokolltabellen für die Ereignisse kommen.

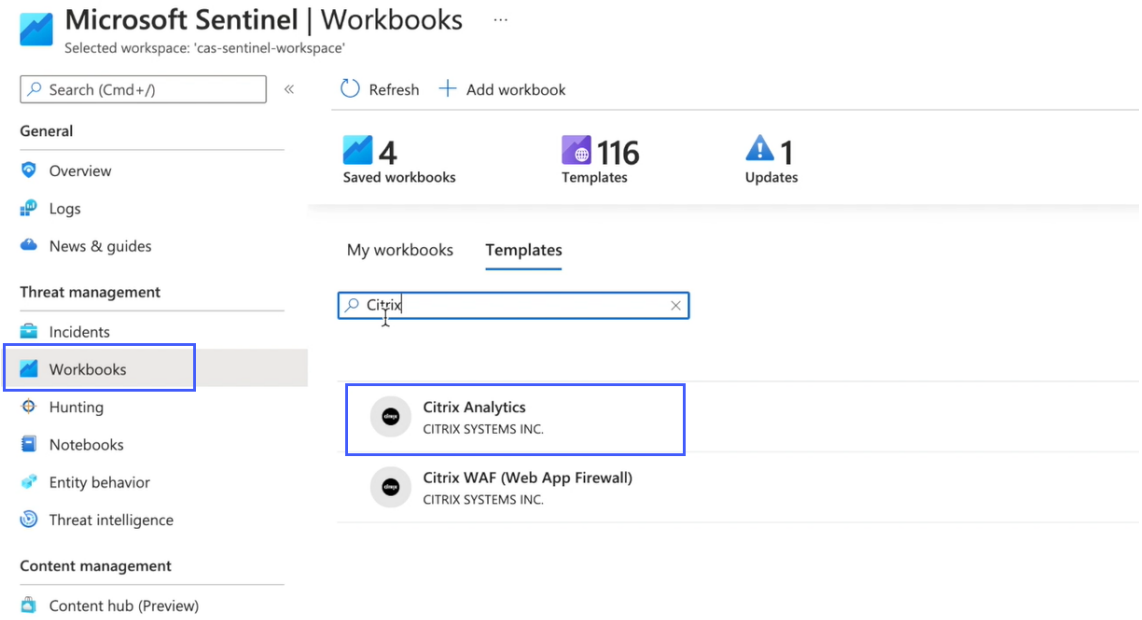


© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Anzeigen der Citrix Analytics-Arbeitsmappe

Wenn die Protokolltabellen erfolgreich erstellt wurden, gehen Sie wie folgt vor:

1. Wählen Sie **Arbeitsmappen** und suchen Sie nach **Citrix Analytics**. Wählen Sie **Citrix Analytics**aus.



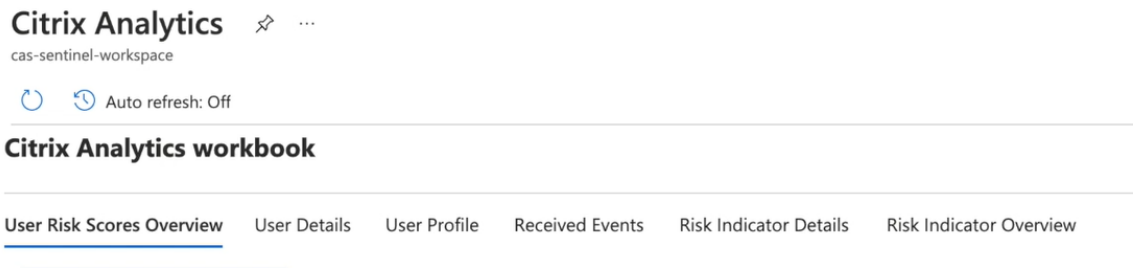
2. Wählen Sie **Vorlage anzeigen** aus, um die Citrix Analytics Arbeitsmappe zu öffnen.

In der Citrix Analytics-Arbeitsmappe können Sie die Benutzerereignisse in den folgenden Dashboards anzeigen:

- **Übersicht über die Risikobewertung der Benutzer**: Bietet eine konsolidierte Ansicht der riskanten Benutzer in Ihrer Organisation.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

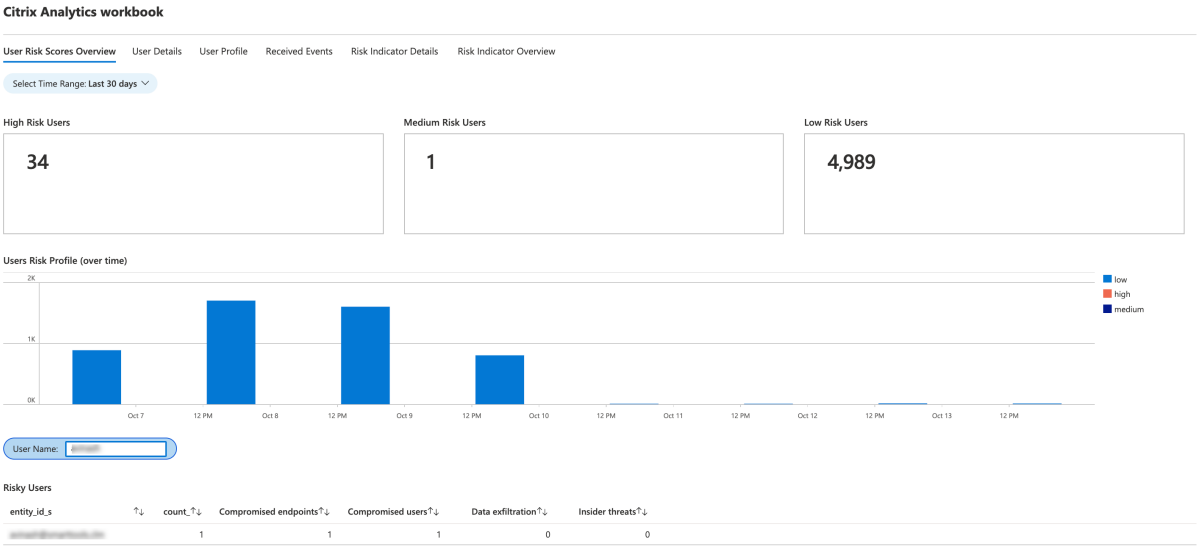
- **Benutzerdetails**: Stellt Details zu den Benutzern und ihrem riskanten Verhalten bereit.
- **Benutzerprofil**: Stellt die mit den Benutzern verknüpften Ereignismetriken bereit.
- **Empfangene Ereignisse**: Stellt die von Citrix Analytics for Security empfangenen Ereignisse bereit.
- **Details zum Risikoindikator**: Enthält Details zu den integrierten und benutzerdefinierten Risikoindikatoren, die von den Benutzern ausgelöst werden.
- **Überblick über die Risikoindikatoren**: Bietet einen konsolidierten Überblick über die von den Benutzern ausgelösten Risikoindikatoren.



Überblick über den Risiko-Score

Dieses Dashboard bietet eine konsolidierte Ansicht der riskanten Benutzer in Ihrem Unternehmen. Die Benutzer werden nach den Risikoniveaus kategorisiert - hoch, mittel und niedrig. Die Risikostufen basieren auf den Anomalien in den Benutzeraktivitäten und dementsprechend wird ein Risiko-Score zugewiesen. Weitere Informationen zu den Arten riskanter Benutzer finden Sie im Benutzer-Dashboard.

Wählen Sie einen Zeitraum aus, um die riskanten Benutzer in Ihrer Organisation anzuzeigen.

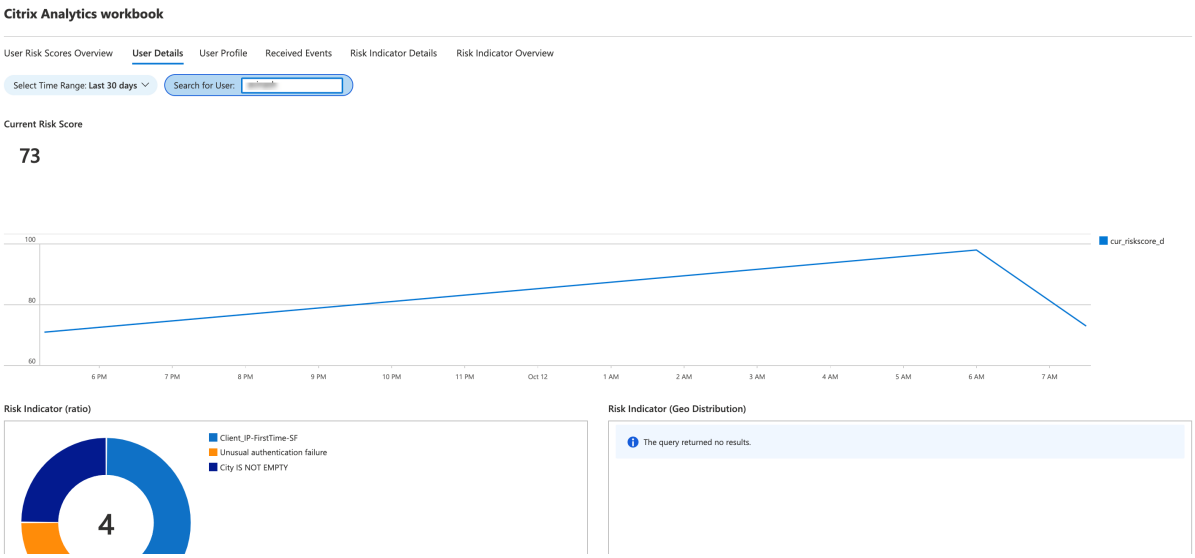


© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Angaben zum Benutzer

Dieses Dashboard enthält die Risikobewertung und die mit einem Benutzer verbundenen Risikoindikatoren.

Suchen Sie einen Benutzer und sehen Sie sich seine riskanten Aktivitäten an, die eine Bedrohung für Ihr Unternehmen darstellen können. Um die Bedrohung zu mindern, können Sie je nach Risikoschweregrad geeignete Maßnahmen für die Benutzerkonten ergreifen.



Benutzerprofil

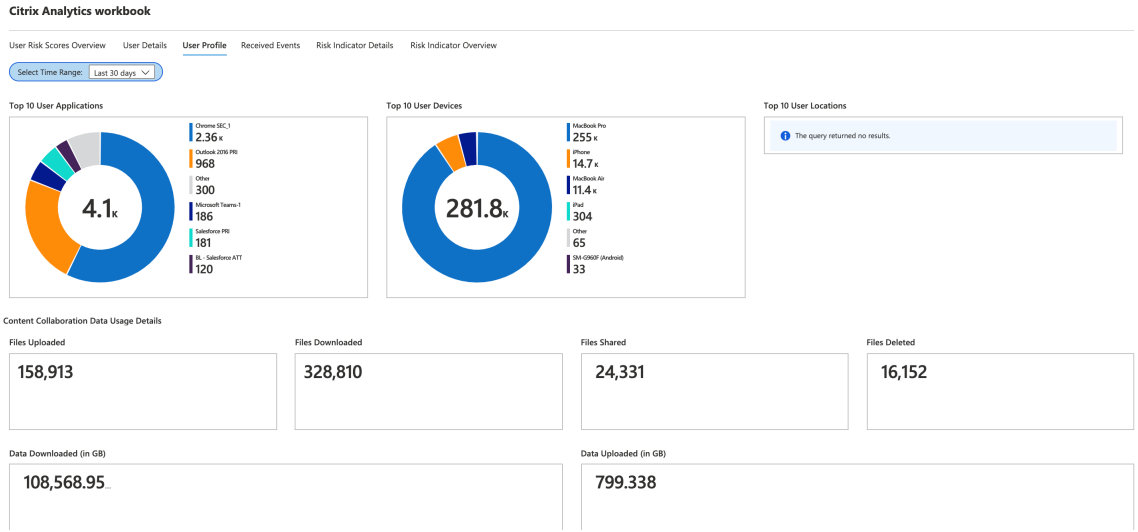
Dieses Dashboard enthält die Details der Ereignismetriken, die Ihren Benutzern für einen ausgewählten Zeitraum zugeordnet sind. Die Metriken bieten Einblicke in die Benutzeraktivitäten wie:

- Top 10 Anwendungen, die von den Benutzern verwendet werden
- Top 10 Geräte, die von den Benutzern verwendet werden
- Top 10 Standorte, an denen sich die Benutzer angemeldet haben

Mithilfe der Berichte können Sie:

- Identifizieren Sie den Nutzungstrend Ihrer Benutzer
- Entdecken Sie die nicht konformen Geräte, die für den Zugriff auf die Ressourcen verwendet werden
- Suchen Sie nach potenziell riskanten Zugriffen Ihrer Benutzer

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Erhaltene Ereignisse

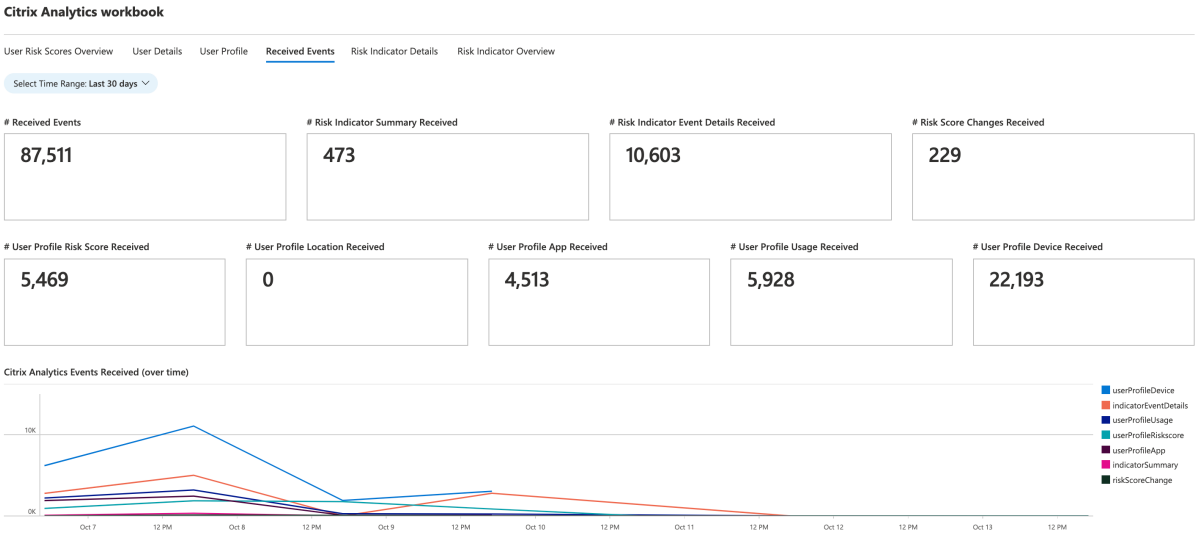
Für einen ausgewählten Zeitraum können Sie die Gesamtzahl der Ereignisse anzeigen, die von Citrix Analytics for Security empfangen wurden. Die Gesamtzahl der empfangenen Ereignisse umfasst Folgendes:

- Zusammenfassung der Risikoindikatoren: Zeigt die Ereignisse an, die mit der Zusammenfassung der Benutzerrisikoindikatoren verknüpft sind. Informationen zu verschiedenen zusammenfassenden Ereignissen der Risikoindikatoren finden Sie unter Risikoindikatorschema.
- Ereignisdetails zum Risikoindikator: Zeigt die Ereignisse an, die mit den Details der Benutzerrisikoindikatoren verknüpft sind Informationen zu verschiedenen Detailereignissen der Risikoindikatoren finden Sie unter Risikoindikatorschema.
- Risikobewertung des Benutzerprofils: Zeigt die Ereignisse an, die mit der Risikobewertung der Benutzer verknüpft sind. Weitere Informationen finden Sie unter Benutzer-Dashboard.
- Änderungen der Risikobewertung: Zeigt die Ereignisse an, die mit der Änderung der Risikobewertung der Benutzer verbunden sind. Weitere Informationen finden Sie unter Benutzer-Dashboard.
- Standorte des Benutzerprofils: Zeigt die Ereignisse an, die mit den Orten verknüpft sind, von denen aus sich die Benutzer angemeldet haben.
- Benutzerprofil-App: Zeigt die Ereignisse an, die mit den von den Benutzern verwendeten Anwendungen verknüpft sind.
- Verwendung des Benutzerprofils: Zeigt die Ereignisse an, die mit der Datennutzung der Benutzer verknüpft sind.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Benutzerprofil Gerät: Zeigt die Ereignisse an, die mit den von den Benutzern verwendeten Geräten verknüpft sind.

Indem Sie das Dashboard in regelmäßigen Abständen überprüfen, können Sie sicherstellen, dass die Ereignisse ordnungsgemäß in Ihren Microsoft Sentinel-Arbeitsbereich fließen. Jede Abweichung bei den insgesamt empfangenen Ereignissen kann auf Integrationsprobleme mit Citrix Analytics for Security hinweisen. Sie können die erforderlichen Schritte ausführen, um die Probleme zu debuggen.



Angaben zu Risikoindikatoren

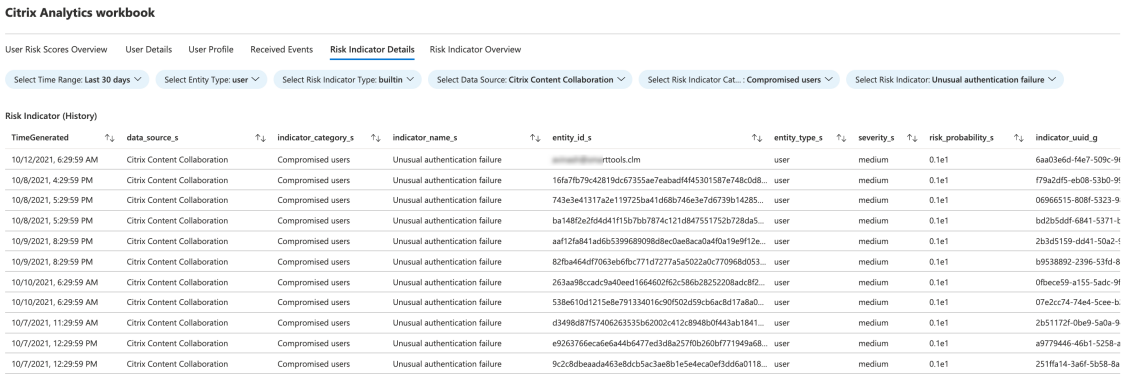
Dieses Dashboard enthält die Details der von Ihren Benutzern ausgelösten Risikoindikatoren.

Sie können die Risikoindikator-Details anzeigen, indem Sie eine oder mehrere Kategorien auswählen:

- Zeitraum: Wählen Sie einen Zeitraum aus, um die Details der während des Zeitraums ausgelösten Risikoindikatoren anzuzeigen.
- Entitätstyp: Wählen Sie einen Benutzer aus, um die Details der zugehörigen Risikoindikatoren anzuzeigen.
- Risikoindikatortyp: Wählen Sie entweder integrierte oder benutzerdefinierte Risikoindikatoren aus, um deren Details anzuzeigen.
- Datenquelle: Wählen Sie eine Datenquelle aus, um die zugehörigen Risikoindikatoren anzuzeigen.
- Kategorie Risikoindikatoren: Wählen Sie die Risikokategorie aus, um die zugehörigen Risikoindikatoren anzuzeigen.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Risikoindikator: Wählen Sie einen Risikoindikator nach Namen aus und zeigen Sie dessen Details an.



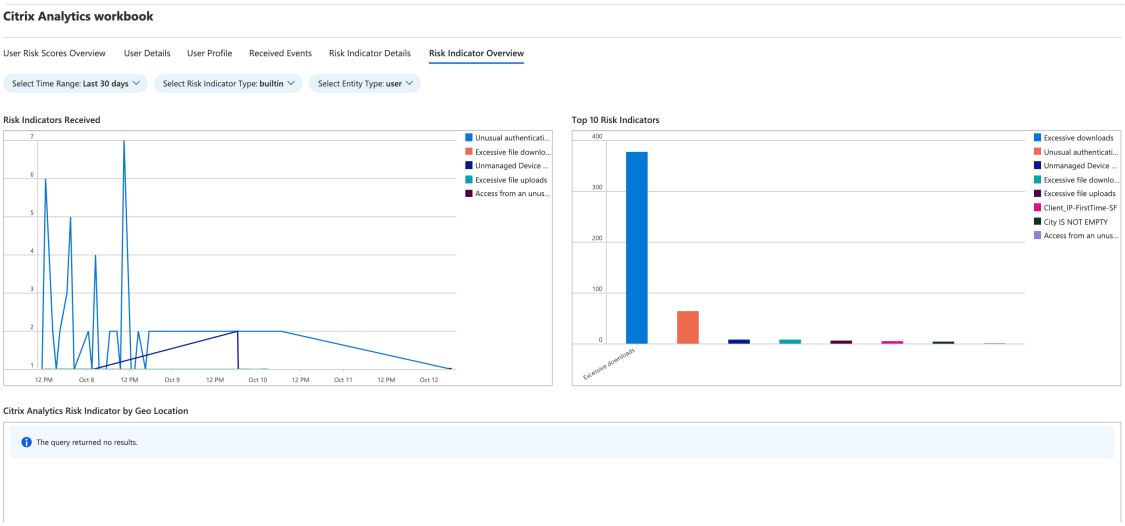
Überblick über Risikoindikatoren

Dieses Dashboard bietet eine konsolidierte Ansicht aller von Ihren Benutzern ausgelösten Risikoindikatoren.

Sie können die Risikoindikatoren anzeigen, indem Sie eine oder mehrere Kategorien auswählen:

- Zeitraum: Wählen Sie einen Zeitraum aus, um die Risikoindikatoren anzuzeigen, die in diesem Zeitraum ausgelöst wurden.
- Risikoindikatortyp: Wählen Sie entweder integriert oder benutzerdefiniert, um die zugehörigen Risikoindikatoren anzuzeigen.
- Entitätstyp: Wählen Sie einen der Benutzer aus, um die zugehörigen Risikoindikatoren anzuzeigen.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Anleitung zur Fehlerbehebung für die Sentinel-Integration über Logstash

May 5, 2023

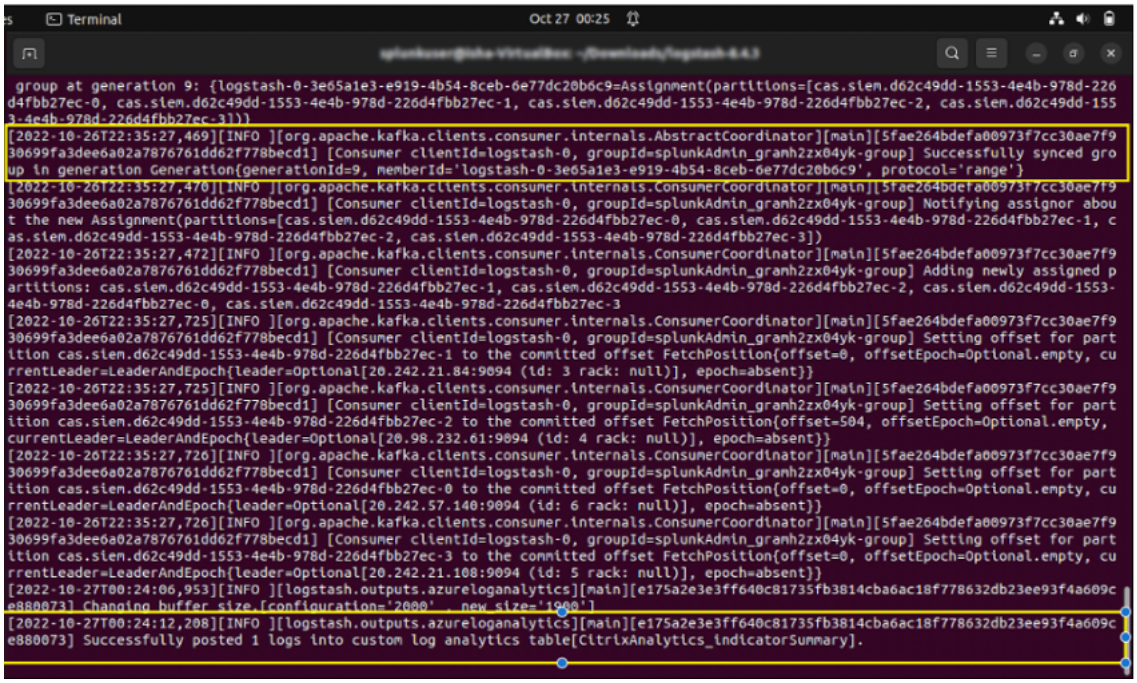
In diesem Artikel finden Sie Hinweise zur Behebung eines Problems, das bei der Integration von Microsoft Sentinel mit Citrix Analytics mithilfe von Logstash auftreten kann. Weitere Informationen dazu finden Sie unter SIEM-Integration mithilfe eines Kafka- oder Logstash-basiertenDatenkonnektors.

Überprüfen Sie die Logstash-Serverprotokolle

Sie können anhand der Logstash-Serverprotokolle, die in Ihrem Terminalfenster angezeigt werden, überprüfen, ob die Daten korrekt in die benutzerdefinierten Protokolltabellen in Ihrem Sentinel-Workspace aufgenommen wurden.

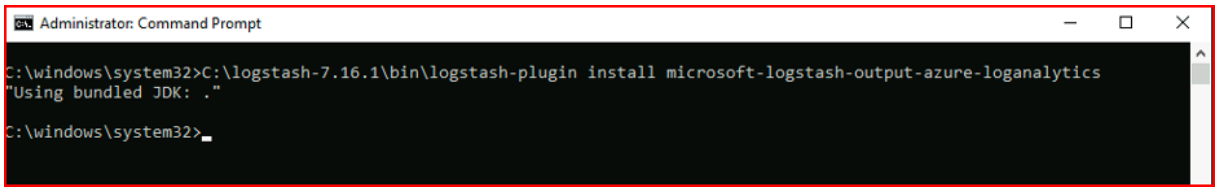
1. Um die Protokolldetails einzusehen, müssen Sie die Logstash-Konfigurationsdatei unter **Einstellungen > Datenexporte Konfiguration** herunterladen **>** und **SIEM-Umgebung** erweitern. Klicken Sie unter **Azure Sentinel (Vorschau)**auf **Logstash-Konfigurationsdatei herunterladen**.
2. Sobald Sie den Logstash-Server mithilfe der Konfigurationsdatei gestartet haben, können Sie im selben Terminalfenster nach den folgenden Protokollen Ausschau halten, die auf eine erfolgreiche Verbindung mit dem von Microsoft Azure gehosteten Log Analytics-Workspace hinweisen.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

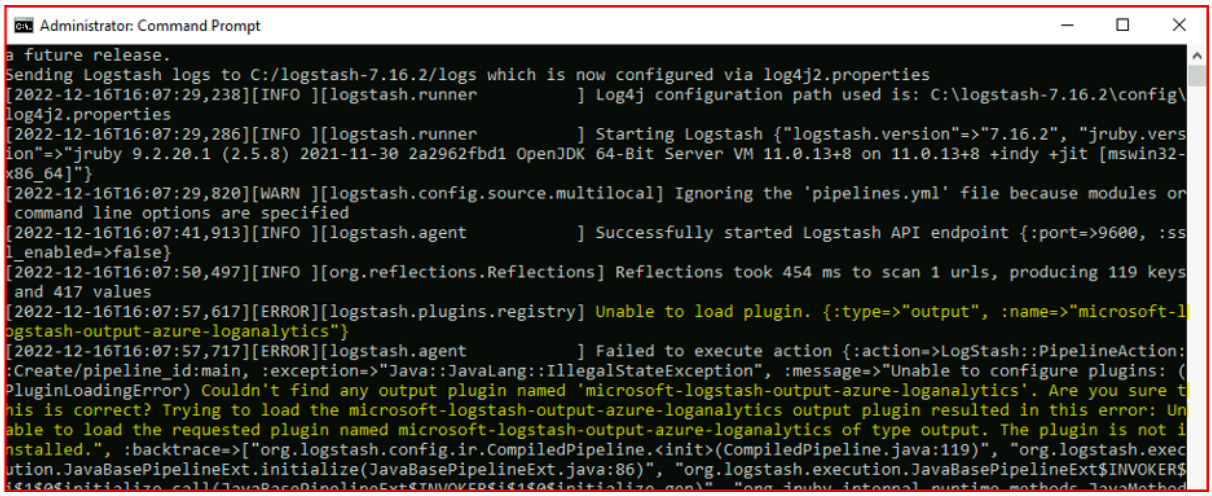


Häufiger Fehler: Verwendung des gebündelten JDK

Beim Versuch, das Microsoft Log Analytics-Plug-In zu installieren, wird ein häufig gemeldeter Fehler wie folgt gemeldet:



Danach wird beim Versuch, den Logstash-Server auszuführen, möglicherweise der folgende Fehler angezeigt:

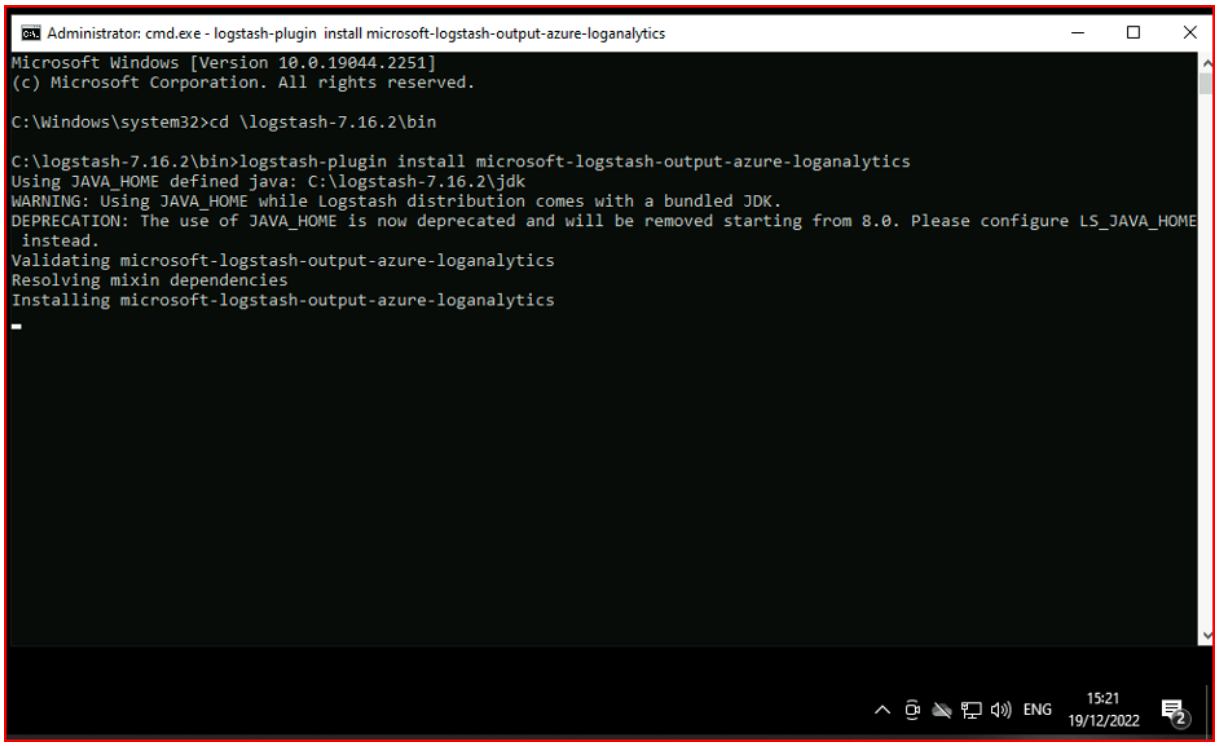


© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Um dieses Problem zu lösen, setzen Sie JAVA_HOME auf das gebündelte JDK:

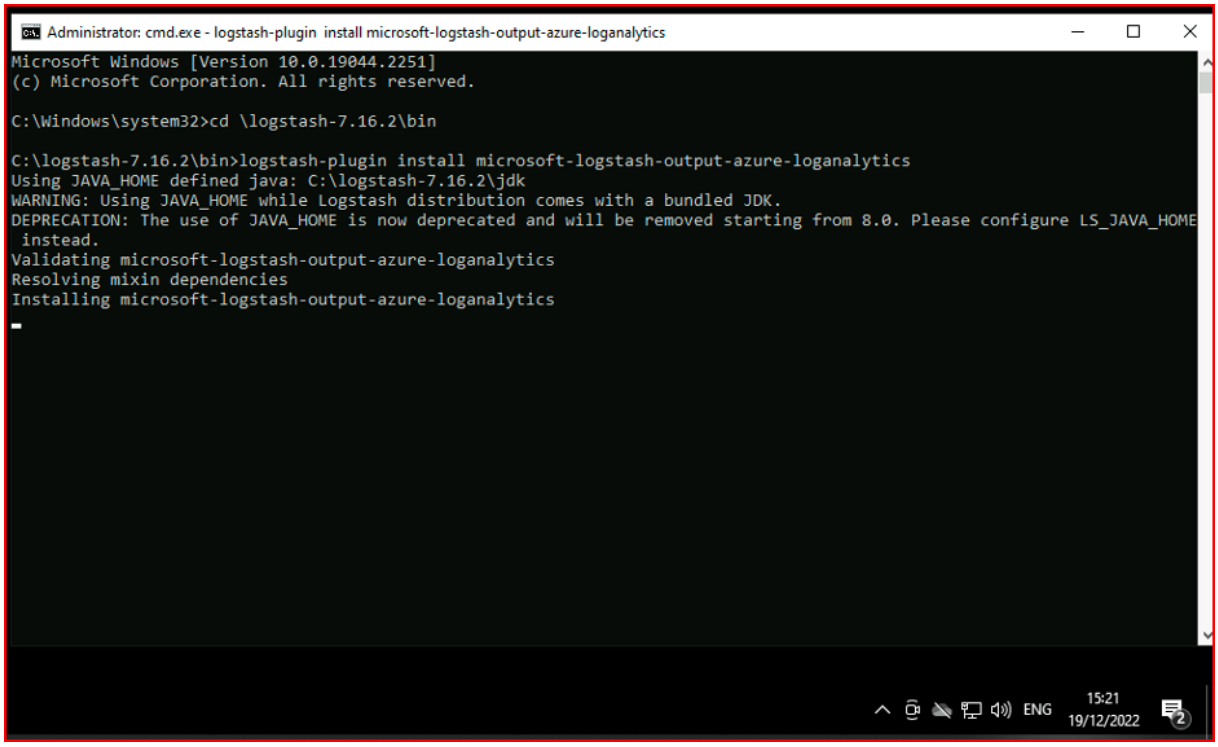
1. Gehe zu Windows-Umgebungsvariablen
2. Erstellen Sie eine neue Systemvariable mit dem Namen “JAVA_HOME”
3. < path_to_logstash >Fügen Sie den Pfad zum gebündelten Logstash-JDK hinzu (/LogStash-x.x.x/JDK)

Nachdem Sie die obigen Schritte ausgeführt haben und erneut versuchen, das Plug-in zu installieren, wird der folgende Bildschirm angezeigt:

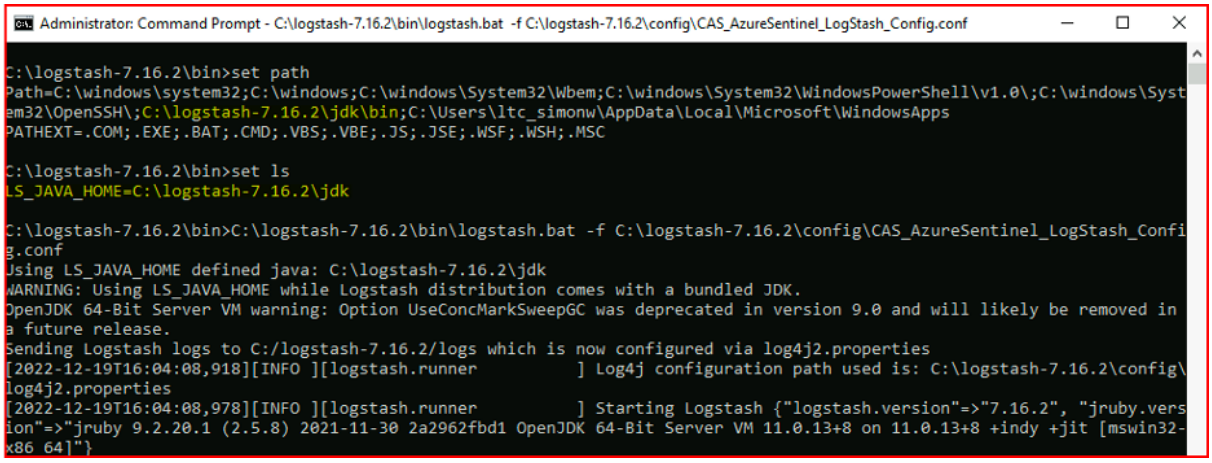


Wenn Sie LS_JAVA_HOME verwenden (da JAVA_HOME veraltet ist), müssen Sie auch den Speicherort des gebündelten JDK in der Systemvariablen PATH angeben, und dieser Pfad muss auf den Ordner jdk\ bin zeigen (im Gegensatz zur Variablen **LS_JAVA_HOME**):

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Wenn Sie LS_JAVA_HOME verwenden (da JAVA_HOME veraltet ist), müssen Sie auch den Speicherort des gebündelten JDK in der Systemvariablen PATH angeben, und dieser Pfad muss auf den Ordner jdk\ bin zeigen (im Gegensatz zur Variablen **LS_JAVA_HOME**):

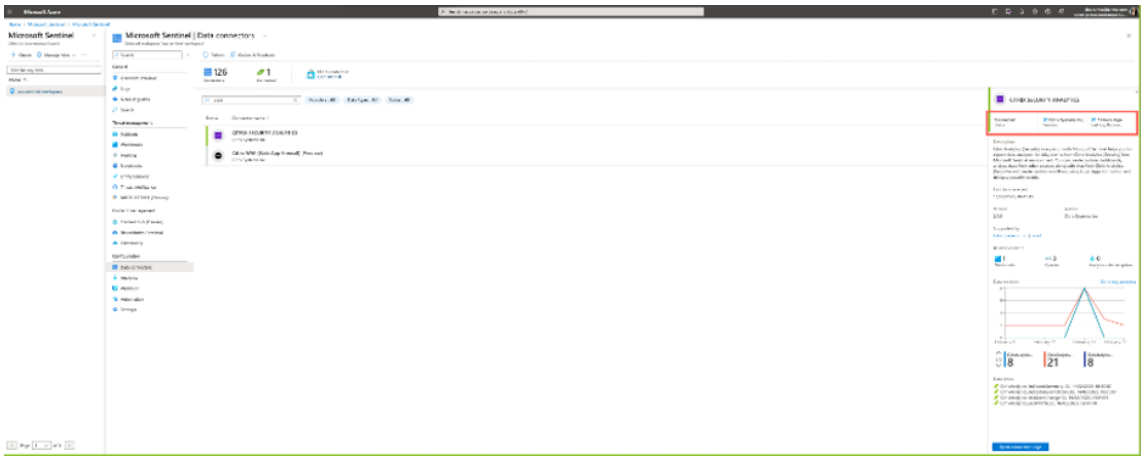


Überprüfen Sie die Microsoft Sentinel-Arbeitsmappe

Um zu überprüfen, ob von Citrix Analytics gesendete Daten erfolgreich in die entsprechende benutzerdefinierte Protokolltabelle im Log Analytics Workspace eingegeben wurden (Weitere Informationen zur Integration von Microsoft Sentinel mit Citrix Analytics finden Sie unter Microsoft Sentinel-Integration):

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

1. Navigieren Sie zum **Azure-Portal > Microsoft Sentinel**. Wählen Sie den gewünschten_Workspace > Datenconnectors. Wählen Sie **Citrix Security Analytics** aus und klicken Sie darauf.
2. Überprüfen Sie in der oberen Leiste den Verbindungsstatus.



3. Unter den Arbeitsmappen können Sie intuitive Filter verwenden, um die Daten weiter aufzuschlüsseln und die Informationen zu den Risikoindikatoren abzurufen. Um die Informationen abzurufen, navigieren Sie zum **Azure-Portal > Microsoft Sentinel > Data Connectors > CITRIX SECURITY ANALYTICS > Workbooks**.

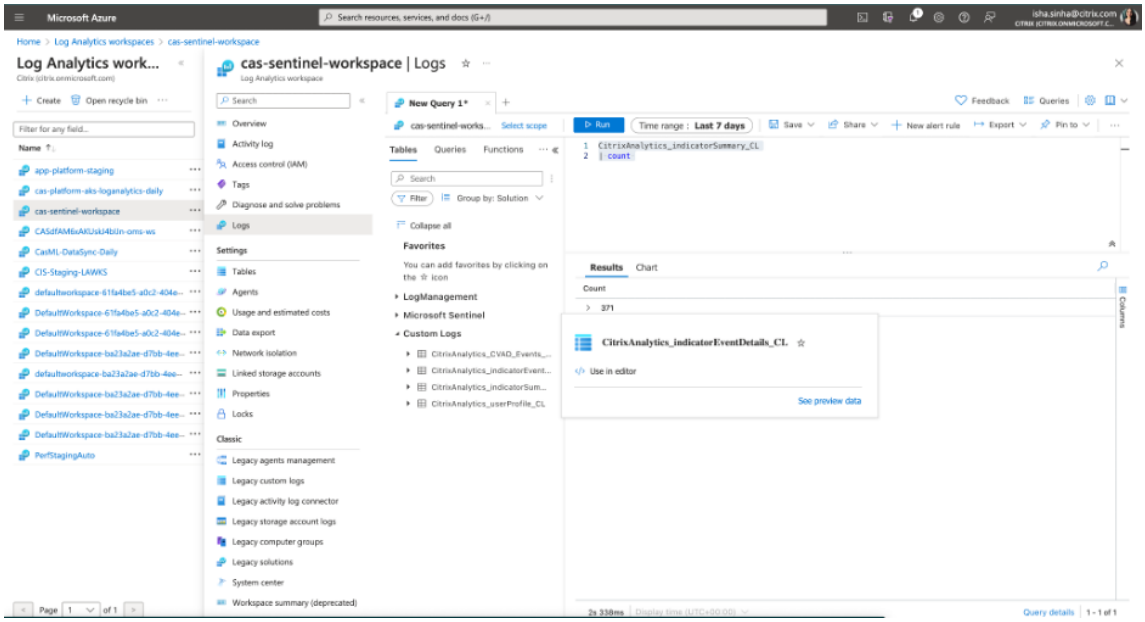
Überprüfen Sie die Log Analytics-Workspace-Protokolle mithilfe von KQL

Sie können auch überprüfen, ob die richtigen Daten in Ihren LogAnalytics-Workspace gelangt sind, indem Sie KQL-Abfragen in den entsprechenden benutzerdefinierten Protokolltabellen ausführen.

1. Navigieren Sie zum **Azure-Portal > Log Analytics-Workspaces** und suchen Sie nach dem richtigen Workspace.
2. Wählen Sie im linken Bereich **Protokolle** aus und suchen Sie auf der Registerkarte **Tabellen** nach der benutzerdefinierten Protokollanalysetabelle.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

3. Wählen Sie die benutzerdefinierte Protokollanalysetabelle aus und klicken Sie auf **Im Editor verwenden**. (Anleitungen zu KQL-Abfragen im Log Analytics-Workspace finden Sie im Log Analytics-Tutorial).
4. Klicken Sie auf **Ausführen**.



Elasticsearch-Integration

November 16, 2023

> **Hinweis**
>
> Wenden Sie sich an CAS-PM-Ext@cloud.com, um Unterstützung für die Elasticsearch-Integration, den Export von Daten nach Elasticsearch anzufordern oder Feedback zu geben.

Integrieren Sie Citrix Analytics for Security mit Elasticsearch mithilfe der Logstash-Engine. Diese Integration ermöglicht es Ihnen, die Daten der Benutzer aus Ihrer Citrix IT-Umgebung nach Elasticsearch zu exportieren und zu korrelieren und so tiefere Einblicke in die Sicherheitslage Ihres Unternehmens zu erhalten. Sie können Elasticsearch auch mit den Visualisierungsdiensten und SIEMs wie Kibana und LogRhythm verwenden.

Weitere Informationen zu den Vorteilen der Integration und der Art der verarbeiteten Daten, die an Ihr SIEM gesendet werden, finden Sie unter Integration von Sicherheitsinformationen und Ereignismanagement.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Voraussetzungen

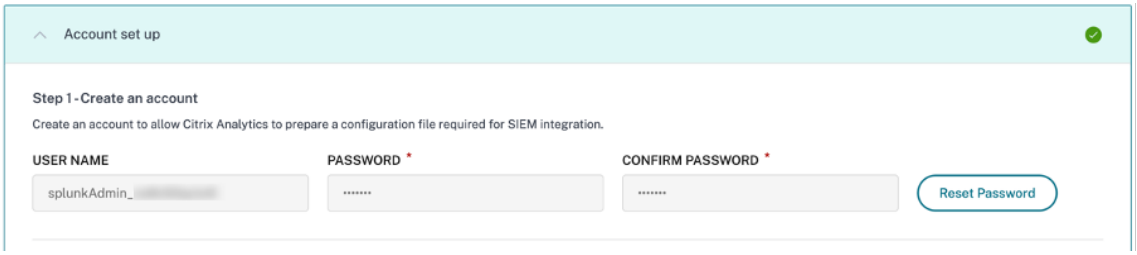
- Aktivieren Sie die Datenverarbeitung für mindestens eine Datenquelle. Es hilft Citrix Analytics for Security, den Integrationsprozess von Elasticsearch zu starten.
- Stellen Sie sicher, dass der folgende Endpunkt in der Zulassen Liste in Ihrem Netzwerk enthalten ist.

Endpunkt	Region der Vereinigten Staaten	Region der Europäischen Union	Asien-Pazifik Süd

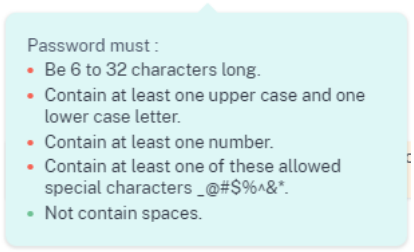
Kafka Broker	`casnb-0.citrix.com:9094`
	`casnb-1.citrix.com:9094`
	`casnb-2.citrix.com:9094`
	`casnb-3.citrix.com:9094`
		`casnb-eu-0.citrix.com:9094`
		`casnb-eu-1.citrix.com:9094`
		`casnb-eu-2.citrix.com:9094`
			`casnb-aps-0.citrix.com:9094`
			`casnb-aps-1.citrix.com:9094`
			`casnb-aps-2.citrix.com:9094`

Integrieren Sie mit Elasticsearch

1. Gehen Sie zu **Einstellungen > Datenexporte**.
2. Erstellen Sie im Abschnitt **Kontoeinrichtung** ein Konto, indem Sie den Benutzernamen und ein Kennwort angeben. Dieses Konto wird verwendet, um eine Konfigurationsdatei vorzubereiten, die für die Integration erforderlich ist.

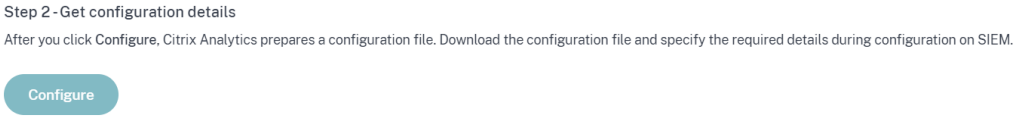


3. Stellen Sie sicher, dass das Kennwort die folgenden Bedingungen erfüllt:



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

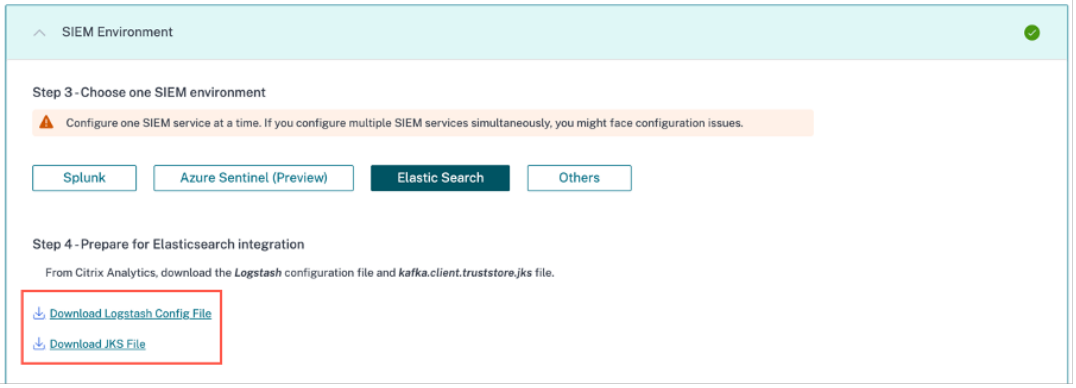
4. Klicken Sie auf **Konfigurieren**, um die Logstash-Konfigurationsdatei zu erstellen



5. Wählen Sie im Abschnitt SIEM-Umgebung die Registerkarte **Elastic Search**, um die Konfigurationsdateien herunterzuladen:

   - **Logstash-Konfigurationsdatei**: Enthält die Konfigurationsdaten (Eingabe-, Filter- und Ausgabeabschnitte) zum Senden von Ereignissen von Citrix Analytics for Security an Elasticsearch mithilfe der Logstash-Datenerfassungsmaschine. Informationen zur Struktur der Logstash-Konfigurationsdatei finden Sie in der Logstash-Dokumentation .
   - **JKS-Datei**: Enthält die für die SSL-Verbindung erforderlichen Zertifikate.

   > **Hinweis**
   >
   > Diese Dateien enthalten sensible Informationen. Bewahren Sie sie an einem sicheren Ort auf.



6. Konfigurieren Sie Logstash:

   a) Installieren Sie Logstash auf Ihrem Linux- oder Windows-Hostcomputer. Sie können auch Ihre vorhandene Logstash-Instanz verwenden.

   b) Platzieren Sie auf dem Host-Computer, auf dem Sie Logstash installiert haben, die folgenden Dateien in das angegebene Verzeichnis:

Host-Maschinentyp	Dateiname	Pfad für das Verzeichnis
Linux	CAS_Elasticsearch_LogStash_Config.conf	Für Debian- und RPM-Pakete: `/etc/logstash/conf.d/`

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Host-Maschinentyp	Dateiname	Pfad für das Verzeichnis
Windows	CAS_Elasticsearch_LogStash_Config.conf	Für .zip- und .tar.gz-Archive: `{ extract.path } / config` Für Debian- und RPM-Pakete: `/etc/logstash/ssl/` Für .zip- und .tar.gz-Archive: `{ extract.path } /ssl` C:\Logstash-7.xx.x\ config
	kafka.client.truststore.jks	

Informationen zur Standardverzeichnisstruktur von Logstash-Installationspaketen finden Sie in der Logstash-Dokumentation .

c) Öffnen Sie die Logstash-Konfigurationsdatei und gehen Sie wie folgt vor:

i. Geben Sie im Eingabebereich der Datei die folgenden Informationen ein:

- **Kennwort**: Das Kennwort des Kontos, das Sie in Citrix Analytics for Security zur Vorbereitung der Konfigurationsdatei erstellt haben.
- **SSL-Truststore-Standort**: Der Speicherort Ihres SSL-Clientzertifikats. Dies ist der Speicherort der Datei kafka.client.truststore.jks auf Ihrem Host-Computer.

```
input {
  kafka {
    bootstrap_servers => "[redacted]"
    topics => ['[redacted]']
    group_id => '[redacted]'
    session_timeout_ms => 60000
    auto_offset_reset => "earliest"
    security_protocol => "SASL_SSL"
    sasl_mechanism => "SCRAM-SHA-256"
    ssl_endpoint_identification_algorithm => ""
    sasl_jaas_config => "org.apache.kafka.common.security.scram.ScramLoginModule required username='[redacted]' password='<your password>';"
    ssl_truststore_location => "/etc/logstash/ssl/kafka.client.truststore.jks"
  }
}
```

ii. Geben Sie im Ausgabebereich der Datei die Adresse Ihres Host-Computers oder des Clusters ein, in dem Elasticsearch ausgeführt wird.

```
}
output {
  elasticsearch {
    hosts => ["<your logstash host : port>"]
    index => "citrixanalytics-%{+YYYY.MM.dd}"
  }
}
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

d) Starten Sie Ihren Host-Computer neu, um verarbeitete Daten von Citrix Analytics for Security an Elasticsearch zu senden.

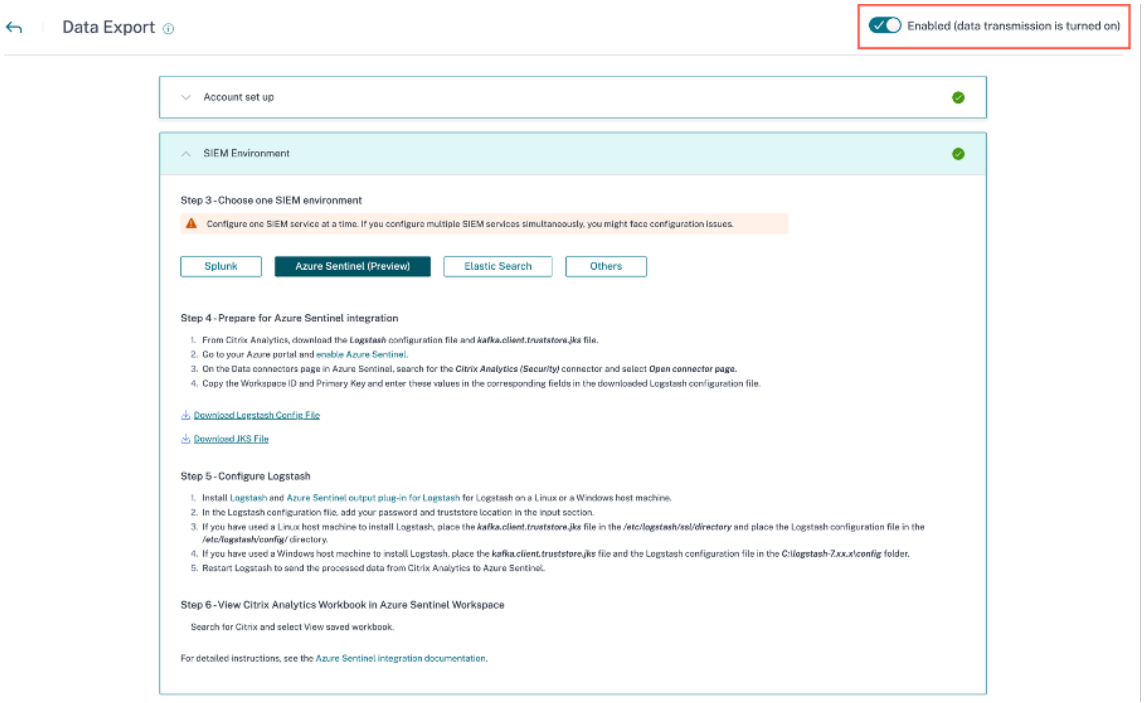
Stellen Sie nach Abschluss der Konfiguration sicher, dass Sie die Citrix Analytics-Daten in Ihrer Elasticsearch anzeigen können.

Aktivieren oder Deaktivieren der Datenübertragung

Nachdem Citrix Analytics for Security die Konfigurationsdatei vorbereitet hat, ist die Datenübertragung für Elasticsearch aktiviert.

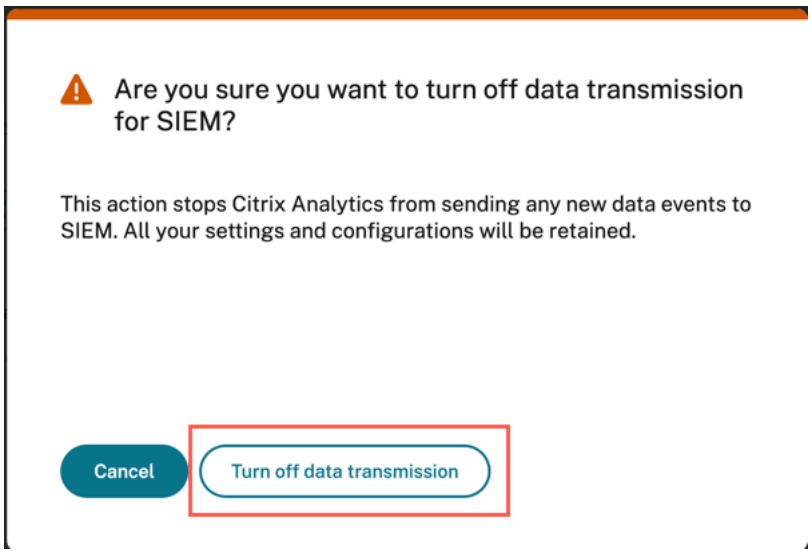
So beenden Sie die Übertragung von Daten aus Citrix Analytics for Security:

1. Gehen Sie zu **Einstellungen > Datenexporte**.
2. Schalten Sie die Umschalttaste aus, um die Datenübertragung zu deaktivieren. Standardmäßig ist die **Datenübertragung** immer aktiviert..



Zur Bestätigung wird ein Warnfenster angezeigt. Klicken Sie auf die Schaltfläche **Datenübertragung ausschalten**, um die Übertragungsaktivität zu beenden.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Um die Datenübertragung wieder zu aktivieren, schalten Sie die Umschalttaste ein.

SIEM-Integration mit Kafka oder Logstash-basiertem DatenConnector

November 16, 2023

Die SIEM-Integration von Citrix Analytics for Security ermöglicht es Ihnen, die Benutzerdaten aus Citrix Analytics in Ihre SIEM-Umgebung zu exportieren und zu korrelieren und tiefere Einblicke in die Sicherheitslage Ihres Unternehmens zu erhalten.

Weitere Informationen zu den Vorteilen der Integration und zur Art der Datenereignisse (Risikoeinblicke und Datenquellenereignisse), die an Ihr SIEM gesendet werden, finden Sie unter Integration von Sicherheitsinformationen und Ereignismanagement.

Sie können Citrix Analytics for Security über die folgenden zwei Mechanismen in Ihre SIEM-Lösungen integrieren (unterstützt von Ihrer SIEM- und IT-Bereitstellung):

1. Stellen Sie eine Verbindung über Kafka-Endpunkte her
2. Stellen Sie eine Verbindung über den Logstash-Datenbroker mit Kafka-basierter Ingestion her

Voraussetzungen

- Aktivieren Sie die Datenverarbeitung für mindestens eine Datenquelle. Es hilft Citrix Analytics for Security, mit der Integration mit Ihrem SIEM-Tool zu beginnen.
- Stellen Sie sicher, dass der folgende Endpunkt in der Zulassen Liste in Ihrem Netzwerk enthalten ist.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Endpunkt	Region der Vereinigten Staaten	Region der Europäischen Union	Asien-Pazifik Süd
Kafka Broker	casnb-0.citrix.com:9094 casnb-1.citrix.com:9094 casnb-2.citrix.com:9094 casnb-3.citrix.com:9094	casnb-eu-0.citrix.com:9094 casnb-eu-1.citrix.com:9094 casnb-eu-2.citrix.com:9094	casnb-aps-0.citrix.com:9094 casnb-aps-1.citrix.com:9094 casnb-aps-2.citrix.com:9094

Integrieren mit Kafka in einen SIEM-Service

Kafka ist eine Open-Source-Software, die für das Streaming von Daten in Echtzeit verwendet wird. Mit Kafka können Sie die Echtzeitdaten analysieren, um schnellere Erkenntnisse zu gewinnen. Vor allem die großen Organisationen, die mit ausreichenden Daten umgehen, verwenden Kafka.

Northbound Kafka ist eine interne mittlere Ebene, die es Citrix Analytics ermöglicht, Echtzeit-Datenfeeds über Kafka-Endpunkte mit den SIEM-Kunden zu teilen. Wenn Ihr SIEM Kafka-Endpoints unterstützt, verwenden Sie die in der Logstash-Konfigurationsdatei angegebenen Parameter und die Zertifikatsdetails in der JKS-Datei oder der PEM-Datei, um Ihr SIEM in Citrix Analytics for Security zu integrieren.

Die folgenden Parameter sind für die Integration mit Kafka erforderlich:

Name des Attributs	Beschreibung	Beispiel für Konfigurationsdaten
Benutzername	Von Kafka bereitgestellter Benutzername.	`'sasl.username': cas_siem_user_name,`
Host	Hostname des Kafka-Servers, zu dem Sie eine Verbindung herstellen möchten.	`'bootstrap.servers': cas_siem_host,`
Topic name/Client ID	Einem Mandanten zugewiesene Client-ID.	`'client.id': cas_siem_topic,`
Gruppenname/ID	Gruppenname, den Sie benötigen, um die von den Verbrauchern geteilten Nachrichten zu lesen.	`'group.id': cas_siem_group_id,`

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Name des Attributs	Beschreibung	Beispiel für Konfigurationsdaten
Sicherheitsprotokoll	Name des Sicherheitsprotokolls.	`'security.protocol': 'SASL_SSL',`
SASL-Mechanismen	Authentifizierungsmechanismus, der normalerweise für die Verschlüsselung verwendet wird, um eine sichere Authentifizierung zu implementieren.	`'sasl.mechanisms': 'SCRAM-SHA-256',`
SSL Truststore-Standort	Ort, an dem Sie die Zertifikatsdatei speichern können. Das Truststore-Kennwort des Clients ist optional und wird voraussichtlich leer gelassen.	`'ssl.ca.location': ca_location`
Sitzungstimeout	Das Sitzungs-Timeout, das verwendet wird, um Client-Fehler bei der Verwendung von Kafka zu erkennen.	`'session.timeout.ms': 60000,`
Autom. Offset	Definiert das Verhalten beim Verbrauchen von Daten aus einer Themenpartition, wenn es keinen anfänglichen Offset gibt. Sie können Werte wie “Späteste”, “Früheste”oder “Keine”festlegen.	`'auto.offset.reset': 'earliest',`

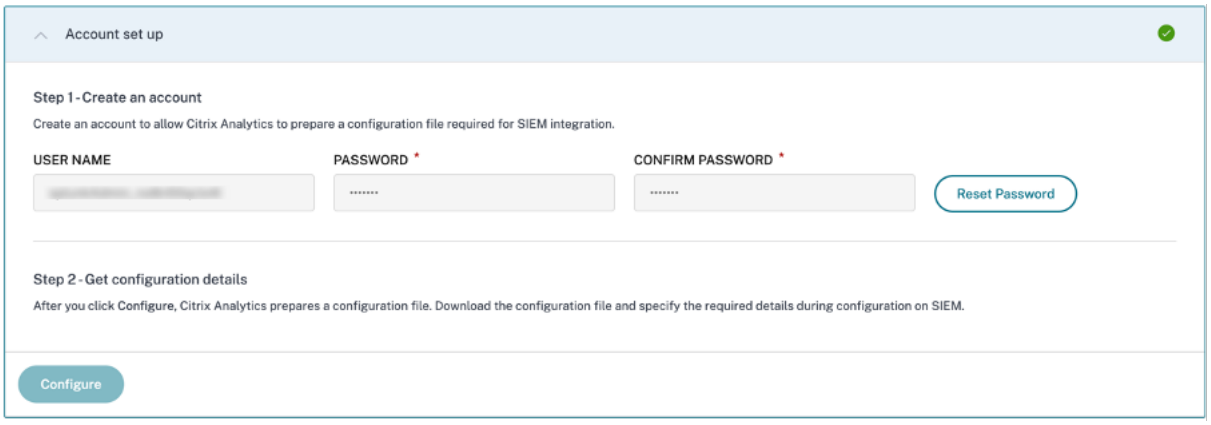
Im Folgenden finden Sie ein Beispiel für eine Konfigurationsausgabe:

```
{
 'bootstrap.servers': cas_siem_host,
                      'client.id': cas_siem_topic,
                      'group.id': cas_siem_group_id,
                      'session.timeout.ms': 60000,
                      'auto.offset.reset': 'earliest',
                      'security.protocol': 'SASL_SSL',
                      'sasl.mechanisms': 'SCRAM-SHA-256',
                      'sasl.username': cas_siem_user_name,
                      'sasl.password': self.CLEAR_PASSWORD,
```

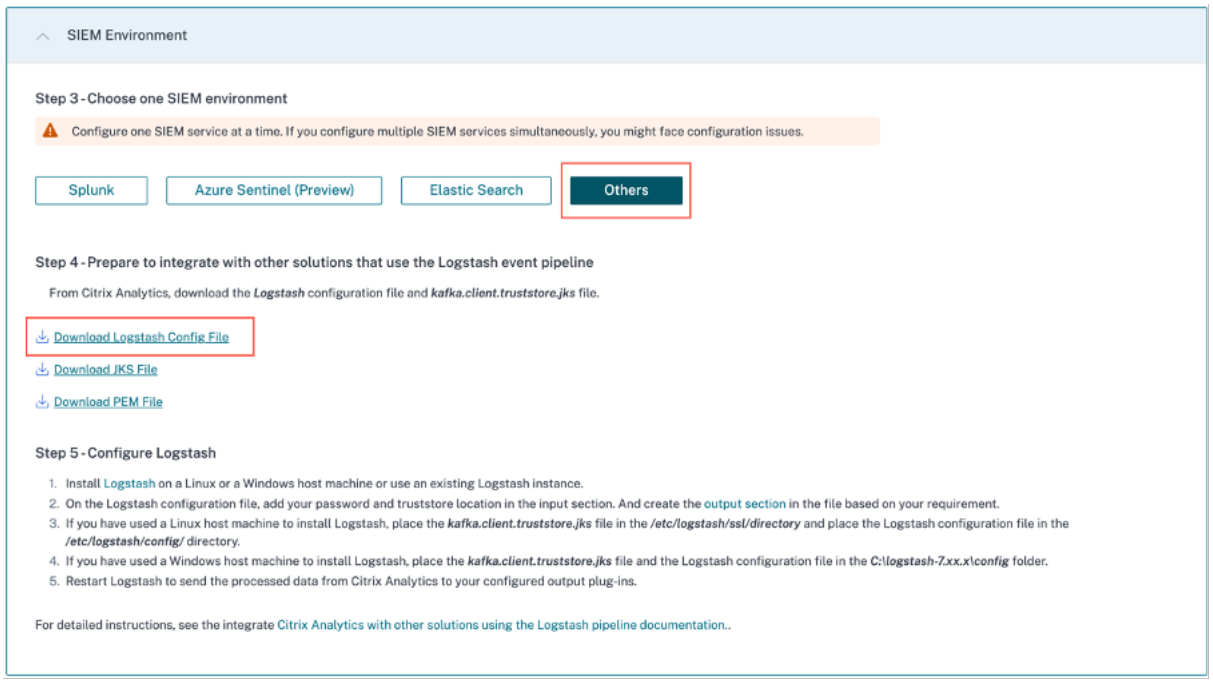
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
                    'ssl.ca.location': ca_location
                }


<!--NeedCopy-->
```



Die oben genannten Parameter sind in der Logstash-Konfigurationsdatei verfügbar. Um die Konfigurationsdatei herunterzuladen, navigieren Sie zu **Einstellungen > Datenexporte > SIEM-Umgebung**, wählen Sie die Registerkarte **Andere** aus und klicken Sie auf **Logstash-Konfigurationsdatei herunterladen**.



Weitere Informationen zu den Konfigurationswerten finden Sie unter Konfiguration.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Datenfluss

Die Kommunikation der Authentifizierungsdaten erfolgt zwischen den serverseitigen Kafka-Brokern (Citrix Analytics for Security Cloud) und den Kafka-Clients. Die gesamte Kommunikation zwischen Brokern und externen Kunden verwendet das aktivierte SASL_SSL-Sicherheitsprotokoll und den Zielport 9094 für den öffentlichen Zugriff.

Apache Kafka verfügt über eine Sicherheitskomponente, um die Daten während des Fluges mithilfe der SSL-Verschlüsselung zu verschlüsseln.
Die Datenübertragung über das Netzwerk ist verschlüsselt und gesichert, wenn die Verschlüsselung aktiviert ist und SSL-Zertifikate gesetzt sind. Nur der erste und der letzte Computer sind in der Lage, die über SSL gesendeten Pakete zu entschlüsseln.

Authentifizierungen

Es stehen zwei Authentifizierungsstufen wie folgt zur Verfügung:

1. TLS/zwischen Client und Server.
    - Die Serverzertifikate (öffentliche Schlüssel) für den TLS-Authentifizierungsaustausch zwischen Client und Server.
    - Die clientbasierte Authentifizierung oder bidirektionale Authentifizierungen werden nicht unterstützt (wenn private Client-Schlüsselzertifikate erforderlich sind).
2. Benutzername/Kennwort für die Zugriffskontrolle zu Themen/Endpunkten
    - Stellt sicher, dass ein bestimmter Kunde nur zu einem bestimmten Kundenthema lesen kann
    - SASL/SCRAM wird für den Authentifizierungsmechanismus für Benutzername/Kennwörter zusammen mit der TLS-Verschlüsselung verwendet, um eine sichere Authentifizierung zu implementieren.

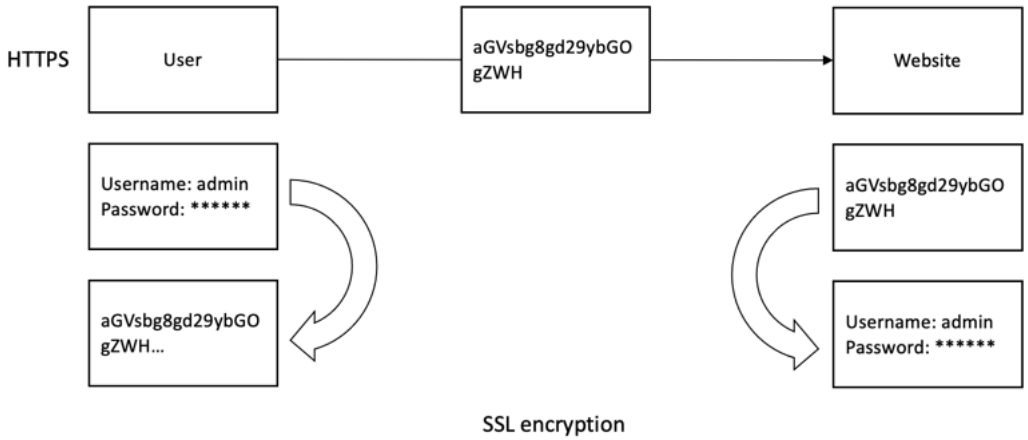
Verschlüsselung mit SSL und Authentifizierung mit SASL/SSL&SASL/PLAINTEXT

Standardmäßig kommuniziert Apache Kafka in PLAINTEXT, wobei alle Daten im Klartext gesendet werden und jeder der Router den Dateninhalt lesen kann. Apache Kafka verfügt über eine Sicherheitskomponente, um die Daten während des Fluges mithilfe der SSL-Verschlüsselung zu verschlüsseln. Wenn die Verschlüsselung aktiviert ist und SSL-Zertifikate sorgfältig eingerichtet wurden, werden die Daten jetzt verschlüsselt und sicher über das Netzwerk übertragen. Bei der SSL-Verschlüsselung besitzt nur das erste und das letzte Gerät die Fähigkeit, das gesendete Paket zu entschlüsseln.

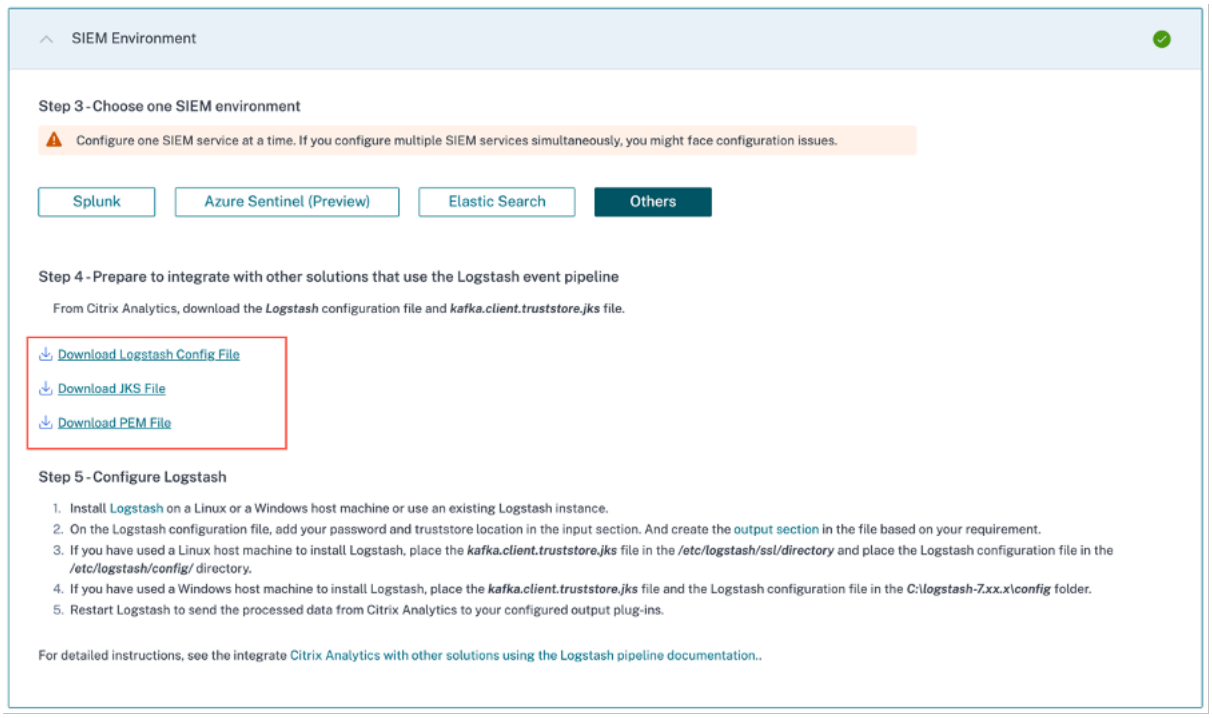
Da die bidirektionale SSL-Verschlüsselung verwendet wird, ist die Anmeldung mit Benutzername/Kennwort für die externe Kommunikation sicher.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Die Verschlüsselung erfolgt nur während des Fluges und die Daten befinden sich immer noch unverschlüsselt auf dem Datenträger des Brokers.



In der Client-Konfiguration sind die Client-Truststore-JKS-Datei und die PEM-Datei (konvertiert aus der Truststore-JKS-Datei) erforderlich. Sie können diese Dateien von der Citrix Analytics for Security GUI herunterladen, wie im folgenden Screenshot gezeigt:



SIEM-Integration mit Logstash

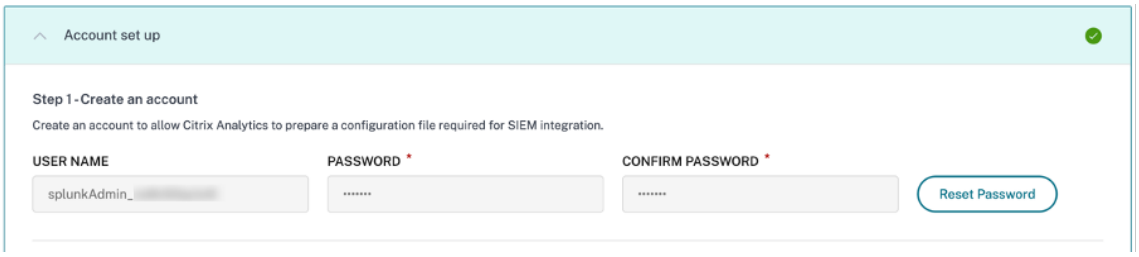
Wenn Ihr SIEM keine Kafka-Endpunkte unterstützt, können Sie die **Logstash-Datenerfassungs-Engine** verwenden. Sie können die Datenereignisse von Citrix Analytics for Security an eines der Ausgabe-Plug-ins senden, die von Logstash unterstützt werden.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

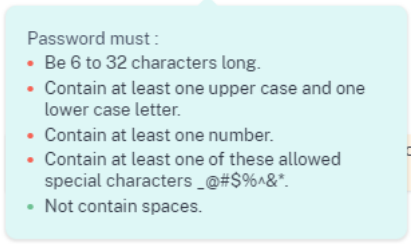
Im folgenden Abschnitt werden die Schritte beschrieben, die Sie ausführen müssen, um Ihr SIEM mithilfe von Logstash in Citrix Analytics for Security zu integrieren.

Mit Logstash in einen SIEM-Dienst integrieren

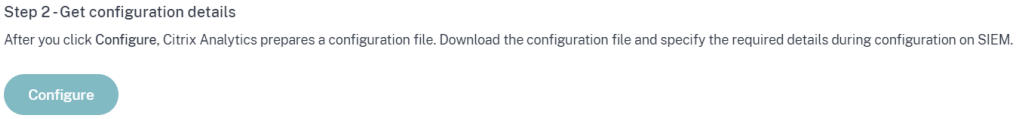
1. Gehen Sie zu **Einstellungen > Datenexporte**.
2. Erstellen Sie auf der Seite **Konto einrichten** ein Konto, indem Sie den Benutzernamen und ein Kennwort angeben. Dieses Konto wird verwendet, um eine Konfigurationsdatei vorzubereiten, die für die Integration erforderlich ist.



3. Stellen Sie sicher, dass das Kennwort die folgenden Bedingungen erfüllt:



4. Wählen Sie **Konfigurieren**, um die Logstash-Konfigurationsdatei zu erstellen.

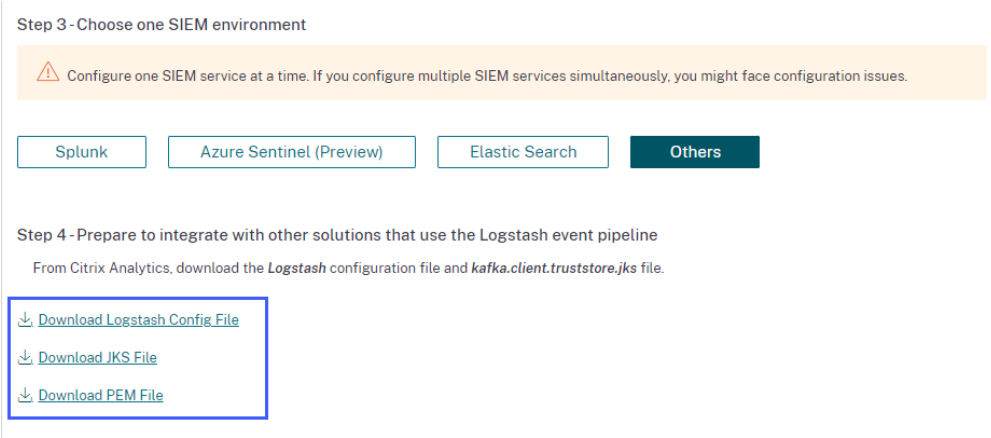


5. Wählen Sie die Registerkarte **Andere**, um die Konfigurationsdateien herunterzuladen.

   - **Logstash-Konfigurationsdatei**: Diese Datei enthält die Konfigurationsdaten (Eingabe-, Filter- und Ausgabeabschnitte) zum Senden von Ereignissen von Citrix Analytics for Security mithilfe der Logstash-Datenerfassungs-Engine. Informationen zur Struktur der Logstash-Konfigurationsdatei finden Sie in der Logstash-Dokumentation .
   - **JKS-Datei**: Diese Datei enthält die für die SSL-Verbindung erforderlichen Zertifikate. Diese Datei ist erforderlich, wenn Sie Ihr SIEM mit Logstash integrieren.
   - **PEM-Datei**: Diese Datei enthält die für die SSL-Verbindung erforderlichen Zertifikate. Diese Datei ist erforderlich, wenn Sie Ihr SIEM mit Kafka integrieren.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Hinweis**
>
> Diese Dateien enthalten sensible Informationen. Bewahren Sie sie an einem sicheren Ort auf.



6. Konfigurieren Sie Logstash:

   a) Installieren Sie Logstash auf Ihrem Linux- oder Windows-Hostcomputer (getestete Versionen auf Kompatibilität mit Citrix Analytics for Security: v7.17.7 und v8.5.3). Sie können auch Ihre vorhandene Logstash-Instanz verwenden.

   b) Platzieren Sie auf dem Host-Computer, auf dem Sie Logstash installiert haben, die folgenden Dateien in das angegebene Verzeichnis:

Host-Maschinentyp	Dateiname	Pfad für das Verzeichnis
Linux	CAS_Others_LogStash_Config.config	Für Debian- und RPM-Pakete: `/etc/logstash/conf.d/` Für .zip- und .tar.gz-Archive: `{ extract.path } /config`
	kafka.client.truststore.jks	Für Debian- und RPM-Pakete: `/etc/logstash/ssl/` Für .zip- und .tar.gz-Archive: `{ extract.path } /ssl`
Windows	CAS_Others_LogStash_Config.config	`C:\logstash-7.xx.x\config`
	kafka.client.truststore.jks	`C:\logstash-7.xx.x\config`

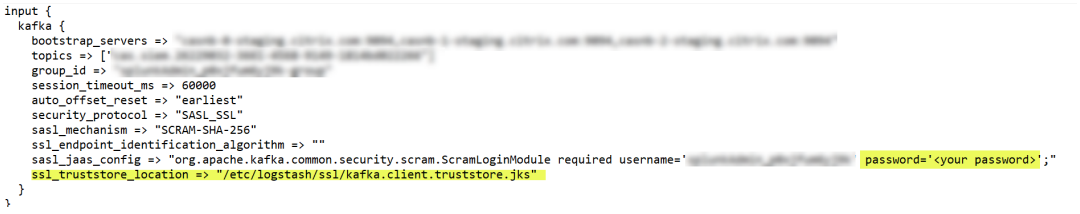
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

c) Die Logstash-Konfigurationsdatei enthält vertrauliche Informationen wie Kafka-Anmeldeinformationen, LogAnalytics Workspace-IDs und Primärschlüssel. Es wird empfohlen, diese vertraulichen Anmeldeinformationen nicht als Klartext zu speichern. Um die Integration zu sichern, kann ein Logstash-Keystore verwendet werden, um Schlüssel mit ihren jeweiligen Werten hinzuzufügen, auf die wiederum mithilfe von Schlüsselnamen in der Konfigurationsdatei verwiesen werden kann. Weitere Informationen über den Logstash-Keystore und wie er die Sicherheit Ihrer Einstellungen verbessert, finden Sie unter Secrets Keystorefür sichere Einstellungen.

d) Öffnen Sie die Logstash-Konfigurationsdatei und gehen Sie wie folgt vor:

Geben Sie im Eingabebereich der Datei die folgenden Informationen ein:

- **Kennwort**: Das Kennwort des Kontos, das Sie in Citrix Analytics for Security zur Vorbereitung der Konfigurationsdatei erstellt haben.
- **SSL-Truststore-Standort**: Der Speicherort Ihres SSL-Clientzertifikats. Dies ist der Speicherort der Datei kafka.client.truststore.jks auf Ihrem Host-Computer.



Geben Sie im Ausgabebereich der Datei den Zielpfad oder die Details ein, an die Sie die Daten senden möchten. Informationen zu den Ausgabe-Plug-Ins finden Sie in der Logstash-Dokumentation .

Das folgende Snippet zeigt, dass die Ausgabe in eine lokale Protokolldatei geschrieben wird.

```
output {
        file {
        path => "./citrixanalytics-%{+YYYY.MM.dd}.log"
    }
}
```

e) Starten Sie Ihren Hostcomputer neu, um verarbeitete Daten von Citrix Analytics for Security an Ihren SIEM-Dienst zu senden.

Melden Sie sich nach Abschluss der Konfiguration bei Ihrem SIEM-Dienst an und überprüfen Sie die Citrix Analytics-Daten in Ihrem SIEM.

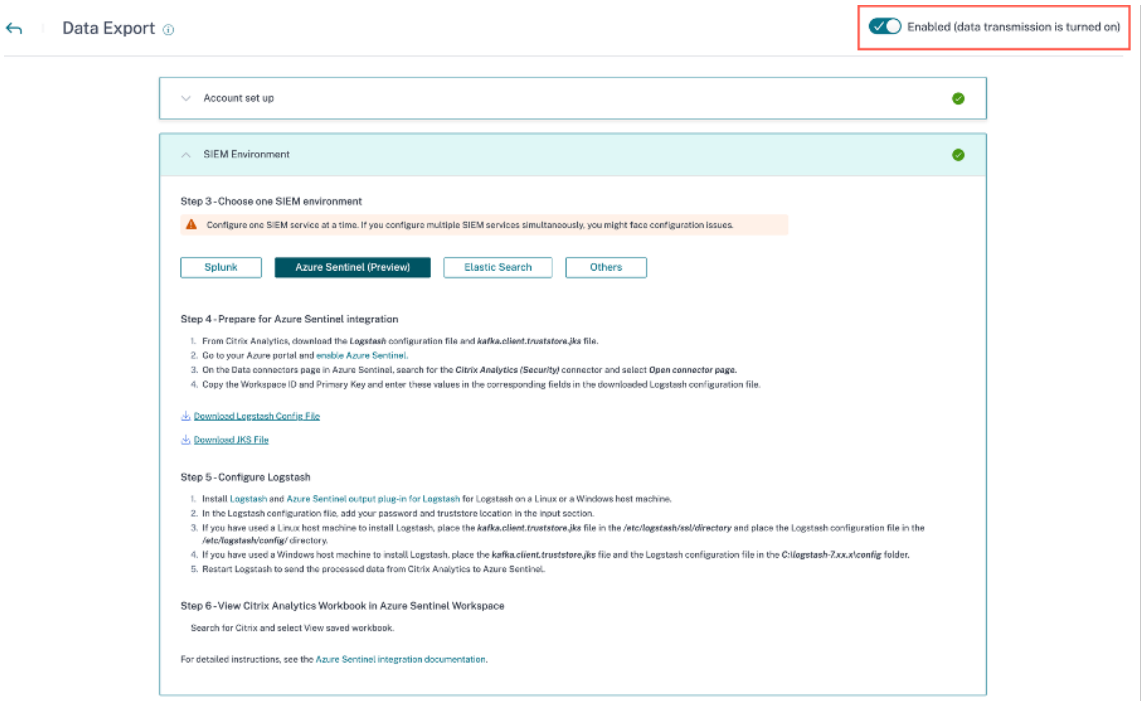
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Aktivieren oder Deaktivieren der Datenübertragung

Nachdem Citrix Analytics for Security die Konfigurationsdatei vorbereitet hat, wird die Datenübertragung für Ihr SIEM aktiviert.

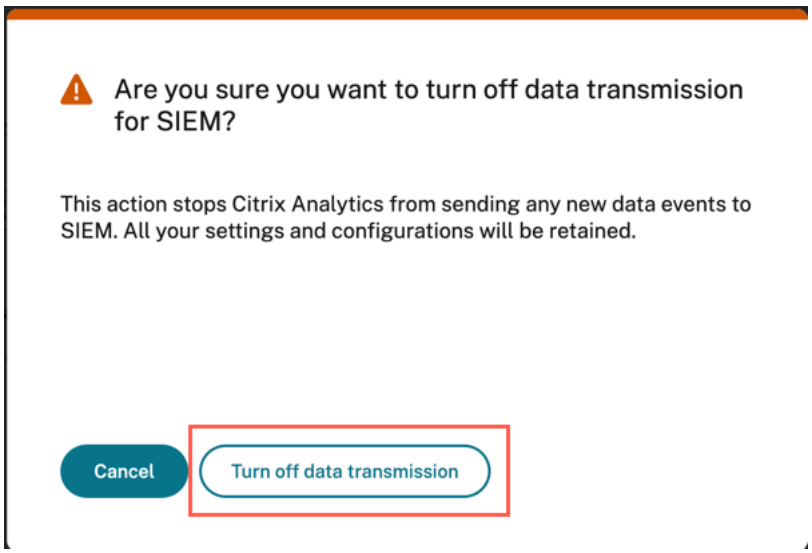
So beenden Sie die Übertragung von Daten aus Citrix Analytics for Security:

1. Gehen Sie zu **Einstellungen > Datenexporte**.
2. Schalten Sie die Umschalttaste aus, um die **Datenübertragung** zu deaktivieren. Standardmäßig ist die Datenübertragung immer aktiviert.



Zur Bestätigung wird ein Warnfenster angezeigt. Klicken Sie auf die Schaltfläche **Datenübertragung ausschalten**, um die Übertragungsaktivität zu beenden.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Um die Datenübertragung wieder zu aktivieren, schalten Sie die Umschalttaste ein.

> **Hinweis**
>
> Wenden Sie sich an CAS-PM-Ext@cloud.com, um Unterstützung für Ihre SIEM-Integration, den Export von Daten in Ihr SIEM anzufordern oder Feedback zu geben.

Citrix Analytics-Datenexportformat für SIEM

February 9, 2024

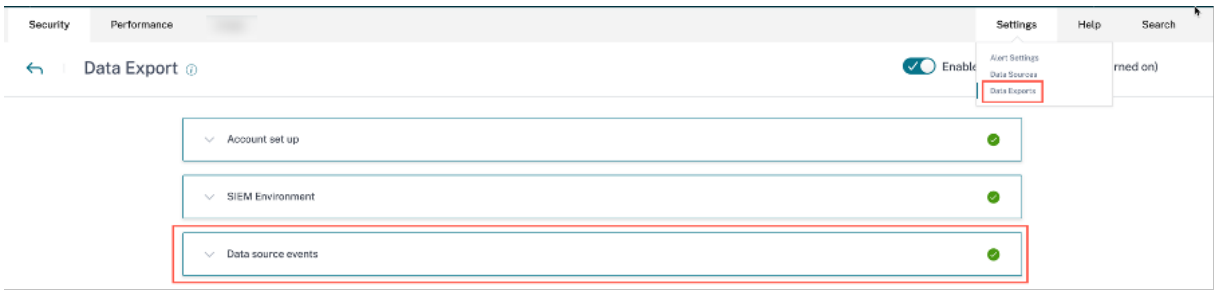
Mit Citrix Analytics for Security können Sie sich in Ihre Sicherheitsinformationen- und Ereignisverwaltungsdienste (SIEM) integrieren. Diese Integration ermöglicht es Citrix Analytics for Security, Daten an Ihre SIEM-Dienste zu senden, und hilft Ihnen, einen Einblick in die Sicherheitsrisiken Ihres Unternehmens zu erhalten.

Derzeit können Sie Citrix Analytics for Security in die folgenden SIEM-Dienste integrieren:

- Splunk
- Microsoft Azure Sentinel
- Elasticsearch
- Andere SIEMs verwenden Kafka- oder Logstash-basierten Datenconnector

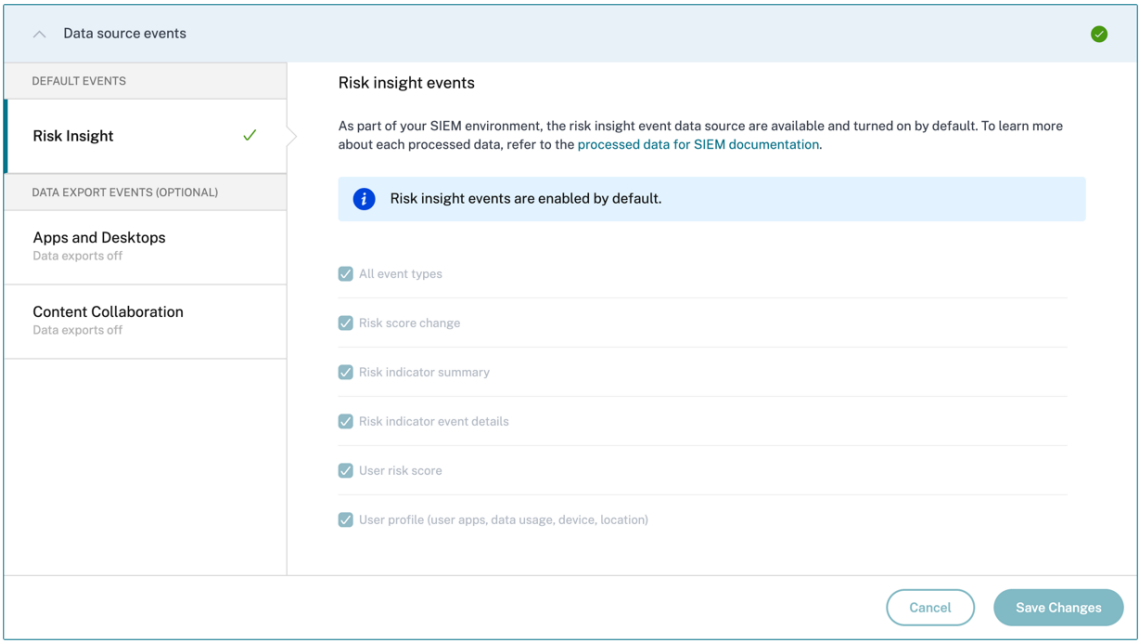
Die **Option Datenexporte** ist jetzt global unter **Einstellungen**verfügbar. Um die Datenquellenereignisse anzuzeigen, navigieren Sie zu **Einstellungen > Datenexporte > Datenquellenereignisse**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Es gibt zwei Arten von Risk Insights-Daten, die von Citrix Analytics for Security an Ihren SIEM-Dienst gesendet werden:

- Ereignisse mit Risikoeinblicken (Standardexporte)
- Datenquellenereignisse (optionale Exporte)



Daten zu Risikoeinblicken für SIEM

Sobald Sie die Kontokonfiguration und das SIEM-Setup abgeschlossen haben, fließen Standarddatensätze (Risk Insights Events) in Ihre SIEM-Bereitstellung ein. Zu den Datensätzen für Risikoinformationen gehören Ereignisse zur Risikobewertung von Benutzern, Benutzerprofilereignisse und Warnmeldungen zu Risikoindikatoren. Diese werden durch Algorithmen für maschinelles Lernen von Citrix Analytics und Benutzerverhaltensanalysen generiert, indem Benutzerereignisse genutzt werden.

Zu den Risk Insights-Datensätzen eines Benutzers gehören:

- **Änderung der Risikobewertung**: Zeigt eine Änderung der Risikobewertung des Benutzers an. Wenn die Änderung der Risikobewertung eines Benutzers gleich oder mehr als 3 ist und diese

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

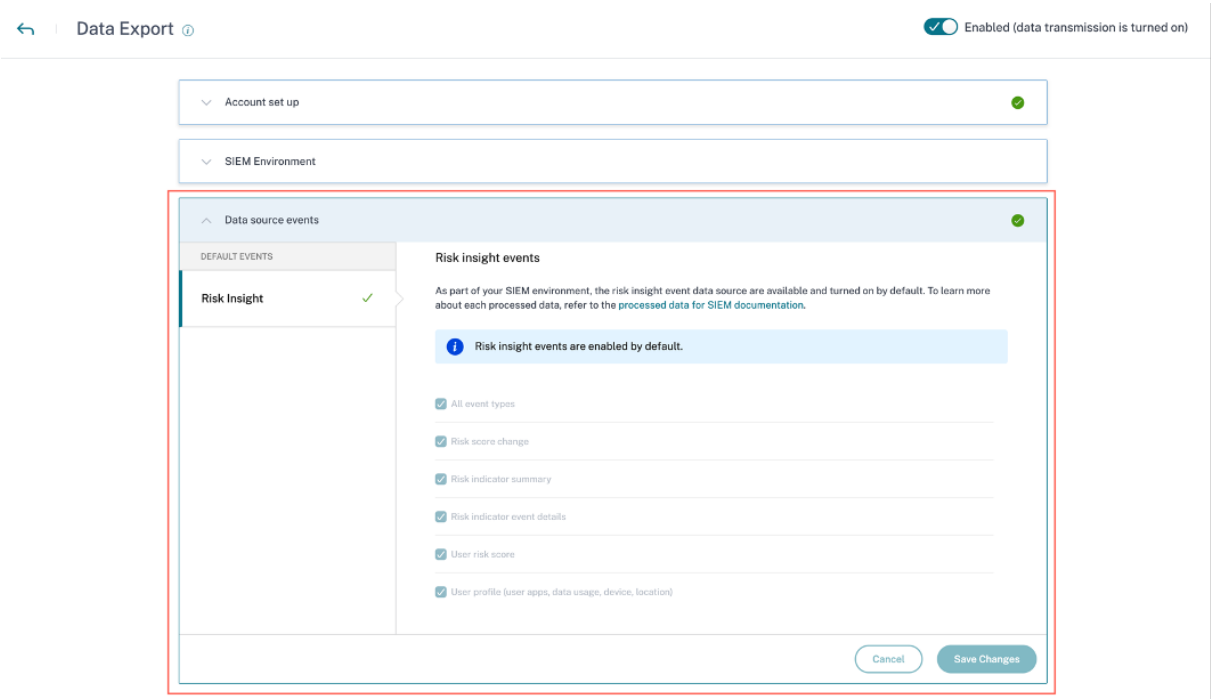
Änderung mit beliebiger Geschwindigkeit zunimmt oder um mehr als 10 % sinkt, werden die Daten an den SIEM-Dienst gesendet.

- **Zusammenfassung der Risikoindikatoren**: Die Details des Risikoindikators, der für einen Benutzer ausgelöst wurde.
- **Details zum Risikoindikatorereignis**: Die Benutzerereignisse, die einem Risikoindikator zugeordnet sind. Citrix Analytics sendet maximal 1000 Ereignisdetails für jedes Auftreten von Risikoindikatoren an Ihren SIEM-Dienst. Diese Ereignisse werden in chronologischer Reihenfolge ihres Auftretens gesendet.
- **Benutzerrisikoeinstufungsereignis**: Die aktuelle Risikobewertung eines Benutzers. Citrix Analytics for Security sendet diese Daten alle 12 Stunden an den SIEM-Dienst.
- **Benutzerprofil**: Die Benutzerprofildaten können wie folgt kategorisiert werden:
  - **Benutzer-Apps**: Die Anwendungen, die ein Benutzer gestartet und verwendet hat. Citrix Analytics for Security ruft diese Daten von Citrix Virtual Apps ab und sendet sie alle 12 Stunden an den SIEM-Dienst.
  - **Benutzergerät**: Die einem Benutzer zugewiesenen Geräte. Citrix Analytics for Security ruft diese Daten von Citrix Virtual Apps und Citrix Endpoint Management ab und sendet sie alle 12 Stunden an den SIEM-Dienst.
  - **Benutzerstandort**: Die Stadt, in der ein Benutzer zuletzt erkannt wurde. Citrix Analytics for Security ruft diese Daten von Citrix Virtual Apps and Desktops und Citrix DaaS (früher Citrix Virtual Apps and Desktops Service) ab. Citrix Analytics for Security sendet diese Informationen alle 12 Stunden an Ihren SIEM-Service.
  - **Benutzer-Client-IP**: Die Client-IP-Adresse des Benutzergeräts. Citrix Analytics for Security ruft diese Daten von Citrix Virtual Apps and Desktops und Citrix DaaS (früher Citrix Virtual Apps and Desktops Service) ab und sendet diese Informationen alle 12 Stunden an Ihren SIEM-Dienst.

Wenn Sie die Einstellungen für Datenquellenereignisse nur anzeigen, aber nicht konfigurieren können, verfügen Sie nicht über die erforderlichen Administratorberechtigungen.
Weitere Informationen finden Sie unter Administratorrollen für Security Analytics verwalten.

Im folgenden Beispiel ist die Schaltfläche **Änderungen speichern** deaktiviert. Die Risk Insight-Ereignisse sind standardmäßig aktiviert.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Schemadetails der Risk Insights-Ereignisse

Im folgenden Abschnitt wird das Schema der verarbeiteten Daten beschrieben, die von Citrix Analytics for Security generiert werden.

> **Hinweis**
>
> Die in den folgenden Schemabeispielen gezeigten Feldwerte dienen nur zur Veranschaulichung. Die tatsächlichen Feldwerte variieren je nach Benutzerprofil, Benutzerereignissen und dem Risikoindikator.

In der folgenden Tabelle werden die Feldnamen beschrieben, die im Schema für alle Benutzerprofildaten, den Benutzerrisikowert und die Änderung der Risikobewertung üblich sind.

Feldname	Beschreibung
`entity_id`	Die mit der Entität verbundene Identität. In diesem Fall ist die Entität der Benutzer.
`entity_type`	Das Unternehmen in Gefahr. In diesem Fall ist die Entität der Benutzer.
`event_type`	Die Art der Daten, die an Ihren SIEM-Dienst gesendet werden. Zum Beispiel: Standort des Benutzers, die Datennutzung des Benutzers oder die Gerätezugriffsinformationen des Benutzers.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Feldname	Beschreibung
tenant_id	Die einzigartige Identität des Kunden.
timestamp	Datum und Uhrzeit der letzten Benutzeraktivität.
version	Die Schemaversion der verarbeiteten Daten. Die aktuelle Schemaversion ist 2.

Datenschema des Benutzerprofils

Benutzerstandortschema

```
{

  "tenant_id": "demo_tenant", "entity_id": "demo_user", "entity_type":
     "user", "timestamp": "2021-02-10T15:00:00Z", "event_type": "
     userProfileLocation", "country": "India", "city": "Bengaluru", "
     cnt": 4, "version": 2
   }


<!--NeedCopy-->
```

Feldbeschreibung für Benutzerstandort

Feldname	Beschreibung
event_type	Die Art der Daten, die an den SIEM-Dienst gesendet werden. In diesem Fall ist der Ereignistyp der Standort des Benutzers.
country	Das Land, aus dem sich der Benutzer angemeldet hat.
city	Die Stadt, von der aus sich der Benutzer angemeldet hat.
cnt	Die Häufigkeit, wie oft auf den Standort in den letzten 12 Stunden zugegriffen wurde.

Benutzer-Client-IP-Schema

```
{

  "client_ip": "149.147.136.10",
  "cnt": 3,
  "entity_id": "r2_up_user_1",
  "entity_type": "user",
  "event_type": "userProfileClientIps",
  "tenant_id": "xaxddaily1",
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
  "timestamp": "2023-09-18T10:45:00Z",
  "version": 2
 }



<!--NeedCopy-->
```

Feldbeschreibung für Client-IP

Feldname	Beschreibung
client_ip	Die IP-Adresse des Benutzergeräts.
cnt	Die Häufigkeit, mit der der Benutzer in den letzten 12 Stunden auf das Gerät zugegriffen hat.
entity_id	Die mit der Entität verbundene Identität. In diesem Fall ist die Entität der Benutzer.
entity_type	Das Unternehmen in Gefahr. In diesem Fall ist der Ereignistyp die Client-IP des Benutzers.
event_type	Die Art der Daten, die an Ihren SIEM-Dienst gesendet werden. Zum Beispiel: der Standort des Benutzers, die Datennutzung des Benutzers oder die Gerätezugriffsinformationen des Benutzers.
tenant_id	Die einzigartige Identität des Kunden.
timestamp	Datum und Uhrzeit der letzten Benutzeraktivität..
version	Die Schemaversion der verarbeiteten Daten. Die aktuelle Schemaversion ist 2.

Nutzungsschema für Benutzerdaten

```
{

  "data_usage_bytes": 87555255, "deleted_file_cnt": 0, "
     downloaded_bytes": 87555255, "downloaded_file_cnt": 5, "entity_id"
     : "demo@demo.com", "entity_type": "user", "event_type": "
     userProfileUsage", "shared_file_cnt": 0, "tenant_id": "demo_tenant
     ", "timestamp": "2021-02-10T21:00:00Z", "uploaded_bytes": 0, "
     uploaded_file_cnt": 0, "version": 2
   }


<!--NeedCopy-->
```

Feldbeschreibung zur Verwendung von Benutzerdaten

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Feldname	Beschreibung
data_usage_bytes	Die vom Benutzer verwendete Datenmenge (in Byte). Es ist das Aggregat des heruntergeladenen und hochgeladenen Volumes für einen Benutzer.
deleted_file_cnt	Die Anzahl der vom Benutzer gelöschten Dateien.
downloaded_bytes	Die vom Benutzer heruntergeladene Datenmenge.
downloaded_file_count	Die Anzahl der vom Benutzer heruntergeladenen Dateien.
event_type	Die Art der Daten, die an den SIEM-Dienst gesendet werden. In diesem Fall ist der Ereignistyp das Nutzungsprofil des Benutzers.
shared_file_count	Die Anzahl der vom Benutzer freigegebenen Dateien.
uploaded_bytes	Die vom Benutzer hochgeladene Datenmenge.
uploaded_file_cnt	Die Anzahl der vom Benutzer hochgeladenen Dateien.

Schema des Benutzergeräts

```
{

  "cnt": 2, "device": "user1612978536 (Windows)", "entity_id": "demo",
     "entity_type": "user", "event_type": "userProfileDevice", "
     tenant_id": "demo_tenant", "timestamp": "2021-02-10T21:00:00Z", "
     version": 2
   }


<!--NeedCopy-->
```

Feldbeschreibung für Benutzergerät.

Feldname	Beschreibung
cnt	Die Häufigkeit, wie oft auf das Gerät in den letzten 12 Stunden zugegriffen wird.
device	Der Name des Geräts.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Feldname	Beschreibung
event_type	Die Art der Daten, die an den SIEM-Dienst gesendet werden. In diesem Fall sind der Ereignistyp die Gerätezugriffsinformationen des Benutzers.

Benutzer-App-Schema

```
{

  "tenant_id": "demo_tenant", "entity_id": "demo", "entity_type": "user
     ", "timestamp": "2021-02-10T21:00:00Z", "event_type": "
     userProfileApp", "version": 2, "session_domain": "99
     e38d488136f62f828d4823edd120b4f32d724396a7410e6dd1b0", "
     user_samaccountname": "testnameeikragz779", "app": "
     Chromeeikragz779", "cnt": 189
   }


<!--NeedCopy-->
```

Feldbeschreibung für Benutzer-App.

Feldname	Beschreibung
event_type	Die Art der Daten, die an den SIEM-Dienst gesendet werden. In diesem Fall sind der Ereignistyp die Gerätezugriffsinformationen des Benutzers.
session_domain	Die ID der Sitzung, an der sich der Benutzer angemeldet hat.
user_samaccountname	Der Anmeldename für Clients und Server einer früheren Version von Windows wie Windows NT 4.0, Windows 95, Windows 98 und LAN Manager. Dieser Name wird verwendet, um sich bei Citrix StoreFront anzumelden und sich auch bei einem Remote-Windows-Computer anzumelden.
app	Der Name der Anwendung, auf die der Benutzer zugegriffen hat.
cnt	Die Häufigkeit, wie oft auf die Anwendung in den letzten 12 Stunden zugegriffen wird.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Schema der Benutzerrisikobewertung

```
{

  "cur_riskscore": 7, "entity_id": "demo", "entity_type": "user", "
     event_type": "userProfileRiskscore", "last_update_timestamp": "
     2021-01-21T16:14:29Z", "tenant_id": "demo_tenant", "timestamp": "
     2021-02-10T20:45:00Z", "version": 2
   }


<!--NeedCopy-->
```

Feldbeschreibung für Benutzerrisiko-Score.

Feldname	Beschreibung
cur_riskscore	Der aktuelle Risikowert, der dem Benutzer zugewiesen wurde. Die Risikobewertung variiert je nach Bedrohungsschweregrad, der mit der Aktivität des Benutzers verbunden ist, zwischen 0 und 100.
event_type	Die Art der Daten, die an den SIEM-Dienst gesendet werden. In diesem Fall ist der Ereignistyp die Risikobewertung des Benutzers.
last_update_timestamp	Der Zeitpunkt, zu dem die Risikobewertung zuletzt für einen Benutzer aktualisiert wurde.
timestamp	Der Zeitpunkt, zu dem das Benutzerrisiko-Score-Ereignis erfasst und an Ihren SIEM-Dienst gesendet wird. Dieses Ereignis wird alle 12 Stunden an Ihren SIEM-Service gesendet.

Schema der Risikobewertung ändern

Beispiel 1:

```
{

  "alert_message": "Large risk score drop percent since last check", "
     alert_type": "riskscore_large_drop_pct", "alert_value": -21.73913,
      "cur_riskscore": 18, "entity_id": "demo_user", "entity_type": "
     user", "event_type": "riskScoreChange", "tenant_id": "demo_tenant"
     , "timestamp": "2021-02-11T05:45:00Z", "version": 2
   }
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
5
6
7 <!--NeedCopy-->
```

Beispiel 2:

```
1 {
2
3   "alert_message": "Risk score increase since last check", "alert_type"
       : "riskscore_increase", "alert_value": 39.0, "cur_riskscore": 76,
       "entity_id": "demo_user", "entity_type": "user", "event_type": "
       riskScoreChange", "tenant_id": "demo_tenant", "timestamp": "
       2021-02-11T03:45:00Z", "version": 2
4    }
5
6
7 <!--NeedCopy-->
```

Feldbeschreibung für die Änderung des Risiko-Scores.

Feldname	Beschreibung
alert_message	Die Meldung, die für die Änderung des Risiko-Scores angezeigt wird.
alert_type	Gibt an, ob die Warnung auf eine Erhöhung der Risikobewertung oder einen signifikanten Rückgang des Risiko-Score-Prozentsatzes dient. Wenn die Änderung der Risikobewertung eines Benutzers gleich oder mehr als drei ist und diese Änderung zunimmt oder um mehr als 10% sinkt, werden die Daten an den SIEM-Dienst gesendet.
alert_value	Ein numerischer Wert, der für die Änderung des Risiko-Score zugewiesen wurde. Die Änderung der Risikobewertung ist die Differenz zwischen dem aktuellen Risiko-Score und dem vorherigen Risiko-Score für einen Benutzer. Der Alarmwert variiert zwischen -100 und 100.
cur_riskscore	Der aktuelle Risikowert, der dem Benutzer zugewiesen wurde. Die Risikobewertung variiert je nach Bedrohungsschweregrad, der mit der Aktivität des Benutzers verbunden ist, zwischen 0 und 100.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Feldname	Beschreibung
`event_type`	Die Art der Daten, die an den SIEM-Dienst gesendet werden. In diesem Fall ist der Ereignistyp die Änderung des Risiko-Score des Benutzers.
`timestamp`	Das Datum und die Uhrzeit, zu der die letzte Änderung des Risiko-Score für den Benutzer erkannt wird.

Risikoindikator-Schema

Das Risikoindikatorschema besteht aus zwei Teilen: dem Schema für die Zusammenfassung der Indikatoren und dem Schema für die Details der Indikatorereignisse. Basierend auf dem Risikoindikator ändern sich die Felder und ihre Werte im Schema entsprechend.

In der folgenden Tabelle werden die Feldnamen beschrieben, die für alle Indikatorzusammenfassungsschemas häufig sind.

Feldname	Beschreibung
`data source`	Die Produkte, die Daten an Citrix Analytics for Security senden. Zum Beispiel: Citrix Secure Private Access, NetScaler Gateway und Citrix Apps and Desktops.
`data_source_id`	Die mit einer Datenquelle verknüpfte ID. ID 1 = Citrix Gateway, ID 2 = Citrix Endpoint Management, ID 3 = Citrix Apps und Desktops, ID 4 = Citrix Secure Private Access
`entity_type`	Das Unternehmen in Gefahr. Es kann ein Benutzer sein.
`entity_id`	Die ID, die mit dem gefährdeten Unternehmen verknüpft ist.
`event_type`	Die Art der Daten, die an den SIEM-Dienst gesendet werden. In diesem Fall ist der Ereignistyp die Zusammenfassung des Risikoindikators.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Feldname	Beschreibung
indicator_category	Gibt die Kategorien von Risikoindikatoren an. Die Risikoindikatoren sind in eine der Risikokategorien unterteilt - kompromittierter Endpunkt, kompromittierte Benutzer, Datenexfiltration oder Insiderbedrohungen.
indicator_id	Die mit dem Risikoindikator verknüpfte eindeutige ID.
indicator_category_id	Die ID, die mit einer Risikoindikatorkategorie verknüpft ist. ID 1 = Datenexfiltration, ID 2 = Insider-Bedrohungen, ID 3 = Kompromittierte Benutzer, ID 4 = Kompromittierter Endpunkt
indicator_name	Der Name des Risikoindikators. Für einen benutzerdefinierten Risikoindikator wird dieser Name beim Erstellen des Indikators definiert.
indicator_type	Gibt an, ob der Risikoindikator Standard (eingebaut) oder benutzerdefiniert ist.
indicator_uuid	Die eindeutige ID, die mit der Risikoindikatorinstanz verbunden ist.
indicator_vector_name	Gibt den Risikovektor an, der einem Risikoindikator zugeordnet ist. Die Risikovektoren sind gerätebasierte Risikoindikatoren, standortbasierte Risikoindikatoren, Anmeldeausfallbasierte Risikoindikatoren, IP-basierte Risikoindikatoren, datenbasierte Risikoindikatoren, dateibasierte Risikoindikatoren und andere Risikoindikatoren.
indicator_vector_id	Die mit einem Risikovektor verknüpfte ID. ID 1 = Gerätebasierte Risikoindikatoren, ID 2 = Standortbasierte Risikoindikatoren, ID 3 = Anmeldeausfall-basierte Risikoindikatoren, ID 4 = IP-basierte Risikoindikatoren, ID 5 = Datenbasierte Risikoindikatoren, ID 6 = Dateibasierte Risikoindikatoren, ID 7 = Andere Risikoindikatoren und ID 999 = Nicht verfügbar
occurrence_details	Die Details über den Risikoindikator auslösenden Zustand.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Feldname	Beschreibung
risk_probability	Gibt die Risikowahrscheinlichkeit an, die mit dem Benutzerereignis verbunden sind. Der Wert variiert zwischen 0 und 1,0. Für einen benutzerdefinierten Risikoindikator beträgt die risk_wahrscheinlichkeit immer 1,0, da es sich um einen richtlinienbasierten Indikator handelt.
severity	Gibt den Schweregrad des Risikos an. Es kann niedrig, mittel oder hoch sein.
tenant_id	Die einzigartige Identität des Kunden.
timestamp	Das Datum und die Uhrzeit, zu der der Risikoindikator ausgelöst wird.
ui_link	Der Link zur Benutzer-Timeline-Ansicht auf der Citrix Analytics-Benutzeroberfläche.
observation_start_time	Die Zeit, ab der Citrix Analytics beginnt, die Benutzeraktivität bis zum Zeitstempel zu überwachen. Wenn in diesem Zeitraum ein anomales Verhalten festgestellt wird, wird ein Risikoindikator ausgelöst.

In der folgenden Tabelle werden die Feldnamen beschrieben, die im gesamten Schema der Indikatorereignisse üblich sind.

Feldname	Beschreibung
data_source_id	Die mit einer Datenquelle verknüpfte ID. ID 1 = Citrix Gateway, ID 2 = Citrix Endpoint Management, ID 3 = Citrix Apps und Desktops, ID 4 = Citrix Secure Private Access
indicator_category_id	Die ID, die mit einer Risikoindikatorkategorie verknüpft ist. ID 1 = Datenexfiltration, ID 2 = Insider-Bedrohungen, ID 3 = Kompromittierte Benutzer, ID 4 = Kompromittierter Endpunkt
entity_id	Die ID, die mit dem gefährdeten Unternehmen verknüpft ist.
entity_type	Das Unternehmen, das gefährdet ist. Es kann ein Benutzer sein.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Feldname	Beschreibung
event_type	Die Art der Daten, die an den SIEM-Dienst gesendet werden. In diesem Fall ist der Ereignistyp die Details des Risikoindikatorereignisses.
indicator_id	Die mit dem Risikoindikator verknüpfte eindeutige ID.
indicator_uuid	Die eindeutige ID, die mit der Risikoindikatorinstanz verbunden ist.
indicator_vector_name	Gibt den Risikovektor an, der einem Risikoindikator zugeordnet ist. Die Risikovektoren sind gerätebasierte Risikoindikatoren, standortbasierte Risikoindikatoren, Anmeldeausfallbasierte Risikoindikatoren, IP-basierte Risikoindikatoren, datenbasierte Risikoindikatoren, dateibasierte Risikoindikatoren und andere Risikoindikatoren.
indicator_vector_id	Die mit einem Risikovektor verknüpfte ID. ID 1 = Gerätebasierte Risikoindikatoren, ID 2 = Standortbasierte Risikoindikatoren, ID 3 = Anmeldeausfall-basierte Risikoindikatoren, ID 4 = IP-basierte Risikoindikatoren, ID 5 = Datenbasierte Risikoindikatoren, ID 6 = Dateibasierte Risikoindikatoren, ID 7 = Andere Risikoindikatoren und ID 999 = Nicht verfügbar
tenant_id	Die einzigartige Identität des Kunden.
timestamp	Das Datum und die Uhrzeit, zu der der Risikoindikator ausgelöst wird.
version	Die Schemaversion der verarbeiteten Daten. Die aktuelle Schemaversion ist 2.
client_ip	Die IP-Adresse des Geräts des Benutzers.

> **Hinweis**
>
> - Wenn ein Feldwert für ganzzahlige Datentypen nicht verfügbar ist, ist der zugewiesene Wert -999. Zum Beispiel `"latitude": -999`, `"longitude": -999`.
> - Wenn ein Feldwert des Zeichenfolgendatentyps nicht verfügbar ist, ist der zugewiesene

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> Wert NA. Zum Beispiel `"city": "NA","region": "NA"`.

Citrix Secure Private Access-Risikoindikatorschema

Versuch, auf ein URL-Risikoindikatorschema auf der Sperrliste zuzugreifen

Zusammenfassungsschema des Indikators

```
{

  "tenant_id": "demo_tenant",
  "indicator_id": 401,
  "indicator_uuid": "8f2a39bd-c7c2-5555-a86a-5cfe5b64dfef",
  "indicator_category_id": 2,
  "indicator_vector": {

    "name": "Other Risk Indicators",
    "id": 7  }
 ,
  "data_source_id": 4,
  "timestamp": "2018-03-15T10:59:58Z",
  "event_type": "indicatorSummary",
  "entity_type": "user",
  "entity_id": "demo_user",
  "version": 2,
  "risk_probability": 1,
  "indicator_category": "Insider threats",
  "indicator_name": "Attempt to access blacklisted URL",
  "severity": "low",
  "data_source": "Citrix Secure Private Access",
  "ui_link": "https://analytics.cloud.com/user/",
  "indicator_type": "builtin",
  "occurrence_details": {

    "observation_start_time": "2018-03-15T10:44:59Z",
    "relevant_event_type": "Blacklisted External Resource Access"
   }

 }


<!--NeedCopy-->
```

Schema für die Ereignisdetails

```
{

  "tenant_id": "demo_tenant",
  "indicator_id": 401,
  "indicator_uuid": "c421f3f8-33d8-59b9-ad47-715b9d4f65f4",
  "indicator_category_id": 2,
  "indicator_vector": {
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
8
9       "name": "Other Risk Indicators",
10      "id": 7  }
11   ,
12    "data_source_id": 4,
13    "timestamp": "2018-03-15T10:57:21Z",
14    "event_type": "indicatorEventDetails",
15    "entity_type": "user",
16    "entity_id": "demo_user",
17    "version": 2,
18    "domain_name": "googleads.g.doubleclick.net",
19    "executed_action": "blocked",
20    "reason_for_action": "URL Category match",
21    "client_ip": "157.xx.xxx.xxx"
22   }
23
24
25  <!--NeedCopy-->
```

In der folgenden Tabelle werden die Feldnamen beschrieben, die für das Übersichtsschema und das Ereignisdetailschema für Versuch, auf die URL auf der Sperrliste zuzugreifen, spezifisch sind.

Feldname	Beschreibung
observation_start_time	Die Zeit, ab der Citrix Analytics beginnt, die Benutzeraktivität bis zum Zeitstempel zu überwachen. Wenn in diesem Zeitraum ein anomales Verhalten festgestellt wird, wird ein Risikoindikator ausgelöst.
executed_action	Die Aktion, die auf die URL auf der Sperrliste angewendet wurde. Die Aktion umfasst Zulassen und Blockieren.
reason_for_action	Der Grund für das Anwenden der Aktion für die URL.

Risikoindikatorschema für übermäßige Datendownloads

Zusammenfassungsschema des Indikators

```
1  {
2
3    "tenant_id": "demo_tenant",
4    "indicator_id": 403,
5    "indicator_uuid": "67d21b81-a89a-531e-af0b-c5688c2e9d40",
6    "indicator_category_id": 2,
7    "indicator_vector": {
8
9      "name": "Other Risk Indicators",
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
    "id": 7  }
 ,
  "data_source_id": 4,
  "timestamp": "2018-03-16T10:59:59Z",
  "event_type": "indicatorSummary",
  "entity_type": "user",
  "entity_id": "demo_user",
  "version": 2,
  "risk_probability": 1,
  "indicator_category": "Insider threats",
  "indicator_name": "Excessive data download",
  "severity": "low",
  "data_source": "Citrix Secure Private Access",
  "ui_link": "https://analytics.cloud.com/user/",
  "indicator_type": "builtin",
  "occurrence_details": {

    "observation_start_time": "2018-03-16T10:00:00Z",
    "data_volume_in_bytes": 24000,
    "relevant_event_type": "External Resource Access"
   }

 }


<!--NeedCopy-->
```

Schema für die Ereignisdetails

```
{

  "tenant_id": "demo_tenant",
  "indicator_id": 403,
  "indicator_uuid": "67d21b81-a89a-531e-af0b-c5688c2e9d40",
  "indicator_category_id": 2,
  "indicator_vector": {

    "name": "Other Risk Indicators",
    "id": 7  }
 ,
  "data_source_id": 4,
  "timestamp": "2018-03-16T10:30:00Z",
  "event_type": "indicatorEventDetails",
  "entity_type": "user",
  "entity_id": "demo_user",
  "version": 2,
  "domain_name": "www.facebook.com",
  "client_ip": "157.xx.xxx.xxx",
  "downloaded_bytes": 24000
 }


<!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

In der folgenden Tabelle werden die für das Zusammenfassungsschema spezifischen Feldnamen und das Ereignisdetailschema für übermäßige Datendownloads beschrieben.

Feldname	Beschreibung
observation_start_time	Die Zeit, ab der Citrix Analytics beginnt, die Benutzeraktivität bis zum Zeitstempel zu überwachen. Wenn in diesem Zeitraum ein anomales Verhalten festgestellt wird, wird ein Risikoindikator ausgelöst.
data_volume_in_bytes	Die Menge der Daten in Bytes, die heruntergeladen wird.
relevant_event_type	Gibt den Typ des Benutzerereignisses an.
domain_name	Der Name der Domäne, von der Daten heruntergeladen werden.
downloaded_bytes	Die Menge der Daten in Bytes, die heruntergeladen wird.

Ungewöhnliches Upload-Volumen-Risiko

Zusammenfassungsschema des Indikators

```
{

  "tenant_id": "demo_tenant",
  "indicator_id": 402,
  "indicator_uuid": "4f2a249c-9d05-5409-9c5f-f4c764f50e67",
  "indicator_category_id": 2,
  "indicator_vector": {

    "name": "Other Risk Indicators",
    "id": 7  }
 ,
  "data_source_id": 4,
  "timestamp": "2018-03-16T10:59:59Z",
  "event_type": "indicatorSummary",
  "entity_type": "user",
  "entity_id": "demo_user",
  "version": 2,
  "risk_probability": 1,
  "indicator_category": "Insider threats",
  "indicator_name": "Unusual upload volume",
  "severity": "low",
  "data_source": "Citrix Secure Private Access",
  "ui_link": "https://analytics.cloud.com/user/",
  "indicator_type": "builtin",
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
  "occurrence_details": {

    "observation_start_time": "2018-03-16T10:00:00Z",
    "data_volume_in_bytes": 24000,
    "relevant_event_type": "External Resource Access"
   }

 }


<!--NeedCopy-->
```

Schema für die Ereignisdetails

```
{

  "tenant_id": "demo_tenant",
  "indicator_id": 402,
  "indicator_uuid": "c6abf40c-9b62-5db4-84bc-5b2cd2c0ca5f",
  "indicator_category_id": 2,
  "indicator_vector": {

    "name": "Other Risk Indicators",
    "id": 7  }
 ,
  "data_source_id": 4,
  "timestamp": "2018-03-16T10:30:00Z",
  "event_type": "indicatorEventDetails",
  "entity_type": "user",
  "entity_id": "demo_user",
  "version": 2,
  "domain_name": "www.facebook.com",
  "client_ip": "157.xx.xxx.xxx",
  "uploaded_bytes": 24000
 }


<!--NeedCopy-->
```

In der folgenden Tabelle werden die für das Zusammenfassungsschema spezifischen Feldnamen und das Ereignisdetailschema für Ungewöhnliches Upload-Volume beschrieben.

Namen von Feldern	Beschreibung
`observation_start_time`	Die Zeit, ab der Citrix Analytics beginnt, die Benutzeraktivität bis zum Zeitstempel zu überwachen. Wenn in diesem Zeitraum ein anomales Verhalten festgestellt wird, wird ein Risikoindikator ausgelöst.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Namen von Feldern	Beschreibung
data_volume_in_bytes	Die Menge der Daten in Bytes, die hochgeladen wird.
relevant_event_type	Gibt den Typ des Benutzerereignisses an.
domain_name	Der Name der Domain, in die die Daten hochgeladen werden.
uploaded_bytes	Die Menge der Daten in Bytes, die hochgeladen wird.

Citrix Endpoint Management-Risikoindikatoren Schema

Jailbroken oder gerootetes Gerät erkannt Indikatoren Schema

Zusammenfassungsschema des Indikators

```
{

  "data_source": "Citrix Endpoint Management",
  "data_source_id": 2,
  "indicator_id": 200,
  "indicator_name": "Jailbroken / Rooted Device Detected",
  "entity_id": "demo_user",
  "entity_type": "user",
  "event_type": "indicatorSummary",
  "indicator_category": "Compromised endpoints",
  "indicator_category_id": 4,
  "indicator_vector": {

    "name": "Other Risk Indicators",
    "id": 7  }
 ,
  "indicator_type": "builtin",
  "indicator_uuid": "aa872f86-a991-4219-ad01-2a070b6e633d",
  "occurrence_details": {
  }
 ,
  "risk_probability": 1.0,
  "severity": "low",
  "tenant_id": "demo_tenant",
  "timestamp": "2021-04-13T17:49:05Z",
  "ui_link": "https://analytics.cloud.com/user/",
  "version": 2
 }


<!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Schema für die Ereignisdetails

```
{

  "indicator_id": 200,
  "client_ip": "122.xx.xx.xxx",
  "data_source_id": 2,
  "entity_id": "demo_user",
  "entity_type": "user",
  "event_type": "indicatorEventDetails",
  "indicator_category_id": 4,
  "indicator_vector": {

    "name": "Other Risk Indicators",
    "id": 7  }
 ,
  "indicator_uuid": "9aaaa9e1-39ad-4daf-ae8b-2fa2caa60732",
  "tenant_id": "demo_tenant",
  "timestamp": "2021-04-09T17:50:35Z",
  "version": 2
 }


<!--NeedCopy-->
```

Gerät mit Apps auf der Sperrliste erkannt

Zusammenfassungsschema des Indikators

```
{

  "data_source": "Citrix Endpoint Management",
  "data_source_id": 2,
  "indicator_id": 201,
  "indicator_name": "Device with Blacklisted Apps Detected",
  "entity_id": "demo_user",
  "entity_type": "user",
  "event_type": "indicatorSummary",
  "indicator_category": "Compromised endpoints",
  "indicator_category_id": 4,
  "indicator_vector": {

    "name": "Other Risk Indicators",
    "id": 7  }
 ,
  "indicator_type": "builtin",
  "indicator_uuid": "3ff7bd54-4319-46b6-8b98-58a9a50ae9a7",
  "occurrence_details": {
  }
 ,
  "risk_probability": 1.0,
  "severity": "low",
  "tenant_id": "demo_tenant",
  "timestamp": "2021-04-13T17:49:23Z",
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
  "ui_link": "https://analytics.cloud.com/user/",
  "version": 2
 }


<!--NeedCopy-->
```

Schema für die Ereignisdetails

```
{

  "indicator_id": 201,
  "client_ip": "122.xx.xx.xxx",
  "data_source_id": 2,
  "entity_id": "demo_user",
  "entity_type": "user",
  "event_type": "indicatorEventDetails",
  "indicator_category_id": 4,
  "indicator_vector": {

    "name": "Other Risk Indicators",
    "id": 7  }
 ,
  "indicator_uuid": "743cd13a-2596-4323-8da9-1ac279232894",
  "tenant_id": "demo_tenant",
  "timestamp": "2021-04-09T17:50:39Z",
  "version": 2
 }


<!--NeedCopy-->
```

Nicht verwaltetes Gerät erkannt

Zusammenfassungsschema des Indikators

```
{

  "data_source": "Citrix Endpoint Management",
  "data_source_id": 2,
  "indicator_id": 203,
  "indicator_name": "Unmanaged Device Detected",
  "entity_id": "demo_user",
  "entity_type": "user",
  "event_type": "indicatorSummary",
  "indicator_category": "Compromised endpoints",
  "indicator_category_id": 4,
  "indicator_vector": {

    "name": "Other Risk Indicators",
    "id": 7  }
 ,
  "indicator_type": "builtin",
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
  "indicator_uuid": "e28b8186-496b-44ff-9ddc-ae50e87bd757",
  "occurrence_details": {
  }
 ,
  "risk_probability": 1.0,
  "severity": "low",
  "tenant_id": "demo_tenant",
  "timestamp": "2021-04-13T12:56:30Z",
  "ui_link": "https://analytics.cloud.com/user/",
  "version": 2
 }


<!--NeedCopy-->
```

Schema für die Ereignisdetails

```
{

  "indicator_id": 203,
  "client_ip": "127.xx.xx.xxx",
  "data_source_id": 2,
  "entity_id": "demo_user",
  "entity_type": "user",
  "event_type": "indicatorEventDetails",
  "indicator_category_id": 4,
  "indicator_vector": {

    "name": "Other Risk Indicators",
    "id": 7  }
 ,
  "indicator_uuid": "dd280122-04f2-42b4-b9fc-92a715c907a0",
  "tenant_id": "demo_tenant",
  "timestamp": "2021-04-09T18:41:30Z",
  "version": 2
 }


<!--NeedCopy-->
```

NetScaler Gateway-Risikoindikatoren

Risikoindikatorschema für EPA-Scanausfall

Zusammenfassungsschema des Indikators

```
{

  "tenant_id": "demo_tenant",
  "indicator_id": 100,
  "indicator_uuid": "3c17454c-86f5-588a-a4ac-0342693d8a70",
  "indicator_category_id": 3,
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
  "indicator_vector": {

    "name": "Other Risk Indicators",
    "id": 7  }
 ,
  "data_source_id": 1,
  "timestamp": "2017-12-21T07:14:59Z",
  "event_type": "indicatorSummary",
  "entity_type": "user",
  "entity_id": "demo_user",
  "version": 2,
  "risk_probability": 1,
  "indicator_category": "Compromised users",
  "indicator_name": "EPA scan failure",
  "severity": "low",
  "data_source": "Citrix Gateway",
  "ui_link": "https://analytics.cloud.com/user/",
  "indicator_type": "builtin",
  "occurrence_details": {

    "event_description": "Post auth failed, no quarantine",
    "observation_start_time": "2017-12-21T07:00:00Z",
    "relevant_event_type": "EPA Scan Failure at Logon"
   }

 }


<!--NeedCopy-->
```

Schema für die Ereignisdetails

```
{

  "tenant_id": "demo_tenant",
  "indicator_id": 100,
  "indicator_uuid": "3c17454c-86f5-588a-a4ac-0342693d8a70",
  "indicator_category_id": 3,
  "indicator_vector": {

    "name": "Other Risk Indicators",
    "id": 7  }
 ,
  "data_source_id": 1,
  "timestamp": "2017-12-21T07:12:00Z",
  "event_type": "indicatorEventDetails",
  "entity_type": "user",
  "entity_id": "demo_user",
  "version": 2,
  "event_description": "Post auth failed, no quarantine",
  "gateway_domain_name": "10.102.xx.xx",
  "gateway_ip": "56.xx.xxx.xx",
  "policy_name": "postauth_act_1",
  "client_ip": "210.91.xx.xxx",
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
  "country": "United States",
  "city": "San Jose",
  "region": "California",
  "cs_vserver_name": "demo_vserver",
  "device_os": "Windows OS",
  "security_expression": "CLIENT.OS(Win12) EXISTS",
  "vpn_vserver_name": "demo_vpn_vserver",
  "vserver_fqdn": "10.xxx.xx.xx"
 }

<!--NeedCopy-->
```

In der Tabelle werden die Feldnamen beschrieben, die für das Zusammenfassungsschema spezifisch sind, und das Ereignisdetailschema für den Risikoindikator für den EPA-Scanausfall.

Namen von Feldern	Beschreibung
event_description	Beschreibt die Gründe für den Fehler des EPA-Scans wie die fehlgeschlagene Postauthentifizierung und keine Quarantänegruppe.
relevant_event_type	Gibt den Typ des EPA-Scan-Fehlereignisses an.
gateway_domain_name	Der Domänenname von NetScaler Gateway.
gateway_ip	Die IP-Adresse von NetScaler Gateway.
policy_name	Der auf dem NetScaler Gateway konfigurierte EPA-Scanrichtlinienname.
country	Das Land, aus dem die Benutzeraktivität erkannt wurde.
city	Die Stadt, von der aus die Benutzeraktivität erkannt wurde.
region	Die Region, aus der die Benutzeraktivität erkannt wurde.
cs_vserver_name	Der Name des virtuellen Content-Switch-Servers.
device_os	Das Betriebssystem des Geräts des Benutzers.
security_expression	Der auf NetScaler Gateway konfigurierte Sicherheitsausdruck.
vpn_vserver_name	Der Name des virtuellen NetScaler Gateway-Servers.
vserver_fqdn	Der FQDN des virtuellen NetScaler Gateway-Servers.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Risikoindikatorschema für übermäßige Authentifizierung

Zusammenfassungsschema des Indikators

```
{

  "tenant_id": "demo_tenant",
  "indicator_id": 101,
  "indicator_uuid": "4bc0f759-93e0-5eea-9967-ed69de9dd09a",
  "indicator_category_id": 3,
  "indicator_vector": {

    "name": "Logon-Failure-Based Risk Indicators",
    "id": 3  }
 ,
  "data_source_id": 1,
  "timestamp": "2017-12-21T07:14:59Z",
  "event_type": "indicatorSummary",
  "entity_type": "user",
  "entity_id": "demo_user",
  "version": 2,
  "risk_probability": 1,
  "indicator_category": "Compromised users",
  "indicator_name": "Excessive authentication failures",
  "severity": "medium",
  "data_source": "Citrix Gateway",
  "ui_link": "https://analytics.cloud.com/user/” ,
  "indicator_type": "builtin",
  "occurrence_details": {

    "observation_start_time": "2017-12-21T07:00:00Z",
    "relevant_event_type": "Logon Failure"
   }

 }

<!--NeedCopy-->
```

Schema für die Ereignisdetails

```
{

  "tenant_id": "demo_tenant",
  "indicator_id": 101,
  "indicator_uuid": "a391cd1a-d298-57c3-a17b-01f159b26b99",
  "indicator_category_id": 3,
  "indicator_vector": {

    "name": "Logon-Failure-Based Risk Indicators",
    "id": 3  }
 ,
  "data_source_id": 1,
  "timestamp": "2017-12-21T07:10:00Z",
  "event_type": "indicatorEventDetails",
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
  "entity_type": "user",
  "entity_id": "demo-user",
  "version": 2,
  "event_description": "Bad (format) password passed to nsaaad",
  "authentication_stage": "Secondary",
  "authentication_type": "LDAP",
  "auth_server_ip": "10.xxx.x.xx",
  "client_ip": "24.xxx.xxx.xx",
  "gateway_ip": "24.xxx.xxx.xx",
  "vserver_fqdn": "demo-fqdn.citrix.com",
  "vpn_vserver_name": "demo_vpn_vserver",
  "cs_vserver_name": "demo_cs_vserver",
  "gateway_domain_name": "xyz",
  "country": "United States",
  "region": "California",
  "city": "San Jose",
  "nth_failure": 5
 }


<!--NeedCopy-->
```

In der folgenden Tabelle werden die Feldnamen beschrieben, die für das Zusammenfassungsschema spezifisch sind, und das Ereignisdetailschema für einen übermäßigen Authentifizierungsfehler.

Namen von Feldern	Beschreibung
`relevant_event_type`	Gibt den Typ des Ereignisses an, z. B. ein Anmeldefehler.
`event_description`	Beschreibt den Grund für den übermäßigen Authentifizierungsfehler, z. B. ein falsches Kennwort.
`authentication_stage`	Gibt an, ob die Authentifizierungsphase primär, sekundär oder tertiär ist.
`authentication_type`	Gibt die Authentifizierungstypen wie LDAP, Local oder OAuth an.
`auth_server_ip`	Die IP-Adresse des Authentifizierungsservers.
`gateway_domain_name`	Der Domänenname von NetScaler Gateway.
`gateway_ip`	Die IP-Adresse von NetScaler Gateway.
`cs_vserver_name`	Der Name des virtuellen Content-Switch-Servers.
`vpn_vserver_name`	Der Name des virtuellen NetScaler Gateway-Servers.
`vserver_fqdn`	Der FQDN des virtuellen NetScaler Gateway-Servers.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Namen von Feldern	Beschreibung
nth_failure	Die Häufigkeit, mit der die Benutzerauthentifizierung fehlgeschlagen ist.
country	Das Land, aus dem die Benutzeraktivität erkannt wurde.
city	Die Stadt, von der aus die Benutzeraktivität erkannt wurde.
region	Die Region, aus der die Benutzeraktivität erkannt wurde.

Risikoindikator für unmögliche Reise

Zusammenfassungsschema des Indikators

```
{

  "tenant_id": "demo_tenant",
  "indicator_id": "111",
  "indicator_uuid": "83d68a6d-6588-5b77-9118-8a9e6a5b462b",
  "indicator_category_id": 3,
  "indicator_vector": {

    "name": "Location-Based Risk Indicators",
    "id": 2
   }
 ,
  "data_source_id": 1,
  "timestamp": "2020-06-06T12:14:59Z",
  "event_type": "indicatorSummary",
  "entity_type": "user",
  "entity_id": "demo_user",
  "version": 2,
  "risk_probability": 1,
  "indicator_category": "Compromised users",
  "indicator_name": "Impossible travel",
  "severity": "medium",
  "data_source": "Citrix Gateway",
  "ui_link": "https://analytics.cloud.com/user/",
  "indicator_type": "builtin",
  "occurrence_details": {

    "relevant_event_type": "Impossible travel",
    "distance": 7480.44718,
    "observation_start_time": "2020-06-06T12:00:00Z",
    "historical_logon_locations": "[{
"country":"United States","region":"Florida","city":"Miami","latitude"
   :25.7617,"longitude":-80.191,"count":28 }
 ,{
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
 "country":"United States","latitude":37.0902,"longitude":-95.7129,"
    count":2 }
 ]",
    "historical_observation_period_in_days": 30
   }

 }


<!--NeedCopy-->
```

Schema für die Ereignisdetails

```
{

  "tenant_id": "demo_tenant",
  "indicator_id": "111",
  "indicator_uuid": "83d68a6d-6588-5b77-9118-8a9e6a5b462b",
  "pair_id": 2,
  "indicator_category_id": 3,
  "indicator_vector": {

    "name": "Location-Based Risk Indicators",
    "id": 2
   }
 ,
  "data_source_id": 1,
  "timestamp": "2020-06-06T05:05:00Z",
  "event_type": "indicatorEventDetails",
  "entity_type": "user",
  "entity_id": "demo_user",
  "version": 2,
  "client_ip": "95.xxx.xx.xx",
  "ip_organization": "global telecom ltd",
  "ip_routing_type": "mobile gateway",
  "country": "Norway",
  "region": "Oslo",
  "city": "Oslo",
  "latitude": 59.9139,
  "longitude": 10.7522,
  "device_os": "Linux OS",
  "device_browser": "Chrome 62.0.3202.94"
 }


<!--NeedCopy-->
```

In der folgenden Tabelle werden die Feldnamen für das Zusammenfassungsschema und das Ereignisdetailschema für Unmögliche Reisen beschrieben.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Feldname	Beschreibung
distance	Die Entfernung (km) zwischen den Ereignissen, die mit unmöglichem Reisen verbunden sind.
historical_logon_locations	Die Standorte, auf die der Benutzer zugegriffen hat, und wie oft während des Beobachtungszeitraums auf jeden Standort zugegriffen wurde.
historical_observation_period_in_days	Jeder Standort wird 30 Tage lang überwacht.
relevant_event_type	Gibt den Typ des Ereignisses wie Anmeldung an.
observation_start_time	Die Zeit, ab der Citrix Analytics beginnt, die Benutzeraktivität bis zum Zeitstempel zu überwachen. Wenn in diesem Zeitraum ein anomales Verhalten festgestellt wird, wird ein Risikoindikator ausgelöst.
country	Das Land, aus dem sich der Benutzer angemeldet hat.
city	Die Stadt, von der sich der Benutzer angemeldet hat.
region	Gibt die Region an, aus der sich der Benutzer angemeldet hat.
latitude	Gibt den Breitengrad des Standorts an, von dem sich der Benutzer angemeldet hat.
longitude	Gibt den Längengrad des Ortes an, von dem sich der Benutzer angemeldet hat.
device_browser	Der vom Benutzer verwendete Webbrowser.
device_os	Das Betriebssystem des Geräts des Benutzers.
ip_organization	Registrierung der Organisation der Client-IP-Adresse
ip_routing_type	Client-IP-Routingtyp

Anmeldung von einem verdächtigen IP-Risikoindikator-Schema

Zusammenfassungsschema des Indikators

```
{

  "tenant_id": "demo_tenant",
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
  "indicator_id": 102,
  "indicator_uuid": "0100e910-561a-5ff3-b2a8-fc556d199ba5",
  "indicator_category_id": 3,
  "indicator_vector": {

    "name": "IP-Based Risk Indicators",
    "id": 4  }
 ,
  "data_source_id": 1,
  "timestamp": "2019-10-10T10:14:59Z",
  "event_type": "indicatorSummary",
  "entity_type": "user",
  "entity_id": "demo_user",
  "version": 2,
  "risk_probability": 0.91,
  "indicator_category": "Compromised users",
  "indicator_name": "Logon from suspicious IP",
  "severity": "medium",
  "data_source": "Citrix Gateway",
  "ui_link": "https://analytics.cloud.com/user/",
  "indicator_type": "builtin",
  "occurrence_details": {

    "relevant_event_type": "Logon",
    "client_ip": "1.0.xxx.xx",
    "observation_start_time": "2019-10-10T10:00:00Z",
    "suspicion_reasons": "brute_force|external_threat"
   }

 }

<!--NeedCopy-->
```

Schema für die Ereignisdetails

```
{

  "tenant_id": "demo_tenant",
  "indicator_id": 102,
  "indicator_uuid": "4ba77b6c-bac0-5ad0-9b4a-c459a3e2ec33",
  "indicator_category_id": 3,
  "indicator_vector": {

    "name": "IP-Based Risk Indicators",
    "id": 4  }
 ,
  "data_source_id": 1,
  "timestamp": "2019-10-10T10:11:00Z",
  "event_type": "indicatorEventDetails",
  "entity_type": "user",
  "entity_id": "demo_user",
  "version": 2,
  "suspicion_reasons": "external_threat",
  "gateway_ip": "gIP1",
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
  "client_ip": "128.0.xxx.xxx",
  "country": "Sweden",
  "city": "Stockholm",
  "region": "Stockholm",
  "webroot_reputation": 14,
  "webroot_threat_categories": "Windows Exploits|Botnets|Proxy",
  "device_os": "Windows OS",
  "device_browser": "Chrome"
 }


<!--NeedCopy-->
```

In der folgenden Tabelle werden die Feldnamen beschrieben, die für das Übersichtsschema und das Ereignisdetailschema für die Anmeldung von einer verdächtigen IP-Adresse spezifisch sind.

Feldname	Beschreibung
suspicious_reasons	Der Grund für die Identifizierung der IP-Adresse als verdächtig.
webroot_reputation	Der IP-Reputationsindex, der vom Threat Intelligence Provider Webroot bereitgestellt wird.
webroot_threat_categories	Die Bedrohungskategorie, die vom Threat Intelligence Provider Webroot für die verdächtige IP identifiziert wurde.
device_os	Das Betriebssystem des Benutzergeräts.
device_browser	Der verwendete Webbrowser.
country	Das Land, aus dem die Benutzeraktivität erkannt wurde.
city	Die Stadt, von der aus die Benutzeraktivität erkannt wurde.
region	Die Region, aus der die Benutzeraktivität erkannt wurde.

Ungewöhnliches Risikoindikator-Schema für

Zusammenfassungsschema des Indikators

```
{

  "tenant_id": "demo_tenant",
  "indicator_id": 109,
  "indicator_uuid": "dc0174c9-247a-5e48-a2ab-d5f92cd83d0f",
  "indicator_category_id": 3,
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
  "indicator_vector": {

    "name": "Logon-Failure-Based Risk Indicators",
    "id": 3  }
 ,
  "data_source_id": 1,
  "timestamp": "2020-04-01T06:44:59Z",
  "event_type": "indicatorSummary",
  "entity_type": "user",
  "entity_id": "demo_user",
  "version": 2,
  "risk_probability": 1,
  "indicator_category": "Compromised users",
  "indicator_name": "Unusual authentication failure",
  "severity": "medium",
  "data_source": "Citrix Gateway",
  "ui_link": "https://analytics.cloud.com/user/",
  "indicator_type": "builtin",
  "occurrence_details": {

    "relevant_event_type": "Logon Failure",
    "observation_start_time": "2020-04-01T05:45:00Z"
   }

 }


<!--NeedCopy-->
```

Schema für die Ereignisdetails

```
{

  "tenant_id": "demo_tenant",
  "indicator_id": 109,
  "indicator_uuid": "ef4b9830-39d6-5b41-bdf3-84873a77ea9a",
  "indicator_category_id": 3,
  "indicator_vector": {

    "name": "Logon-Failure-Based Risk Indicators",
    "id": 3  }
 ,
  "data_source_id": 1,
  "timestamp": "2020-04-01T06:42:00Z",
  "event_type": "indicatorEventDetails",
  "entity_type": "user",
  "entity_id": "demo_user",
  "version": 2,
  "event_description": "Success",
  "authentication_stage": "Secondary",
  "authentication_type": "LDAP",
  "client_ip": "99.xxx.xx.xx",
  "country": "United States",
  "city": "San Jose",
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
24    "region": "California",
25    "device_os": "Windows OS ",
26    "device_browser": "Chrome",
27    "is_risky": "false"
28   }
29
30
31  <!--NeedCopy-->
```

In der folgenden Tabelle werden die für das Zusammenfassungsschema spezifischen Feldnamen und das Ereignisdetailschema für einen ungewöhnlichen Authentifizierungsfehler beschrieben.

Namen von Feldern	Beschreibung
relevant_event_type	Gibt den Typ des Ereignisses an, z. B. ein Anmeldefehler.
event_description	Zeigt an, ob die Anmeldung erfolgreich oder erfolglos ist
authentication_stage	Gibt an, ob die Authentifizierungsphase primär, sekundär oder tertiär ist.
authentication_type	Gibt die Authentifizierungstypen wie LDAP, Local oder OAuth an.
is_risky	Für eine erfolgreiche Anmeldung ist der Wert is_risky false. Für eine erfolglose Anmeldung ist der Wert is_risky true.
device_os	Das Betriebssystem des Benutzergeräts.
device_browser	Der vom Benutzer verwendete Webbrowser.
country	Das Land, aus dem die Benutzeraktivität erkannt wurde.
city	Die Stadt, von der aus die Benutzeraktivität erkannt wurde.
region	Die Region, aus der die Benutzeraktivität erkannt wurde.

Risikoanzeige für verdächtige Anmeldung

Zusammenfassungsschema des Indikators

```
1  {
2
3    "tenant_id": "demo_tenant",
4    "indicator_id": "110",
5    "indicator_uuid": "67fd935-a6a3-5397-b596-636aa1588c",
6    "indicator_category_id": 3,
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
  "indicator_vector": [
    {

      "name": "Location-Based Risk Indicators",
      "id": 2
     }
,
    {

      "name": "IP-Based Risk Indicators",
      "id": 4
     }
,
    {

      "name": "Other Risk Indicators",
      "id": 7
     }

 ],
 "data_source_id": 1,
 "timestamp": "2020-06-06T12:14:59Z",
 "event_type": "indicatorSummary",
 "entity_type": "user",
 "entity_id": "demo_user",
 "version": 2,
 "risk_probability": 0.71,
 "indicator_category": "Compromised users",
 "indicator_name": "Suspicious logon",
 "severity": "medium",
 "data_source": "Citrix Gateway",
 "ui_link": "https://analytics.cloud.com/user/",
 "indicator_type": "builtin",
 "occurrence_details": {

   "observation_start_time": "2020-06-06T12:00:00Z",
   "relevant_event_type": "Logon",
   "event_count": 1,
   "historical_observation_period_in_days": 30,
   "country": "United States",
   "region": "Florida",
   "city": "Miami",
   "historical_logon_locations": "[{
"country":"United States","region":"New York","city":"New York City","
    latitude":40.7128,"longitude":-74.0060,"count":9 }
]",
   "user_location_risk": 75,
   "device_id": "",
   "device_os": "Windows OS",
   "device_browser": "Chrome",
   "user_device_risk": 0,
   "client_ip": "99.xxx.xx.xx",
   "user_network_risk": 75,
```


© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
    "webroot_threat_categories": "Phishing",
    "suspicious_network_risk": 89
   }

 }


<!--NeedCopy-->
```

Schema für die Ereignisdetails

```
{

  "tenant_id": "demo_tenant",
  "indicator_id": "110",
  "indicator_uuid": "67fd6935-a6a3-5397-b596-63856aa1588c",
  "indicator_category_id": 3,
  "indicator_vector": [
    {

      "name": "Location-Based Risk Indicators",
      "id": 2
     }
 ,
    {

      "name": "IP-Based Risk Indicators",
      "id": 4
     }
 ,
    {

      "name": "Other Risk Indicators",
      "id": 7
     }

  ],
  "data_source_id": 1,
  "timestamp": "2020-06-06T12:08:40Z",
  "event_type": "indicatorEventDetails",
  "entity_type": "user",
  "entity_id": "demo_user",
  "version": 2,
  "country": "United States",
  "region": "Florida",
  "city": "Miami",
  "latitude": 25.7617,
  "longitude": -80.1918,
  "device_browser": "Chrome",
  "device_os": "Windows OS",
  "device_id": "NA",
  "client_ip": "99.xxx.xx.xx"
 }
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
43
44
45 <!--NeedCopy-->
```

In der folgenden Tabelle werden die für das Zusammenfassungsschema spezifischen Feldnamen und das Ereignisdetail-Schema für verdächtige Anmeldung beschrieben.

Feldname	Beschreibung
historical_logon_locations	Die Standorte, auf die der Benutzer zugegriffen hat, und wie oft während des Beobachtungszeitraums auf jeden Standort zugegriffen wurde.
historical_observation_period_in_days	Jeder Standort wird 30 Tage lang überwacht.
relevant_event_type	Gibt den Typ des Ereignisses wie Anmeldung an.
observation_start_time	Die Zeit, ab der Citrix Analytics beginnt, die Benutzeraktivität bis zum Zeitstempel zu überwachen. Wenn in diesem Zeitraum ein anomales Verhalten festgestellt wird, wird ein Risikoindikator ausgelöst.
occurrence_event_type	Gibt den Benutzerereignistyp wie die Kontoanmeldung an.
country	Das Land, aus dem sich der Benutzer angemeldet hat.
city	Die Stadt, von der sich der Benutzer angemeldet hat.
region	Gibt die Region an, aus der sich der Benutzer angemeldet hat.
latitude	Gibt den Breitengrad des Standorts an, von dem sich der Benutzer angemeldet hat.
longitude	Gibt den Längengrad des Ortes an, von dem sich der Benutzer angemeldet hat.
device_browser	Der vom Benutzer verwendete Webbrowser.
device_os	Das Betriebssystem des Geräts des Benutzers.
device_id	Der Name des vom Benutzer verwendeten Geräts.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Feldname	Beschreibung
user_location_risk	Zeigt die Verdachtsstufe des Standorts an, von dem aus sich der Benutzer angemeldet hat. Niedriger Verdacht: 0—69, mittlerer Verdacht: 70—89 und Hoher Verdacht: 90—100
user_device_risk	Zeigt die Verdachtsstufe des Geräts an, von dem aus sich der Benutzer angemeldet hat. Niedriger Verdacht: 0—69, mittlerer Verdacht: 70—89 und Hoher Verdacht: 90—100
user_network_risk	Zeigt die Verdachtsstufe des Netzwerks oder des Subnetzes an, von dem aus sich der Benutzer angemeldet hat. Niedriger Verdacht: 0—69, mittlerer Verdacht: 70—89 und Hoher Verdacht: 90—100
suspicious_network_risk	Gibt die IP-Bedrohungsstufe basierend auf dem Webroot IP-Bedrohungs-Intelligence-Feed an. Niedrige Bedrohungsstufe: 0—69, mittlere Bedrohungsstufe: 70—89 und hohe Bedrohungsstufe: 90—100
webroot_threat_categories	Gibt die Arten von Bedrohungen an, die von der IP-Adresse basierend auf dem Webroot IP-Bedrohungsinfo-Feed erkannt wurden. Die Bedrohungskategorien können Spam-Quellen, Windows-Exploits, Webangriffe, Botnetze, Scanner, Denial of Service, Reputation, Phishing, Proxy, nicht spezifiziert, mobile Bedrohungen und Tor-Proxy sein

Schema der Risikoindikatoren für Citrix DaaS und Citrix Virtual Apps and Desktops

Risikoindikator für unmögliche Reise

Zusammenfassungsschema des Indikators

```
{

  "tenant_id": "demo_tenant",
  "indicator_id": "313",
  "indicator_uuid": "c78d1dd4-5e70-5642-ba6f-1cdf31bc6ab2",
  "indicator_category_id": 3,
  "indicator_vector": {
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
 8
 9      "name": "Location-Based Risk Indicators",
10      "id": 2
11     }
12   ,
13    "data_source_id": 3,
14    "timestamp": "2020-06-06T12:14:59Z",
15    "event_type": "indicatorSummary",
16    "entity_type": "user",
17    "entity_id": "demo_user",
18    "version": 2,
19    "risk_probability": 1,
20    "indicator_category": "Compromised users",
21    "indicator_name": "Impossible travel",
22    "severity": "medium",
23    "data_source": "Apps and Desktops",
24    "ui_link": "https://analytics.cloud.com/user/",
25    "indicator_type": "builtin",
26    "occurrence_details": {
27
28      "relevant_event_type": "Impossible travel",
29      "distance": 7480.44718,
30      "observation_start_time": "2020-06-06T12:00:00Z",
31      "historical_logon_locations": "[{
32   "country":"United States","region":"Florida","city":"Miami","latitude"
        :25.7617,"longitude":-80.191,"count":28 }
33   ,{
34   "country":"United States","latitude":37.0902,"longitude":-95.7129,"
        count":2 }
35   ]",
36      "historical_observation_period_in_days": 30
37     }
38
39   }
40
41
42 <!--NeedCopy-->
```

Schema für die Ereignisdetails

```
1  {
2
3    "tenant_id": "demo_tenant",
4    "indicator_id": "313",
5    "indicator_uuid": "c78d1dd4-5e70-5642-ba6f-1cdf31bc6ab2",
6    "pair_id": 2,
7    "indicator_category_id": 3,
8    "indicator_vector": {
9
10     "name": "Location-Based Risk Indicators",
11     "id": 2
12    }
13   ,
14    "data_source_id": 3,
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
15    "timestamp": "2020-06-06T05:05:00Z",
16    "event_type": "indicatorEventDetails",
17    "entity_type": "user",
18    "entity_id": "demo_user",
19    "version": 2,
20    "occurrence_event_type": "Account.Logon",
21    "client_ip": "95.xxx.xx.xx",
22     “ ip_organization ” :  “ global telecom ltd ” ,
23     “ ip_routing_type ” :  “ mobile gateway ” ,
24    "country": "Norway",
25    "region": "Oslo",
26    "city": "Oslo",
27    "latitude": 59.9139,
28    "longitude": 10.7522,
29    "device_id": "device1",
30    "receiver_type": "XA.Receiver.Linux",
31    "os": "Linux OS",
32    "browser": "Chrome 62.0.3202.94"
33   }
34
35
36  <!--NeedCopy-->
```

In der folgenden Tabelle werden die Feldnamen für das Zusammenfassungsschema und das Ereignisdetailschema für Unmögliche Reisen beschrieben.

Feldname	Beschreibung
distance	Die Entfernung (km) zwischen den Ereignissen, die mit unmöglichem Reisen verbunden sind.
historical_logon_locations	Die Standorte, auf die der Benutzer zugegriffen hat, und wie oft während des Beobachtungszeitraums auf jeden Standort zugegriffen wurde.
historical_observation_period_in_days	Jeder Standort wird 30 Tage lang überwacht.
relevant_event_type	Gibt den Typ des Ereignisses wie Anmeldung an.
observation_start_time	Die Zeit, ab der Citrix Analytics beginnt, die Benutzeraktivität bis zum Zeitstempel zu überwachen. Wenn in diesem Zeitraum ein anomales Verhalten festgestellt wird, wird ein Risikoindikator ausgelöst.
country	Das Land, aus dem sich der Benutzer angemeldet hat.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Feldname	Beschreibung
city	Die Stadt, von der sich der Benutzer angemeldet hat.
region	Gibt die Region an, aus der sich der Benutzer angemeldet hat.
latitude	Gibt den Breitengrad des Standorts an, von dem sich der Benutzer angemeldet hat.
longitude	Gibt den Längengrad des Ortes an, von dem sich der Benutzer angemeldet hat.
browser	Der vom Benutzer verwendete Webbrowser.
os	Das Betriebssystem des Geräts des Benutzers.
device_id	Der Name des vom Benutzer verwendeten Geräts.
receiver_type	Der Typ der Citrix Workspace-App oder Citrix Receiver, die auf dem Gerät des Benutzers installiert ist.
ip_organization	Registrierung der Organisation der Client-IP-Adresse
ip_routing_type	Client-IP-Routingtyp

Indikator für potenzielle Datenexfiltrationsrisiken

Zusammenfassungsschema des Indikators


```
{

  "tenant_id": "demo_tenant",
  "indicator_id": 303,
  "indicator_uuid": "fb649ff7-5b09-5f48-8a04-12836b9eed85",
  "indicator_category_id": 1,
  "indicator_vector": {

    "name": "Data-Based Risk Indicators",
    "id": 5  }
 ,
  "data_source_id": 3,
  "timestamp": "2018-04-02T10:59:59Z",
  "event_type": "indicatorSummary",
  "entity_type": "user",
  "entity_id": "demo_user",
  "version": 2,
  "risk_probability": 1,
  "indicator_category": "Data exfiltration",
```


© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
  "indicator_name": "Potential data exfiltration",
  "severity": "low",
  "data_source": "Citrix Apps and Desktops",
  "ui_link": "https://analytics.cloud.com/user/ ",
  "indicator_type": "builtin",
  "occurrence_details": {

    "relevant_event_type": "Download/Print/Copy",
    "observation_start_time": "2018-04-02T10:00:00Z",
    "exfil_data_volume_in_bytes": 1172000
   }

 }


<!--NeedCopy-->
```

Schema für die Ereignisdetails

```
{

  "tenant_id": "demo_tenant",
  "indicator_id": 303,
  "indicator_uuid": "fb649ff7-5b09-5f48-8a04-12836b9eed85",
  "indicator_category_id": 1,
  "indicator_vector": {

    "name": "Data-Based Risk Indicators",
    "id": 5  }
 ,
  "data_source_id": 3,
  "timestamp": "2018-04-02T10:57:36Z",
  "event_type": "indicatorEventDetails",
  "entity_type": "user",
  "entity_id": "demo_user",
  "version": 2,
  "occurrence_event_type": "App.SaaS.Clipboard",
  "file_size_in_bytes": 98000,
  "file_type": "text",
  "device_id": "dvc5",
  "receiver_type": "XA.Receiver.Windows",
  "app_url": "https://www.citrix.com",
  "client_ip": "10.xxx.xx.xxx",
  "entity_time_zone": "Pacific Standard Time"
 }


<!--NeedCopy-->
```

In der folgenden Tabelle werden die Felder beschrieben, die für das Zusammenfassungsschema und das Ereignisdetailschema für die potenzielle Datenexfiltration spezifisch sind.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Feldname	Beschreibung
observation_start_time	Die Zeit, ab der Citrix Analytics beginnt, die Benutzeraktivität bis zum Zeitstempel zu überwachen. Wenn in diesem Zeitraum ein anomales Verhalten festgestellt wird, wird ein Risikoindikator ausgelöst.
relevant_event_type	Gibt die Benutzeraktivitäten wie Herunterladen, Drucken oder Kopieren der Daten an.
exfil_data_volume_in_bytes	Die Menge der Datenexfiltration.
occurrence_event_type	Gibt an, wie die Datenexfiltration stattgefunden hat, z. B. die Zwischenablage in einer SaaS-App.
file_size_in_bytes	Die Größe der Datei.
file_type	Der Typ der Datei.
device_id	Die ID des Benutzergeräts.
receiver_type	Die Citrix Workspace-App oder Citrix Receiver, die auf dem Benutzergerät installiert ist.
app_url	Die URL der Anwendung, auf die der Benutzer zugreift.
entity_time_zone	Die Zeitzone des Benutzers.

Verdächtiges Logon-Risikoindikator-Schema

Zusammenfassungsschema des Indikators

```
{

  "tenant_id": "tenant_1",
  "indicator_id": "312",
  "indicator_uuid": "1b97c3be-abcd-efgh-ijkl-1234567890",
  "indicator_category_id": 3,
  "indicator_vector":
  [
    {

      "name": "Other Risk Indicators",
      "id": 7
     }
 ,
    {

      "name":"Location-Based Risk Indicators",
      "id":2
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
      }
  ,
     {

       "name":"IP-Based Risk Indicators",
       "id":4
      }
  ,
     {

       "name": "Device-Based Risk Indicators",
       "id": 1
      }
  ,
   ],
   "data_source_id": 3,
   "timestamp": "2020-06-06T12:14:59Z",
   "event_type": "indicatorSummary",
   "entity_type": "user",
   "entity_id": "user2",
   "version": 2,
   "risk_probability": 0.78,
   "indicator_category": "Compromised users",
   "indicator_name": "Suspicious logon",
   "severity": "medium",
   "data_source": "Citrix Apps and Desktops",
   "ui_link": "https://analytics.cloud.com/user/ ",
   "indicator_type": "builtin",
   "occurrence_details":
   {

     "user_location_risk": 0,
     "city": "Some_city",
     "observation_start_time": "2020-06-06T12:00:00Z",
     "event_count": 1,
     "user_device_risk": 75,
     "country": "United States",
     "device_id": "device2",
     "region": "Some_Region",
     "client_ip": "99.xx.xx.xx",
     "webroot_threat_categories": "'Spam Sources', 'Windows Exploits', '
        Web Attacks', 'Botnets', 'Scanners', 'Denial of Service'",
     "historical_logon_locations": "[{
"country":"United States","latitude":45.0,"longitude":45.0,"count":12
     }
,{
"country":"United States","region":"Some_Region_A","city":"Some_City_A
    ","latitude":0.0,"longitude":0.0,"count":8 }
]",
     "relevant_event_type": "Logon",
     "user_network_risk": 100,
     "historical_observation_period_in_days": 30,
     "suspicious_network_risk": 0
```


© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
    }

 }


<!--NeedCopy-->
```

Schema für die Ereignisdetails

```
{

  "tenant_id": "tenant_1",
  "indicator_id": "312",
  "indicator_uuid": "1b97c3be-abcd-efgh-ijkl-1234567890",
  "indicator_category_id": 3,
  "indicator_vector":
  [
    {

      "name": "Other Risk Indicators",
      "id": 7
     }
 ,
    {

      "name":"Location-Based Risk Indicators",
      "id":2
     }
 ,
    {

      "name":"IP-Based Risk Indicators",
      "id":4
     }
 ,
    {

      "name": "Device-Based Risk Indicators",
      "id": 1
     }
 ,
  ],
  "data_source_id": 3,
  "timestamp": "2020-06-06 12:02:30",
  "event_type": "indicatorEventDetails",
  "entity_type": "user",
  "entity_id": "user2",
  "version": 2,
  "occurrence_event_type": "Account.Logon",
  "city": "Some_city",
  "country": "United States",
  "region": "Some_Region",
  "latitude": 37.751,
  "longitude": -97.822,
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
46    "browser": "Firefox 1.3",
47    "os": "Windows OS",
48    "device_id": "device2",
49    "receiver_type": "XA.Receiver.Chrome",
50    "client_ip": "99.xxx.xx.xx"
51   }
52
53
54  <!--NeedCopy-->
```

In der folgenden Tabelle werden die für das Zusammenfassungsschema spezifischen Feldnamen und das Ereignisdetail-Schema für verdächtige Anmeldung beschrieben.

Feldname	Beschreibung
historical_logon_locations	Die Standorte, auf die der Benutzer zugegriffen hat, und wie oft während des Beobachtungszeitraums auf jeden Standort zugegriffen wurde.
historical_observation_period_in_days	Jeder Standort wird 30 Tage lang überwacht.
relevant_event_type	Gibt den Typ des Ereignisses wie Anmeldung an.
observation_start_time	Die Zeit, ab der Citrix Analytics beginnt, die Benutzeraktivität bis zum Zeitstempel zu überwachen. Wenn in diesem Zeitraum ein anomales Verhalten festgestellt wird, wird ein Risikoindikator ausgelöst.
occurrence_event_type	Gibt den Benutzerereignistyp wie die Kontoanmeldung an.
country	Das Land, aus dem sich der Benutzer angemeldet hat.
city	Die Stadt, von der sich der Benutzer angemeldet hat.
region	Gibt die Region an, aus der sich der Benutzer angemeldet hat.
latitude	Gibt den Breitengrad des Standorts an, von dem sich der Benutzer angemeldet hat.
longitude	Gibt den Längengrad des Ortes an, von dem sich der Benutzer angemeldet hat.
browser	Der vom Benutzer verwendete Webbrowser.
os	Das Betriebssystem des Geräts des Benutzers.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Feldname	Beschreibung
device_id	Der Name des vom Benutzer verwendeten Geräts.
receiver_type	Der Typ der Citrix Workspace-App oder Citrix Receiver, die auf dem Gerät des Benutzers installiert ist.
user_location_risk	Zeigt die Verdachtsstufe des Standorts an, von dem aus sich der Benutzer angemeldet hat. Niedriger Verdacht: 0—69, mittlerer Verdacht: 70—89 und Hoher Verdacht: 90—100
user_device_risk	Zeigt die Verdachtsstufe des Geräts an, von dem aus sich der Benutzer angemeldet hat. Niedriger Verdacht: 0—69, mittlerer Verdacht: 70—89 und Hoher Verdacht: 90—100
user_network_risk	Zeigt die Verdachtsstufe des Netzwerks oder des Subnetzes an, von dem aus sich der Benutzer angemeldet hat. Niedriger Verdacht: 0—69, mittlerer Verdacht: 70—89 und Hoher Verdacht: 90—100
suspicious_network_risk	Gibt die IP-Bedrohungsstufe basierend auf dem Webroot IP-Bedrohungs-Intelligence-Feed an. Niedrige Bedrohungsstufe: 0—69, mittlere Bedrohungsstufe: 70—89 und hohe Bedrohungsstufe: 90—100
webroot_threat_categories	Gibt die Arten von Bedrohungen an, die von der IP-Adresse basierend auf dem Webroot IP-Bedrohungsinfo-Feed erkannt wurden. Die Bedrohungskategorien können Spam-Quellen, Windows-Exploits, Webangriffe, Botnetze, Scanner, Denial of Service, Reputation, Phishing, Proxy, nicht spezifiziert, mobile Bedrohungen und Tor-Proxy sein

Microsoft Active Directory-Indikator

Zusammenfassungsschema des Indikators

```
{

  "data_source": "Microsoft Graph Security",
  "entity_id": "demo_user",
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
  "entity_type": "user",
  "event_type": "indicatorSummary",
  "indicator_category": "Compromised users",
  "indicator_id": 1000,
  "indicator_name": "MS Active Directory Indicator",
  "indicator_vector": {

    "name": "IP-Based Risk Indicators",
    "id": 4  }
 ,
  "indicator_type": "builtin",
  "indicator_uuid": "9880f479-9fbe-4ab0-8348-a613f9de5eba",
  "occurrence_details": {
  }
 ,
  "risk_probability": 1.0,
  "severity": "low",
  "tenant_id": "demo_tenant",
  "timestamp": "2021-01-27T16:03:46Z",
  "ui_link": "https://analytics-daily.cloud.com/user/",
  "version": 2
 }


<!--NeedCopy-->
```

Schema für die Ereignisdetails

```
{

  "entity_id": "demo_user",
  "entity_type": "user",
  "event_type": "indicatorEventDetails",
  "indicator_id": 1000,
  "indicator_vector": {

    "name": "IP-Based Risk Indicators",
    "id": 4  }
 ,
  "indicator_uuid": "9880f479-9fbe-4ab0-8348-a613f9de5eba",
  "tenant_id": "demo_tenant",
  "timestamp": "2021-01-27T16:03:46Z",
  "version": 2
 }


<!--NeedCopy-->
```

Benutzerdefinierte Risikoindikator-Schema

Im folgenden Abschnitt wird das Schema für den benutzerdefinierten Risikoindikator beschrieben.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Hinweis**
>
> Derzeit sendet Citrix Analytics die Daten zu den benutzerdefinierten Risikoindikatoren von Citrix DaaS und Citrix Virtual Apps and Desktops an Ihren SIEM-Dienst.

In der folgenden Tabelle werden die Feldnamen für das zusammenfassende Schema für benutzerdefinierte Risikoindikatoren beschrieben.

Feldname	Beschreibung
`data source`	Die Produkte, die Daten an Citrix Analytics for Security senden. Zum Beispiel: Citrix Secure Private Access, NetScaler Gateway und Citrix Apps and Desktops.
`data_source_id`	Die mit einer Datenquelle verknüpfte ID. ID 1 = Citrix Gateway, ID 2 = Citrix Endpoint Management, ID 3 = Citrix Apps und Desktops, ID 4 = Citrix Secure Private Access
`entity_id`	Die ID, die mit dem gefährdeten Unternehmen verknüpft ist.
`entity_type`	Das Unternehmen in Gefahr. In diesem Fall ist die Entität ein Benutzer.
`event_type`	Die Art der Daten, die an den SIEM-Dienst gesendet werden. In diesem Fall ist der Ereignistyp die Zusammenfassung des Risikoindikators.
`indicator_category`	Gibt die Kategorien von Risikoindikatoren an. Die Risikoindikatoren sind in eine der Risikokategorien unterteilt - kompromittierter Endpunkt, kompromittierte Benutzer, Datenexfiltration oder Insiderbedrohungen.
`indicator_id`	Die mit dem Risikoindikator verknüpfte eindeutige ID.
`indicator_category_id`	Die der Risikoindikatorkategorie zugeordnete ID. ID 1 = Datenexfiltration, ID 2 = Insider-Bedrohungen, ID 3 = Kompromittierte Benutzer, ID 4 = Kompromittierte Endpunkte
`indicator_name`	Der Name des Risikoindikators. Für einen benutzerdefinierten Risikoindikator wird dieser Name beim Erstellen des Indikators definiert.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Feldname	Beschreibung
indicator_type	Gibt an, ob der Risikoindikator Standard (eingebaut) oder benutzerdefiniert ist.
indicator_uuid	Die eindeutige ID, die mit der Risikoindikatorinstanz verbunden ist.
occurrence_details	Die Details über den Risikoindikator auslösenden Zustand.
pre_configured	Zeigt an, ob der benutzerdefinierte Risikoindikator vorkonfiguriert ist.
risk_probability	Gibt die Risikowahrscheinlichkeit an, die mit dem Benutzerereignis verbunden sind. Der Wert variiert zwischen 0 und 1,0. Für einen benutzerdefinierten Risikoindikator beträgt die risk_wahrscheinlichkeit immer 1,0, da es sich um einen richtlinienbasierten Indikator handelt.
severity	Gibt den Schweregrad des Risikos an. Es kann niedrig, mittel oder hoch sein.
tenant_id	Die einzigartige Identität des Kunden.
timestamp	Das Datum und die Uhrzeit, zu der der Risikoindikator ausgelöst wird.
ui_link	Der Link zur Benutzer-Timeline-Ansicht auf der Citrix Analytics-Benutzeroberfläche.
version	Die Schemaversion der verarbeiteten Daten. Die aktuelle Schemaversion ist 2.

In der folgenden Tabelle werden die Feldnamen beschrieben, die im Ereignisdetail-Schema für benutzerdefinierte Risikoindikatoren üblich sind.

Feldname	Beschreibung
data_source_id	Die mit einer Datenquelle verknüpfte ID. ID 1 = Citrix Gateway, ID 2 = Citrix Endpoint Management, ID 3 = Citrix Apps und Desktops, ID 4 = Citrix Secure Private Access
indicator_category_id	Die der Risikoindikatorkategorie zugeordnete ID. ID 1 = Datenexfiltration, ID 2 = Insider-Bedrohungen, ID 3 = Kompromittierte Benutzer, ID 4 = Kompromittierte Endpunkte

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Feldname	Beschreibung
event_type	Die Art der Daten, die an den SIEM-Dienst gesendet werden. In diesem Fall ist der Ereignistyp die Details des Risikoindikatorereignisses.
tenant_id	Die einzigartige Identität des Kunden.
entity_id	Die ID, die mit dem gefährdeten Unternehmen verknüpft ist.
entity_type	Das Unternehmen, das gefährdet ist. In diesem Fall ist es der Benutzer.
indicator_id	Die mit dem Risikoindikator verknüpfte eindeutige ID.
indicator_uuid	Die eindeutige ID, die mit der Risikoindikatorinstanz verbunden ist.
timestamp	Das Datum und die Uhrzeit, zu der der Risikoindikator ausgelöst wird.
version	Die Schemaversion der verarbeiteten Daten. Die aktuelle Schemaversion ist 2.
event_id	Die mit dem Benutzerereignis verknüpfte ID.
occurrence_event_type	Zeigt den Typ des Benutzerereignisses an, wie Sitzungsanmeldung, Sitzungsstart und Kontoanmeldung.
product	Gibt den Typ der Citrix Workspace-App an, z. B. die Citrix Workspace-App für Windows.
client_ip	Die IP-Adresse des Geräts des Benutzers.
session_user_name	Der Benutzername, der mit der Citrix Apps and Desktops-Sitzung verknüpft ist.
city	Der Name der Stadt, von der aus die Benutzeraktivität erkannt wird.
country	Der Name des Landes, aus dem die Benutzeraktivität erkannt wird.
device_id	Der Name des vom Benutzer verwendeten Geräts.
os_name	Das Betriebssystem, das auf dem Gerät des Benutzers installiert ist. Weitere Informationen finden Sie unter Self-Service-Suche nach Apps und Desktops.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Feldname	Beschreibung
os_version	Die Version des Betriebssystems, die auf dem Gerät des Benutzers installiert ist. Weitere Informationen finden Sie unter Self-Service-Suche nach Apps und Desktops.
os_extra_info	Die zusätzlichen Details im Zusammenhang mit dem Betriebssystem, das auf dem Gerät des Benutzers installiert ist. Weitere Informationen finden Sie unter Self-Service-Suche nach Apps und Desktops.

Benutzerdefinierter Risikoindikator für Citrix DaaS und Citrix Virtual Apps and Desktops

Zusammenfassungsschema des Indikators

```
{

  "data_source": " Citrix Apps and Desktops",
  "data_source_id": 3,
  "entity_id": "demo_user",
  "entity_type": "user",
  "event_type": "indicatorSummary",
  "indicator_category": "Compromised users",
  "indicator_category_id": 3,
  "indicator_id": "ca97a656ab0442b78f3514052d595936",
  "indicator_name": "Demo_user_usage",
  "indicator_type": "custom",
  "indicator_uuid": "8e680e29-d742-4e09-9a40-78d1d9730ea5",
  "occurrence_details": {

    "condition": "User-Name ~ demo_user", "happen": 0, "new_entities":
       "", "repeat": 0, "time_quantity": 0, "time_unit": "", "type": "
       everyTime" }
 ,
  "pre_configured": "N",
  "risk_probability": 1.0,
  "severity": "low",
  "tenant_id": "demo_tenant",
  "timestamp": "2021-02-10T14:47:25Z",
  "ui_link": "https://analytics.cloud.com/user/ ",
  "version": 2
 }


<!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Indicator Ereignisdetails Schema für das Sitzungsanmeldeereignis

```
{

  "event_type": "indicatorEventDetails",
  "data_source_id": 3,
  "indicator_category_id": 3,
  "tenant_id": "demo_tenant",
  "entity_id": "demo_user",
  "entity_type": "user",
  "indicator_id": "9033b2f6a8914a9282937b35ce497bcf",
  "timestamp": "2021-03-19T10:08:05Z",
  "indicator_uuid": "e0abfcb4-fd41-4612-ad59-ef7567508ac0",
  "version": 2,
  "event_id": "8fc3dd5e-d049-448a-ab70-0fc4d554e41e",
  "occurrence_event_type": "Session.Logon",
  "product": "XA.Receiver.Windows",
  "client_ip": "103.xx.xxx.xxx",
  "session_user_name": "user01",
  "city": "Mumbai",
  "country": "India",
  "device_id": "5-Synthetic_device",
  "os_name": "Windows NT 6.1",
  "os_version": "7601",
  "os_extra_info": "Service Pack 1",
  "app_name": "notepad",
  "launch_type": "Application",
  "domain": "test_domain",
  "server_name": "SYD04-MS1-S102",
  "session_guid": "f466e318-9065-440c-84a2-eec49d978a96",
 }


<!--NeedCopy-->
```

In der folgenden Tabelle werden die Feldnamen beschrieben, die für das Ereignisdetailschema für das Sitzungsanmeldeereignis spezifisch sind.

Feldname	Beschreibung
app_name	Name einer gestarteten Anwendung oder eines Desktops.
launch_type	Zeigt entweder eine Anwendung oder einen Desktop an.
domain	Der Domainname des Servers, der die Anfrage gesendet hat.
server_name	Name des Servers.
session_guid	Die GUID der aktiven Sitzung.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Indikator Ereignisdetails Schema für das Session-Start-Ereignis

```
{

  "event_type": "indicatorEventDetails",
  "data_source_id": 3,
  "indicator_category_id": 3,
  "tenant_id": "demo_tenant",
  "entity_id": "demo_user",
  "entity_type": "user",
  "indicator_id": "9033b2f6a8914a9282937b35ce497bcf",
  "timestamp": "2021-03-19T10:08:05Z",
  "indicator_uuid": "e0abfcb4-fd41-4612-ad59-ef7567508ac0",
  "version": 2,
  "event_id": "8fc3dd5e-d049-448a-ab70-0fc4d554e41e",
  "occurrence_event_type": "Session.Launch",
  "product": "XA.Receiver.Windows",
  "client_ip": "103.xx.xxx.xxx",
  "session_user_name": "user01",
  "city": "Mumbai",
  "country": "India",
  "device_id": "5-Synthetic_device",
  "os_name": "Windows NT 6.1",
  "os_version": "7601",
  "os_extra_info": "Service Pack 1",
  "app_name": "notepad",
  "launch_type": "Application",
 }


<!--NeedCopy-->
```

In der folgenden Tabelle werden die Feldnamen beschrieben, die für das Ereignisdetailschema für das Sitzungsstartereignis spezifisch sind.

Feldname	Beschreibung
app_name	Name einer gestarteten Anwendung oder eines Desktops.
launch_type	Zeigt entweder eine Anwendung oder einen Desktop an.

Indicator Ereignisdetails Schema für das Kontoanmeldeereignis

```
{

  "event_type": "indicatorEventDetails",
  "data_source_id": 3,
  "indicator_category_id": 3,
  "tenant_id": "demo_tenant",
  "entity_id": "demo_user",
  "entity_type": "user",
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
  "indicator_id": "9033b2f6a8914a9282937b35ce497bcf",
  "timestamp": "2021-03-19T10:08:05Z",
  "indicator_uuid": "e0abfcb4-fd41-4612-ad59-ef7567508ac0",
  "version": 2,
  "event_id": "8fc3dd5e-d049-448a-ab70-0fc4d554e41e",
  "occurrence_event_type": "Account.Logon",
  "product": "XA.Receiver.Windows",
  "client_ip": "103.xx.xxx.xxx",
  "session_user_name": "user01",
  "city": "Mumbai",
  "country": "India",
  "device_id": "5-Synthetic_device",
  "os_name": "Windows NT 6.1",
  "os_version": "7601",
  "os_extra_info": "Service Pack 1",
  "app_name": "notepad",
 }


<!--NeedCopy-->
```

In der folgenden Tabelle werden die Feldnamen beschrieben, die für das Ereignisdetailschema für das Kontoanmeldeereignis spezifisch sind.

Feldname	Beschreibung
app_name	Name einer gestarteten Anwendung oder eines Desktops.

Indikatorereignisdetailsschema für das Sitzungsendereignis

```
{

  "event_type": "indicatorEventDetails",
  "data_source_id": 3,
  "indicator_category_id": 3,
  "tenant_id": "demo_tenant",
  "entity_id": "demo_user",
  "entity_type": "user",
  "indicator_id": "9033b2f6a8914a9282937b35ce497bcf",
  "timestamp": "2021-03-19T10:08:05Z",
  "indicator_uuid": "e0abfcb4-fd41-4612-ad59-ef7567508ac0",
  "version": 2,
  "event_id": "8fc3dd5e-d049-448a-ab70-0fc4d554e41e",
  "occurrence_event_type": "Session.End",
  "product": "XA.Receiver.Windows",
  "client_ip": "103.xx.xxx.xxx",
  "session_user_name": "user01",
  "city": "Mumbai",
  "country": "India",
  "device_id": "5-Synthetic_device",
  "os_name": "Windows NT 6.1",
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
  "os_version": "7601",
  "os_extra_info": "Service Pack 1",
  "app_name": "notepad",
  "launch_type": "Application",
  "domain": "test_domain",
  "server_name": "test_server",
  "session_guid": "f466e318-9065-440c-84a2-eec49d978a96",
 }


<!--NeedCopy-->
```

In der folgenden Tabelle werden die Feldnamen beschrieben, die für das Ereignisdetailschema für das Sitzungsendereignis spezifisch sind.

Feldname	Beschreibung
app_name	Name einer gestarteten Anwendung oder eines Desktops.
launch_type	Zeigt entweder eine Anwendung oder einen Desktop an.
domain	Der Domainname des Servers, der die Anfrage gesendet hat.
server_name	Name des Servers.
session_guid	Die GUID der aktiven Sitzung.

Indikator Ereignisdetails Schema für das App-Startereignis

```
{

  "event_type": "indicatorEventDetails",
  "data_source_id": 3,
  "indicator_category_id": 3,
  "tenant_id": "demo_tenant",
  "entity_id": "demo_user",
  "entity_type": "user",
  "indicator_id": "9033b2f6a8914a9282937b35ce497bcf",
  "timestamp": "2021-03-19T10:08:05Z",
  "indicator_uuid": "e0abfcb4-fd41-4612-ad59-ef7567508ac0",
  "version": 2,
  "event_id": "8fc3dd5e-d049-448a-ab70-0fc4d554e41e",
  "occurrence_event_type": "App.Start",
  "product": "XA.Receiver.Windows",
  "client_ip": "103.xx.xxx.xxx",
  "session_user_name": "user01",
  "city": "Mumbai",
  "country": "India",
  "device_id": "5-Synthetic_device",
  "os_name": "Windows NT 6.1",
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
  "os_version": "7601",
  "os_extra_info": "Service Pack 1",
  "app_name": "notepad",
  "launch_type": "Application",
  "domain": "test_domain",
  "server_name": "test_server",
  "session_guid": "f466e318-9065-440c-84a2-eec49d978a96",
  "module_file_path": "/root/folder1/folder2/folder3"
 }


<!--NeedCopy-->
```

In der folgenden Tabelle werden die Feldnamen beschrieben, die für das Ereignisdetailschema für das App-Startereignis spezifisch sind.

Feldname	Beschreibung
app_name	Name einer gestarteten Anwendung oder eines Desktops.
launch_type	Zeigt entweder eine Anwendung oder einen Desktop an.
domain	Der Domainname des Servers, der die Anfrage gesendet hat.
server_name	Name des Servers.
session_guid	Die GUID der aktiven Sitzung.
module_file_path	Der Pfad der Anwendung, die verwendet wird.

Anzeigeereignisdetailschema für das App-Endereignis

```
{

  "event_type": "indicatorEventDetails",
  "data_source_id": 3,
  "indicator_category_id": 3,
  "tenant_id": "demo_tenant",
  "entity_id": "demo_user",
  "entity_type": "user",
  "indicator_id": "9033b2f6a8914a9282937b35ce497bcf",
  "timestamp": "2021-03-19T10:08:05Z",
  "indicator_uuid": "e0abfcb4-fd41-4612-ad59-ef7567508ac0",
  "version": 2,
  "event_id": "8fc3dd5e-d049-448a-ab70-0fc4d554e41e",
  "occurrence_event_type": "App.End",
  "product": "XA.Receiver.Windows",
  "client_ip": "103.xx.xxx.xxx",
  "session_user_name": "user01",
  "city": "Mumbai",
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
  "country": "India",
  "device_id": "5-Synthetic_device",
  "os_name": "Windows NT 6.1",
  "os_version": "7601",
  "os_extra_info": "Service Pack 1",
  "app_name": "notepad",
  "launch_type": "Application",
  "domain": "test_domain",
  "server_name": "test_server",
  "session_guid": "f466e318-9065-440c-84a2-eec49d978a96",
  "module_file_path": "/root/folder1/folder2/folder3"
 }


<!--NeedCopy-->
```

In der folgenden Tabelle werden die Feldnamen beschrieben, die für das Ereignisdetailschema für das App-Endereignis spezifisch sind.

Feldname	Beschreibung
app_name	Name einer gestarteten Anwendung oder eines Desktops.
launch_type	Zeigt entweder eine Anwendung oder einen Desktop an.
domain	Der Domainname des Servers, der die Anfrage gesendet hat.
server_name	Name des Servers.
session_guid	Die GUID der aktiven Sitzung.
module_file_path	Der Pfad der Anwendung, die verwendet wird.

Indicator Ereignisdetails Schema für das Datei-Download-Ereignis

```
{

  "event_type": "indicatorEventDetails",
  "data_source_id": 3,
  "indicator_category_id": 3,
  "tenant_id": "demo_tenant",
  "entity_id": "demo_user",
  "entity_type": "user",
  "indicator_id": "9033b2f6a8914a9282937b35ce497bcf",
  "timestamp": "2021-03-19T10:08:05Z",
  "indicator_uuid": "e0abfcb4-fd41-4612-ad59-ef7567508ac0",
  "version": 2,
  "event_id": "8fc3dd5e-d049-448a-ab70-0fc4d554e41e",
  "occurrence_event_type": "File.Download",
  "product": "XA.Receiver.Windows",
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
  "client_ip": "103.xx.xxx.xxx",
  "session_user_name": "user01",
  "city": "Mumbai",
  "country": "India",
  "device_id": "5-Synthetic_device",
  "os_name": "Windows NT 6.1",
  "os_version": "7601",
  "os_extra_info": "Service Pack 1",
  "file_download_file_name": "File5.txt",
  "file_download_file_path": "/root/folder1/folder2/folder3",
  "file_size_in_bytes": 278,
  "launch_type": "Desktop",
  "domain": "test_domain",
  "server_name": "test_server",
  "session_guid": "f466e318-9065-440c-84a2-eec49d978a96",
  "device_type": "USB"
 }


<!--NeedCopy-->
```

In der folgenden Tabelle werden die Feldnamen beschrieben, die für das Ereignisdetailschema des Datei-Download-Ereignisses spezifisch sind.

Feldname	Beschreibung
file_download_file_name	Name der Download-Datei.
file_download_file_path	Der Zielpfad, in den die Datei heruntergeladen wird.
launch_type	Zeigt entweder eine Anwendung oder einen Desktop an.
domain	Der Domainname des Servers, der die Anfrage gesendet hat.
server_name	Name des Servers.
session_guid	Die GUID der aktiven Sitzung.
device_type	Gibt den Typ des Geräts an, auf das die Datei heruntergeladen wird.

Anzeigeereignisdetailschema für das Druckereignis

```
{

  "event_type": "indicatorEventDetails",
  "data_source_id": 3,
  "indicator_category_id": 3,
  "tenant_id": "demo_tenant",
  "entity_id": "demo_user",
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
  "entity_type": "user",
  "indicator_id": "9033b2f6a8914a9282937b35ce497bcf",
  "timestamp": "2021-03-19T10:08:05Z",
  "indicator_uuid": "e0abfcb4-fd41-4612-ad59-ef7567508ac0",
  "version": 2,
  "event_id": "8fc3dd5e-d049-448a-ab70-0fc4d554e41e",
  "occurrence_event_type": "Printing",
  "product": "XA.Receiver.Windows",
  "client_ip": "103.xx.xxx.xxx",
  "session_user_name": "user01",
  "city": "Mumbai",
  "country": "India",
  "device_id": "5-Synthetic_device",
  "os_name": "Windows NT 6.1",
  "os_version": "7601",
  "os_extra_info": "Service Pack 1",
  "printer_name": "Test-printer",
  "launch_type": "Desktop",
  "domain": "test_domain",
  "server_name": "test_server",
  "session_guid": "f466e318-9065-440c-84a2-eec49d978a96",
  "job_details_size_in_bytes": 454,
  "job_details_filename": "file1.pdf",
  "job_details_format": "PDF"
 }


<!--NeedCopy-->
```

In der folgenden Tabelle werden die Feldnamen beschrieben, die für das Ereignisdetailschema für das Druckereignis spezifisch sind.

Feldname	Beschreibung
printer_name	Name des für den Druckauftrag verwendeten Druckers.
launch_type	Zeigt entweder eine Anwendung oder einen Desktop an.
domain	Der Domainname des Servers, der die Anfrage gesendet hat.
server_name	Name des Servers.
session_guid	Die GUID der aktiven Sitzung.
job_details_size_in_bytes	Die Größe des Druckauftrags, z. B. Datei oder Ordner.
job_details_filename	Name der gedruckten Datei.
job_details_format	Das Format des gedruckten Auftrags.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Indicator Ereignisdetails Schema für das App SaaS Launch-Ereignis

```
{

  "event_type": "indicatorEventDetails",
  "data_source_id": 3,
  "indicator_category_id": 3,
  "tenant_id": "demo_tenant",
  "entity_id": "demo_user",
  "entity_type": "user",
  "indicator_id": "9033b2f6a8914a9282937b35ce497bcf",
  "timestamp": "2021-03-19T10:08:05Z",
  "indicator_uuid": "e0abfcb4-fd41-4612-ad59-ef7567508ac0",
  "version": 2,
  "event_id": "8fc3dd5e-d049-448a-ab70-0fc4d554e41e",
  "occurrence_event_type": "App.SaaS.Launch",
  "product": "XA.Receiver.Windows",
  "client_ip": "103.xx.xxx.xxx",
  "session_user_name": "user01",
  "city": "Mumbai",
  "country": "India",
  "device_id": "5-Synthetic_device",
  "os_name": "Windows NT 6.1",
  "os_version": "7601",
  "os_extra_info": "Service Pack 1",
  "launch_type": "Desktop",
 }


<!--NeedCopy-->
```

In der folgenden Tabelle werden die Feldnamen beschrieben, die für das Ereignisdetailschema für das SaaS-Startereignis der App spezifisch sind.

Feldname	Beschreibung
`launch_type`	Zeigt entweder eine Anwendung oder einen Desktop an.

Indikator Ereignisdetails Schema für das SaaS-Endereignis der App

```
{

  "event_type": "indicatorEventDetails",
  "data_source_id": 3,
  "indicator_category_id": 3,
  "tenant_id": "demo_tenant",
  "entity_id": "demo_user",
  "entity_type": "user",
  "indicator_id": "9033b2f6a8914a9282937b35ce497bcf",
  "timestamp": "2021-03-19T10:08:05Z",
  "indicator_uuid": "e0abfcb4-fd41-4612-ad59-ef7567508ac0",
  "version": 2,
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
  "event_id": "8fc3dd5e-d049-448a-ab70-0fc4d554e41e",
  "occurrence_event_type": "App.SaaS.End",
  "product": "XA.Receiver.Windows",
  "client_ip": "103.xx.xxx.xxx",
  "session_user_name": "user01",
  "city": "Mumbai",
  "country": "India",
  "device_id": "5-Synthetic_device",
  "os_name": "Windows NT 6.1",
  "os_version": "7601",
  "os_extra_info": "Service Pack 1",
  "launch_type": "Desktop",
 }


<!--NeedCopy-->
```

In der folgenden Tabelle werden die Feldnamen beschrieben, die für das Ereignisdetailschema für das SaaS-Endereignis der App spezifisch sind.

Feldname	Beschreibung
`launch_type`	Zeigt entweder eine Anwendung oder einen Desktop an.

Datenquellen-Ereignisse

Darüber hinaus können Sie die Funktion Datenexporte so konfigurieren, dass Benutzerereignisse aus Ihren Citrix Analytics for Security-fähigen Produktdatenquellen exportiert werden. Wenn Sie eine Aktivität in der Citrix-Umgebung ausführen, werden die Datenquellenereignisse generiert. Bei den exportierten Ereignissen handelt es sich um unverarbeitete Benutzer- und Produktnutzungsdaten in Echtzeit, wie sie in der Self-Service-Ansicht verfügbar sind. Die in diesen Ereignissen enthaltenen Metadaten können außerdem für eingehendere Bedrohungsanalysen verwendet werden, um neue Dashboards zu erstellen und mit anderen Datenquellenereignissen zu verknüpfen, die nicht von Citrix stammen, in Ihrer Sicherheits- und IT-Infrastruktur.

Derzeit sendet Citrix Analytics for Security Benutzerereignisse für die Citrix Virtual Apps and Desktops-Datenquelle an Ihr SIEM.

Schemadetails der Datenquellenereignisse

Ereignisse für Citrix Virtual Apps and Desktops

Die Benutzerereignisse werden in Echtzeit in Citrix Analytics for Security empfangen, wenn Benutzer virtuelle Apps oder virtuelle Desktops verwenden. Weitere Informationen finden Sie unter Citrix Vir-

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

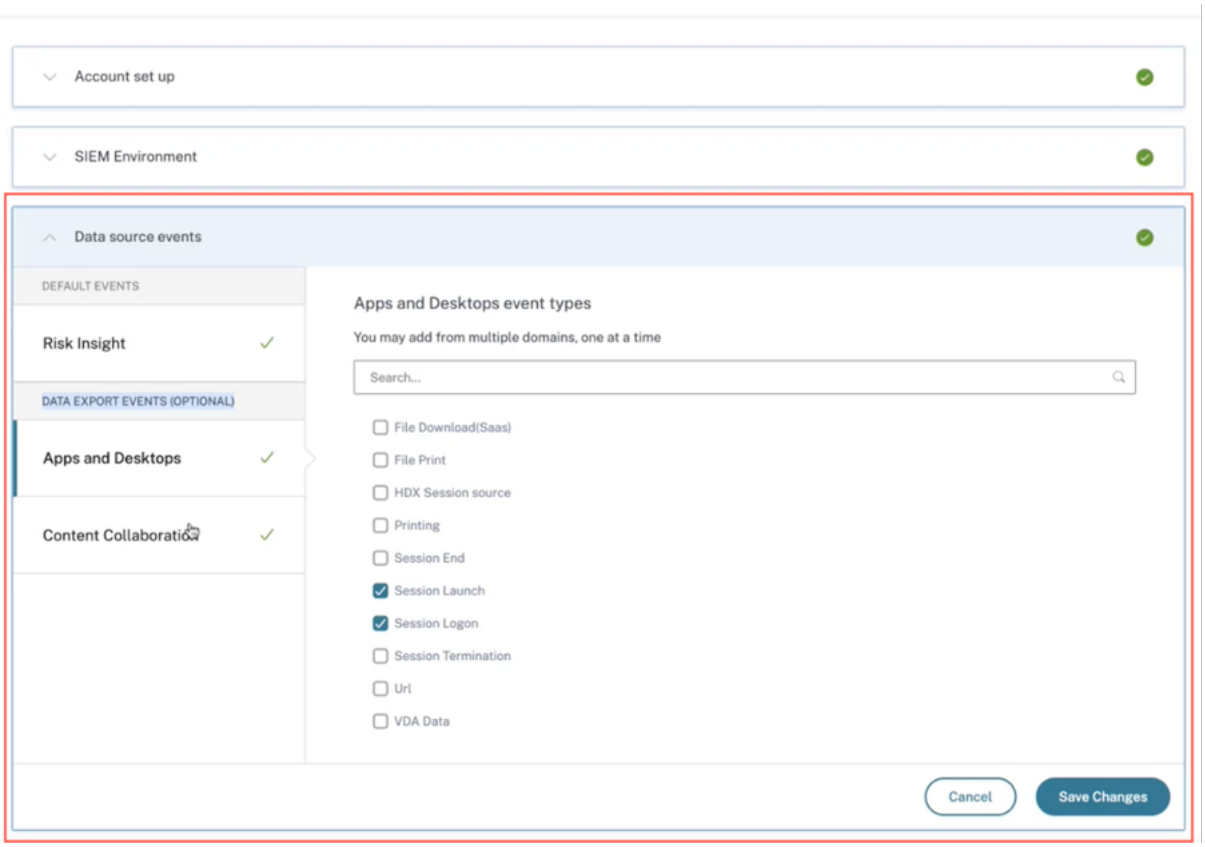
tual Apps and Desktops und Citrix DaaS-Datenquelle. Sie können die folgenden Benutzerereignisse anzeigen, die mit Citrix Virtual Apps and Desktops in Ihrem SIEM verknüpft sind:

- Alle Ereignistypen
- Account-Anmeldung
- App (starten, starten, beenden)
- Zwischenablage
- Datei (drucken, herunterladen)
- Dateidownload (SaaS)
- HDX-Sitzungsquelle
- Drucken
- Sitzung (Anmelden, Starten, Beenden, Beenden)
- URL
- VDA-Daten
- VDA-Prozesserstellung

Weitere Informationen zu den Ereignissen und ihren Attributen finden Sie unter Self-Service-Suche nach Virtual Apps and Desktops.

Sie können überprüfen, welche Ereignistypen aktiviert sind und an SIEM weitergeleitet werden. Sie können den Ereignistyp, der für einen Mandanten gilt, konfigurieren oder entfernen und auf die Schaltfläche **Änderungen speichern** klicken, um Ihre Einstellungen zu speichern.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Nutzung des SIEM-Datenmodells von Citrix Analytics für Bedrohungsanalysen und Datenkorrelation

June 19, 2023

In diesem Artikel wird die Beziehung zwischen Entitätsdaten erläutert, die sich aus den Ereignissen ergeben, die an die SIEM-Umgebung eines Kunden gesendet werden. Um dies zu verdeutlichen, nehmen wir ein Beispiel für ein Threat-Hunting-Szenario, bei dem die Attribute Client-IP und Betriebssystem im Mittelpunkt stehen. Die folgenden Möglichkeiten, die genannten Attribute dem Benutzer zuzuordnen, werden erörtert:

- Verwendung benutzerdefinierter Erkenntnisse zu Risikoindikatoren
- Datenquellenereignisse verwenden

Splunk ist die SIEM-Umgebung, die für das folgende Beispiel ausgewählt wurde. Eine ähnliche Datenkorrelation kann auch auf Sentinel mithilfe der Arbeitsmappenvorlage von Citrix Analytics durchgeführt werden. Weitere Informationen finden Sie in der Citrix Analytics-Arbeitsmappe für Microsoft Sentinel.

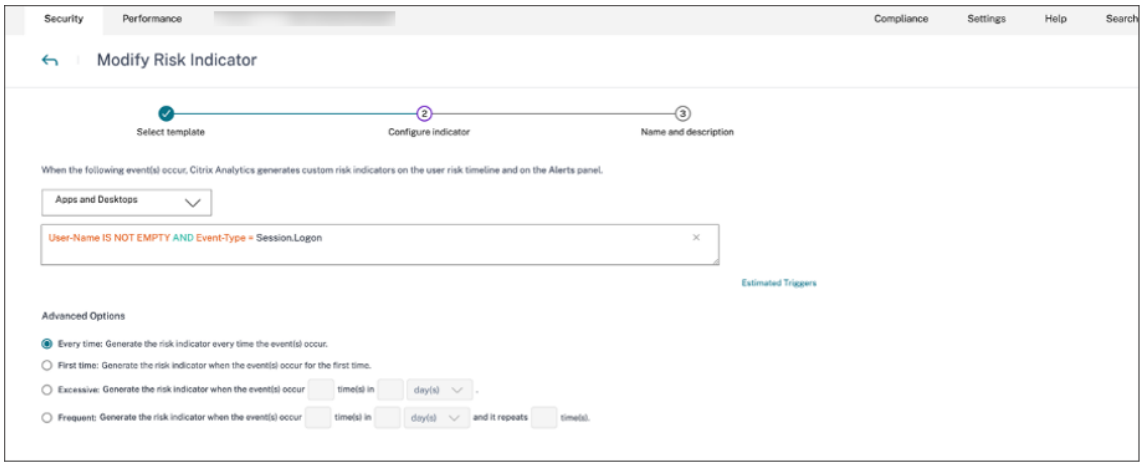
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Benutzerdefinierte Einblicke in Risikoindikatoren

Wie im Citrix Analytics-Datenexportformat für SIEMerwähnt, sind Erkenntnisse zur Indikatorzusammenfassung und zu den Ereignisdetails Teil des Standarddatensatzes für Risikoeinblicke. Für den Indikatordatensatz von Citrix Virtual Apps and Desktops werden Client-IP und Betriebssystem standardmäßig exportiert. Wenn also ein Administrator einen benutzerdefinierten Indikator mit oder ohne die Bedingung einrichtet, die diese Felder enthält, würden die besagten Datenpunkte in Ihre Splunk-Umgebung fließen.

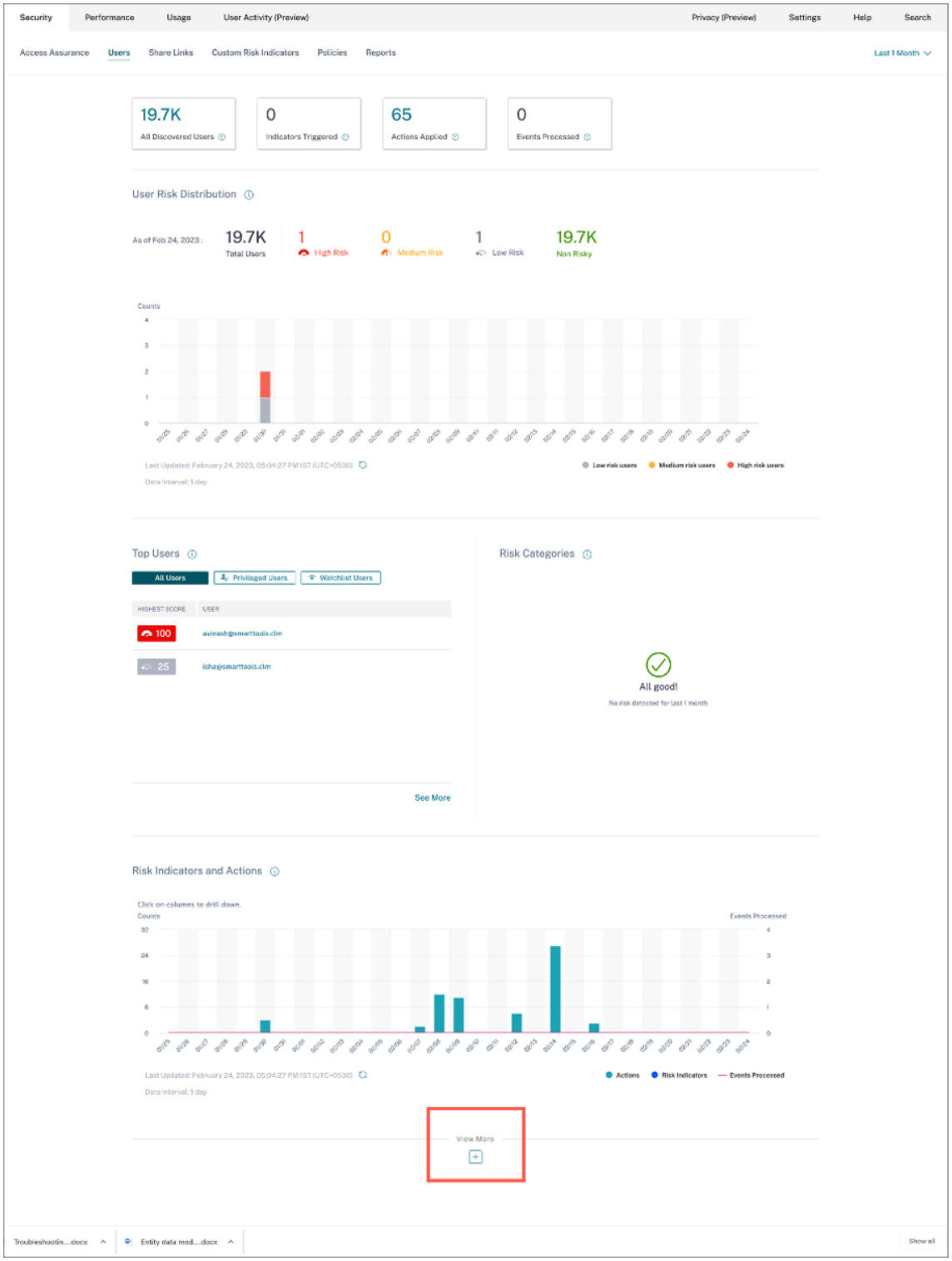
Festlegen eines benutzerdefinierten Risikoindikators in Citrix Analytics

1. Navigieren Sie zum **Citrix Analytics for Security Dashboard > Benutzerdefinierte Risikoindikatoren > Indikator erstellen**. Sie können einen benutzerdefinierten Risikoindikator mit einer beliebigen Bedingung erstellen, der Sie bei der Überwachung des Benutzerverhaltens unterstützt. Nachdem Sie den benutzerdefinierten Indikator eingerichtet haben, sind alle Benutzer, die die zugehörige Bedingung auslösen, in Ihrer Splunk-Umgebung sichtbar.



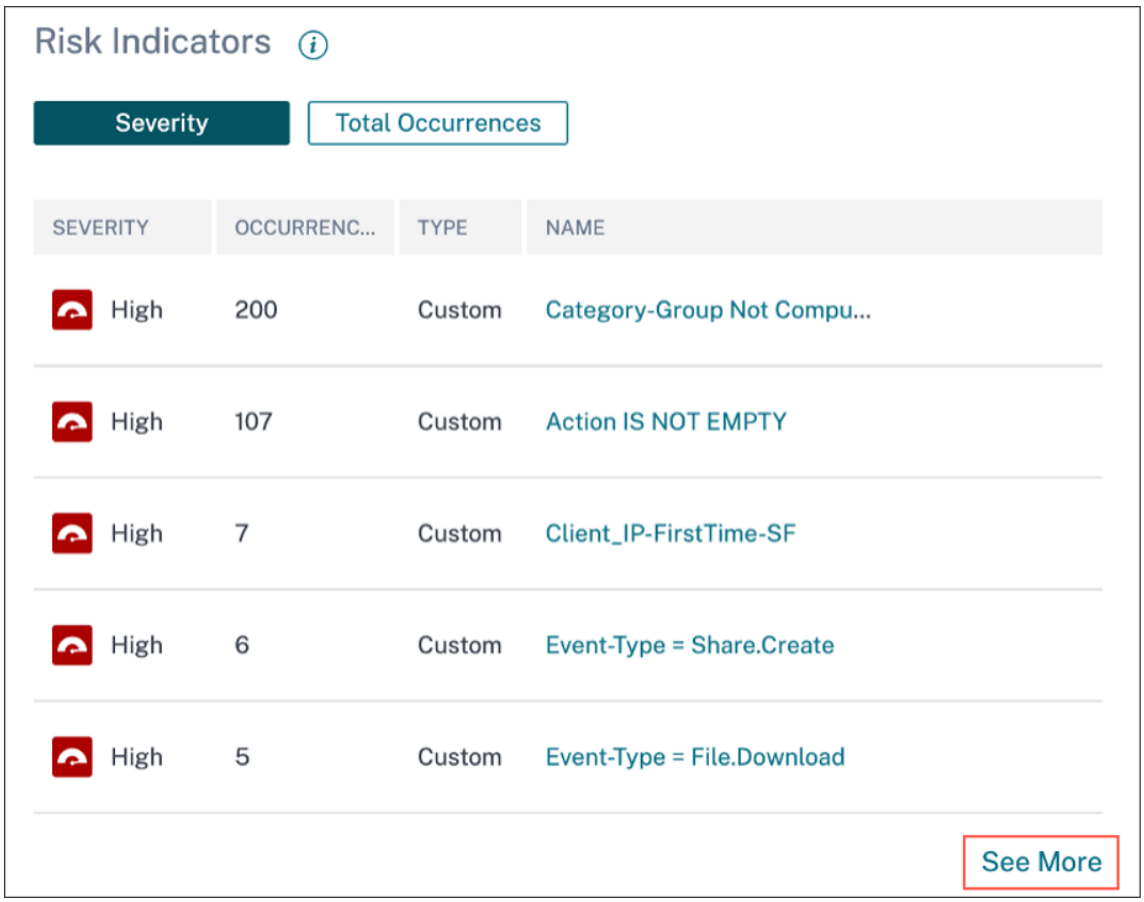
2. Um das Auftreten der erstellten Risikoindikatoren in Citrix Analytics for Security zu sehen, navigieren Sie zu **Sicherheit > Benutzer. Navigieren Sie zum Ende der Seite und klicken Sie auf das Pluszeichen (+)**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

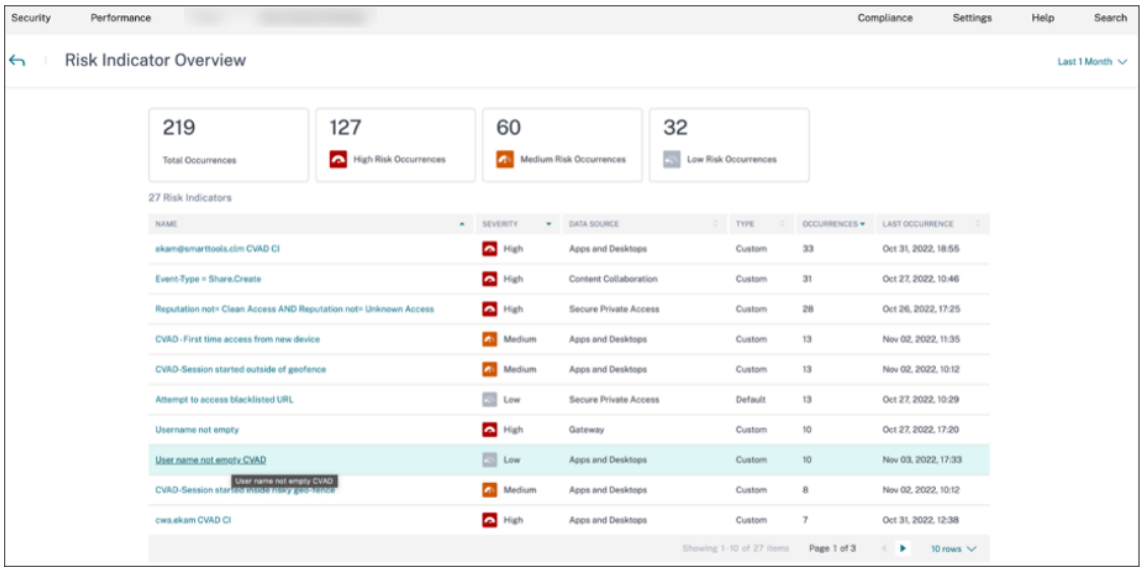


Die Karte mit den Risikoindikatoren wird angezeigt. Sie können die Details des Risikoindikators, des Schweregrads und des Vorkommens einsehen.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



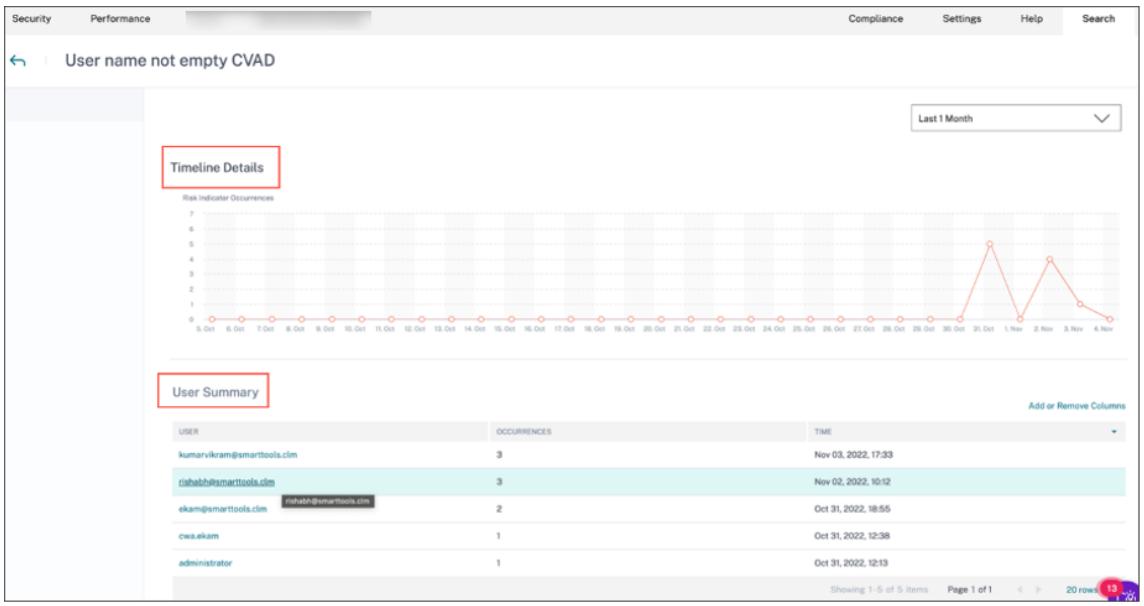
3. Klicken Sie auf **Mehr anzeigen**. Die Seite mit der **Übersicht über** den Risikoindikator wird angezeigt.



Auf der Seite mit der Übersicht über den Risikoindikator können Sie die Details des Benutzers, der den Indikator ausgelöst hat, mit einer detaillierten Zeitleistenansicht und einer

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Benutzerübersicht einsehen. Weitere Informationen zum Zeitplan finden Sie unter Zeitplan und Profil für Benutzerrisiken.



Vorkommen von Risikoindikatoren auf Splunk - Raw Queries

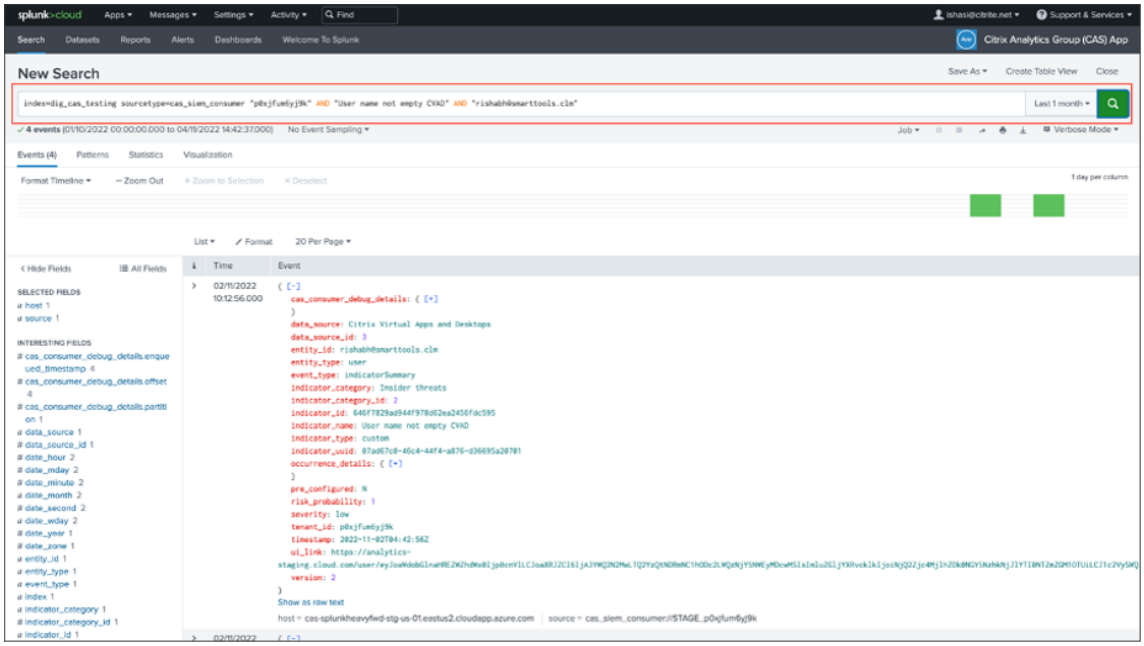
Sie können die Client-IP- und Betriebssysteminformationen auch abrufen, indem Sie den Index und den Quelltyp verwenden, die vom Splunk-Infrastrukturadministrator bei der Einrichtung der Dateneingabe im Splunk Enterprise for Citrix Analytics for Security Add-on verwendet wurden.

1. Navigieren Sie zu **Splunk > Neue Suche**. Geben Sie in der Suchabfrage die folgende Abfrage ein und führen Sie sie aus:

```
index=<index configured by you> sourcetype=<sourcetype configured
    by you> AND "<tenant_id>" AND "<indicator name configured by
    you on CAS>" AND "<user you are interested in>"

<!--NeedCopy-->
```

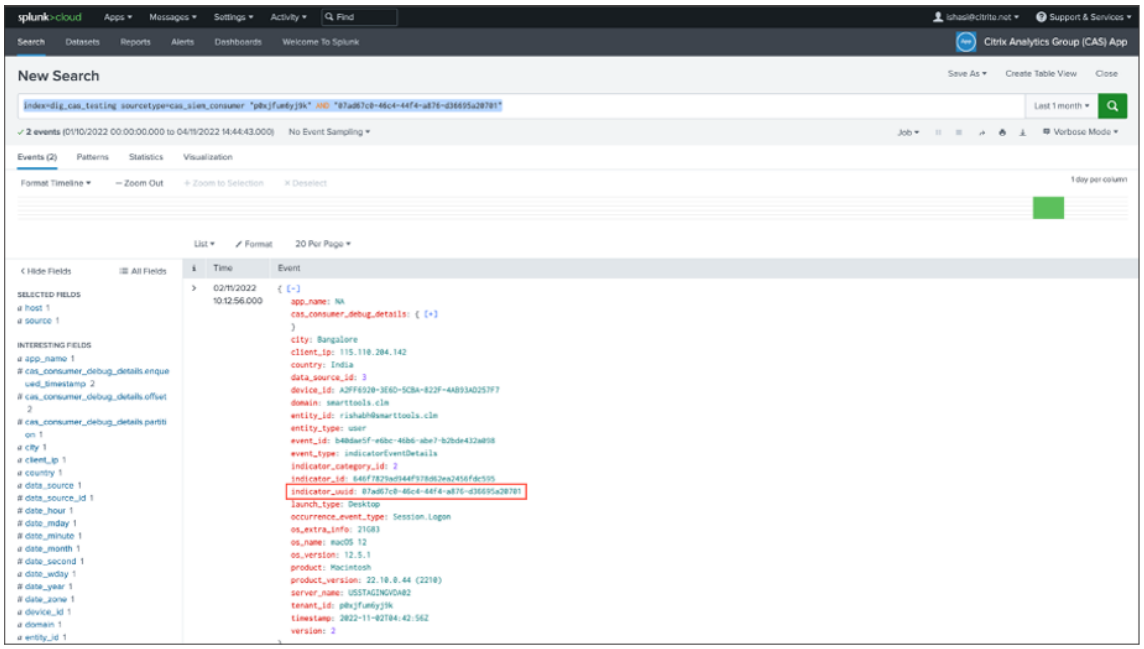
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



2. Holen Sie sich die indicator_uuid und führen Sie die folgende Abfrage aus:

```
index=<index configured by you> sourcetype=<sourcetype configured
    by you> "<tenant_id>" AND "<indicator_uuid>"

<!--NeedCopy-->
```



Das Ereignisergebnis enthält die **Zusammenfassung des Indikatorereignisses** und die **Indikatorereignisdetails** (die Aktivität, die durch Ihren Indikator ausgelöst wird). Die Ereignisdetails enthalten die **Client-IP** - und **Betriebssysteminformationen** (Name, Version, zusätzliche Informationen).

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

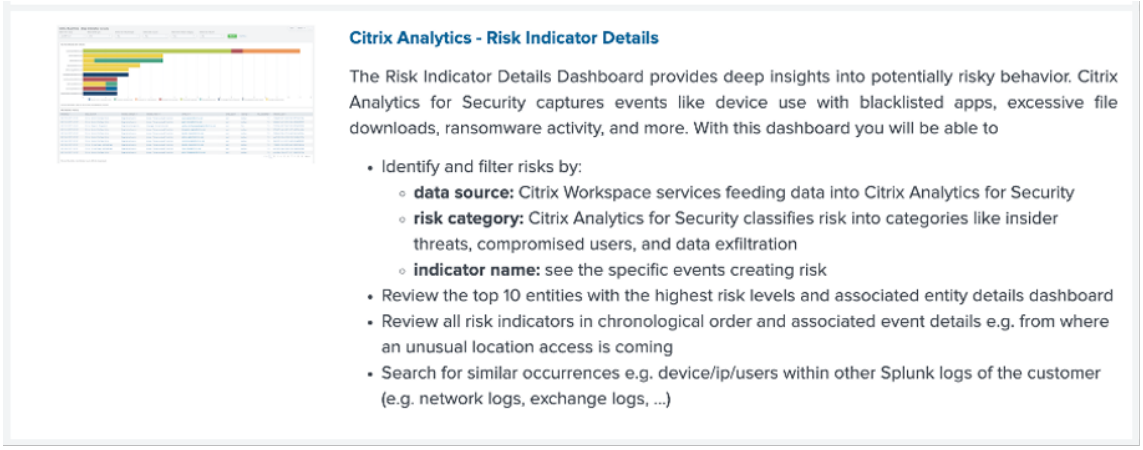
Weitere Informationen zum Datenformat finden Sie unter Citrix Analytics-Datenexportformat für SIEM.

Vorkommen von Risikoindikatoren auf Splunk —Dashboard-App

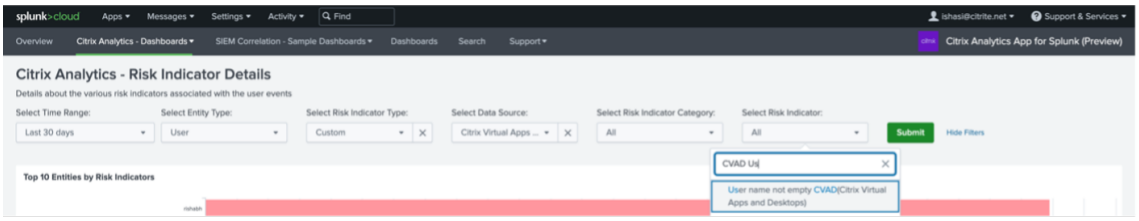
In den folgenden Artikeln finden Sie Anleitungen zur Installation der Citrix Analytics-App für Splunk:

- Citrix Analytics App für Splunk
- Citrix Analytics-Dashboards für Splunk

1. Klicken Sie auf die Registerkarte **Citrix Analytics** —**Dashboard** und wählen Sie in der Dropdownliste die Option **Risikoindikatordetails** aus.

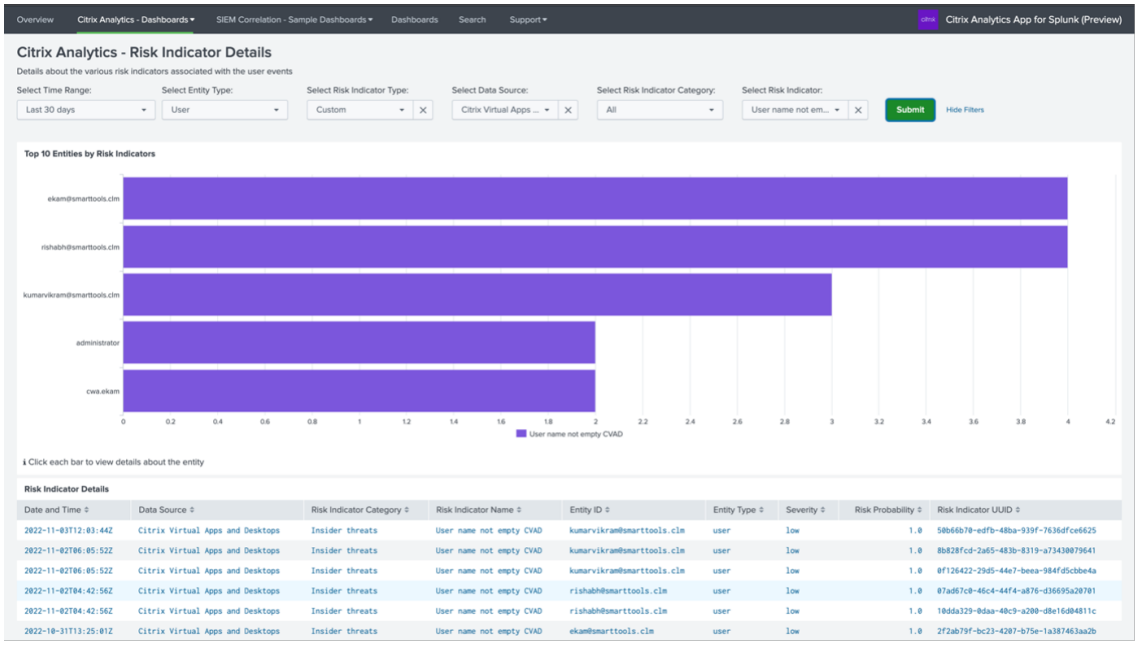


2. Filtern Sie den Inhalt entsprechend aus der Dropdownliste und klicken Sie auf **Senden**.

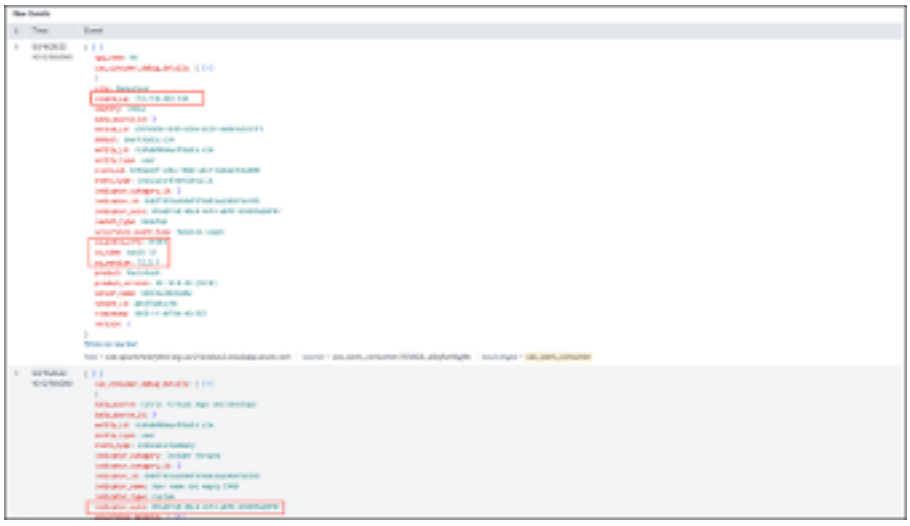


3. Klicken Sie auf die Benutzerinstanz, um die Details abzurufen.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



4. Sie können die **Client-IP** - und **Betriebssysteminformationen** (Name, Version, zusätzliche Informationen) unten auf dieser Seite einsehen:



Datenquellen-Ereignisse

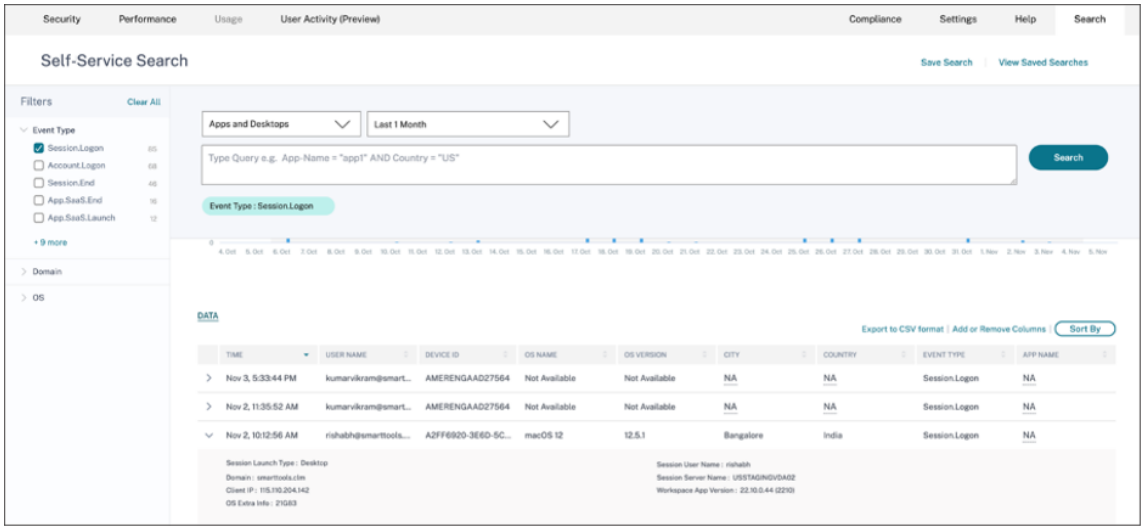
Eine weitere Methode, um die Client-IP- und Betriebssystemdetails in Ihrer Splunk-Umgebung abzurufen, besteht darin, Datenquellenereignisse für den Export zu konfigurieren. Mit dieser Funktion können Ereignisse, die in der Self-Service Search-Ansicht angezeigt werden, direkt in Ihre Splunk-Umgebung fließen. Weitere Informationen zur Konfiguration von Ereignistypen für Virtual Apps and Desktops, die nach SIEM exportiert werden sollen, finden Sie in den folgenden Artikeln:

- Datenereignisse, die aus Citrix Analytics for Security in Ihren SIEM-Dienst exportiert wurden.

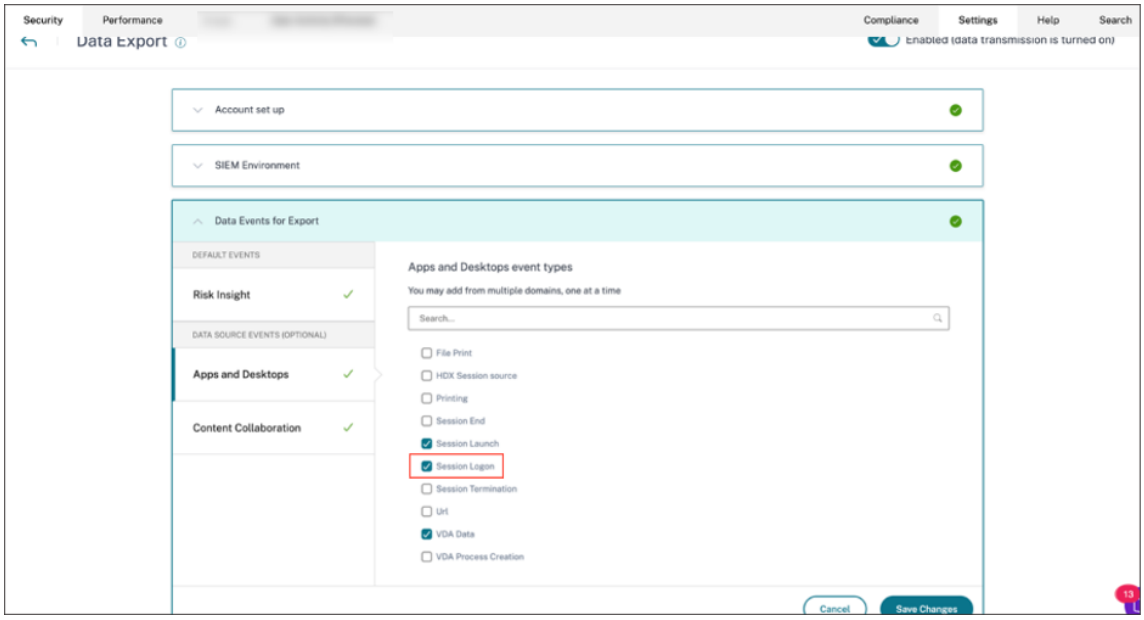
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Datenquellen-Ereignisse

1. Navigieren Sie zum **Dashboard von Citrix Analytic for Security > Suchen**. Auf dieser Self-Service-Suchseite sind alle Ereignistypen und die zugehörigen Informationen verfügbar. Im folgenden Screenshot sehen Sie den Ereignistyp **Session.Logon** als Beispiel:



2. Konfigurieren Sie **Session.Logon** in Data Source Events for Export und klicken **Sie auf Speichern**, damit es in Ihre Splunk-Umgebung einfließen kann.

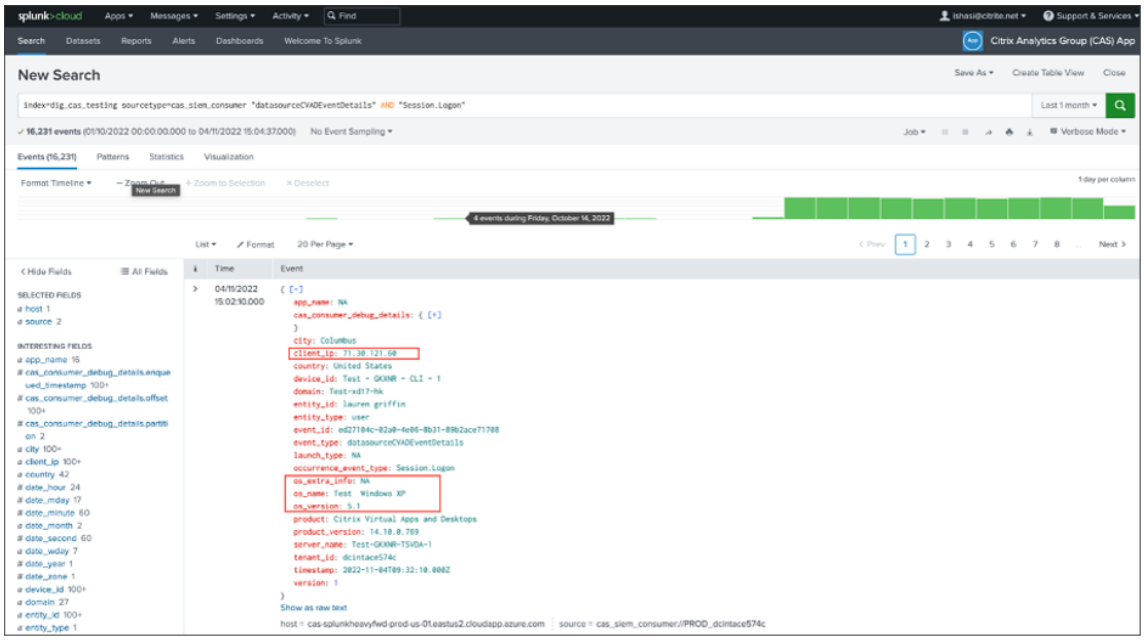


3. Gehen Sie zu Splunk, geben Sie die folgende Abfrage ein und führen Sie sie aus:

```
1 index="<index you configured>" sourcetype="<sourcetype you
     configured>" "<tenant_id>" AND "datasourceCVADEventDetails" AND
      "Session.Logon"  AND "<user you're interested in>"
2
3 <!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Die Felder, die sich auf Client-IP und Betriebssystem beziehen, sind hervorgehoben.

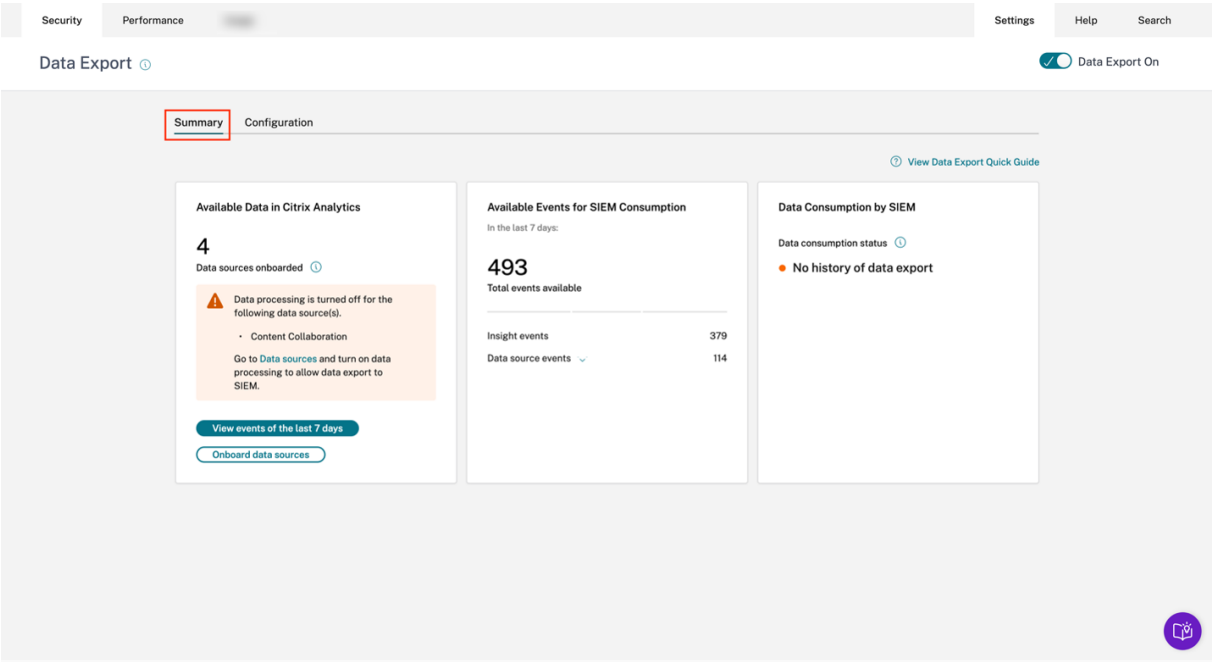


Problembehandlung bei Datenexporten

December 12, 2023

Die Ansicht “Datenexporte für Sicherheit”enthält eine Registerkarte **Zusammenfassung**, die Administratoren bei der Behebung von Problemen bei der SIEM-Integration mit Citrix Analytics unterstützt. Das **Übersichts-Dashboard** bietet einen Überblick über den Zustand und den Datenfluss, indem es die Prüfpunkte durchläuft, die den Fehlerbehebungsprozess unterstützen.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



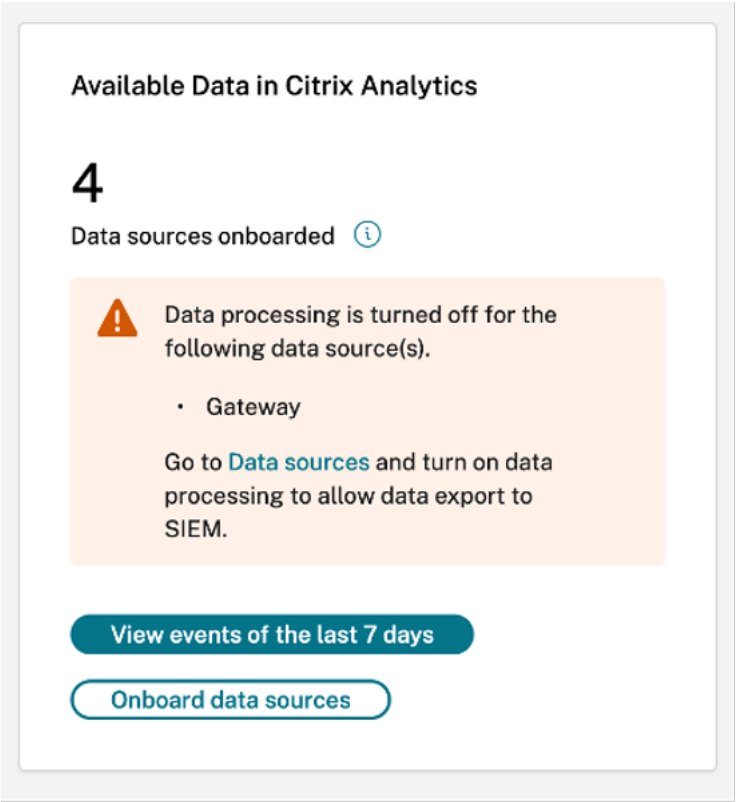
Registerkarte “Zusammenfassung”

Die Registerkarte **Zusammenfassung** bildet die Grundlage für den Self-Service-Problembehebungsworkflow in der Ansicht “Datenexporte”. Es beschreibt Ihr SIEM-Setup mithilfe dieser drei Karten:

- **Verfügbare Daten in Citrix Analytics**: Diese Karte zeigt den Status Ihrer Datenquellenkonfigurationen.
- **Verfügbare Ereignisse für die SIEM-Nutzung**: Diese Karte zeigt die Anzahl der Ereignisse an, die bereit sind, von Ihrer SIEM-Umgebung genutzt zu werden.
- **Datenverbrauch durch SIEM**: Diese Karte zeigt den Status des Datenflusses in Ihrer SIEM-Umgebung an.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Verfügbare Daten in Citrix Analytics

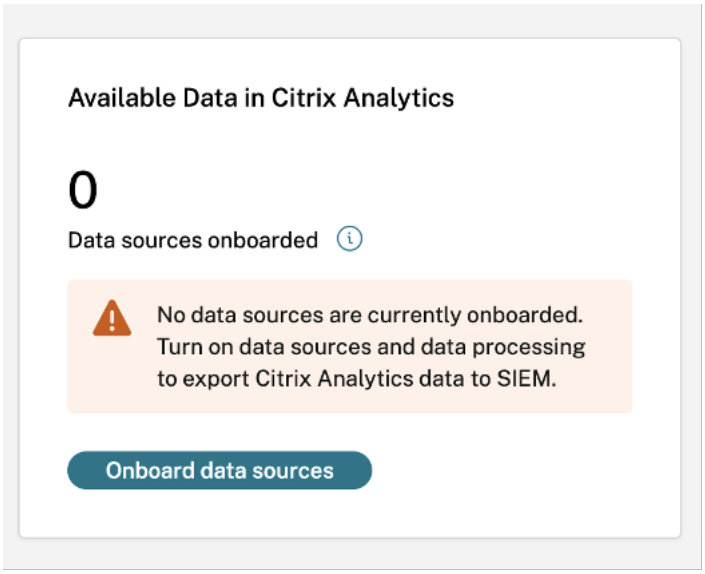


Die Karte **Verfügbare Daten in Citrix Analytics** zeigt die Anzahl der Datenquellen, die letztendlich zu SIEM-Erkenntnissen beitragen können, die in Citrix Analytics for Security integriert wurden. Derzeit werden drei Datenquellen für Datenexporte unterstützt: Apps and Desktops, Gateway und Secure Private Access. Selbst wenn diese Datenquellen integriert wurden, funktioniert der Datenexport für die Datenquellen, deren Datenverarbeitung deaktiviert ist, nicht. Eine entsprechende Warnmeldung, wie sie in der Abbildung oben dargestellt ist, wird angezeigt, wenn solche Datenquellen erkannt werden.

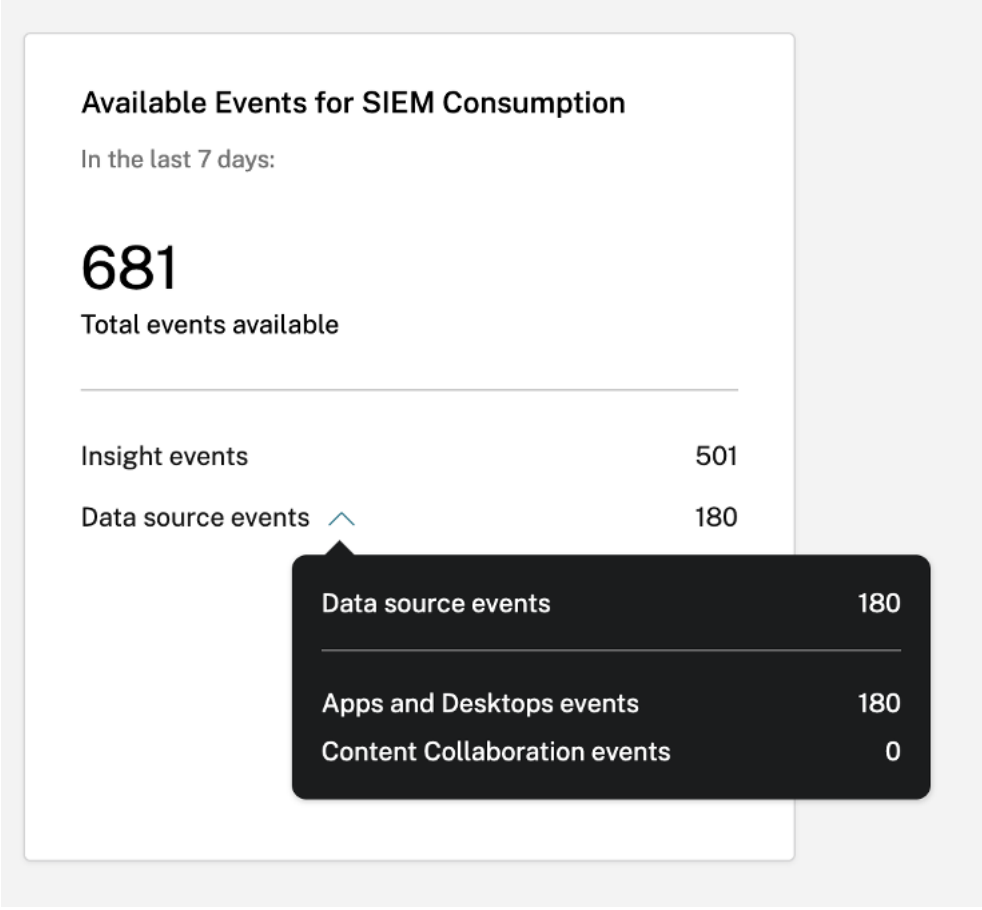
Mit der Schaltfläche **Ereignisse der letzten 7 Tage anzeigen** wird der Administrator zur Self-Service-Suchansicht weitergeleitet, in der Administratoren überprüfen können, ob Ereignisse in Citrix Analytics for Security eingegangen sind. Die Schaltfläche **Datenquellen einbinden** leitet zur Datenquellenansicht weiter, in der Sie den Onboarding-Prozess eingehend durchgehen können.

Wenn keine integrierten Datenquellen vorhanden sind, wird eine entsprechende Warnmeldung angezeigt, wie im folgenden Screenshot dargestellt:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Verfügbare Ereignisse für die SIEM-Nutzung



Auf der Karte **Verfügbare Ereignisse für den SIEM-Verbrauch** wird die Anzahl der Insight- und Datenquellenereignisse zusammen mit deren Aufschlüsselung angezeigt, die voraussichtlich in Ihre SIEM-

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Umgebung einfließen werden. Nach der Erweiterung ist auch eine weitere Aufschlüsselung der einzelnen Arten von Datenereignissen für den Export verfügbar.

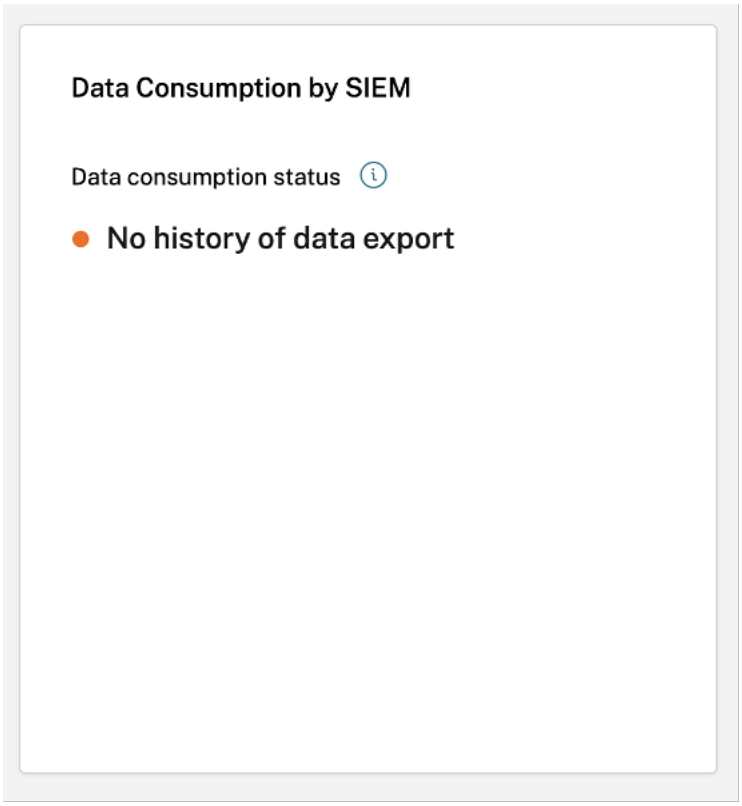
Datenverbrauch durch SIEM

Die Karte **Data Consumption by SIEM** zeigt den Zustand des von Citrix Analytics vorbereiteten Datenflusses in Ihre SIEM-Umgebung. Der Status des Datenverbrauchs basiert auf der Offset-Bewegung innerhalb Ihres **Kafka-Themas** . Sofern verfügbar, zeigt die Karte auch den Zeitstempel an, an dem der letzte erfolgreiche Datenverbrauch festgestellt wurde. Sowohl der Status des Datenverbrauchs als auch der Zeitstempel werden alle 10 Minuten aktualisiert. Klicken Sie hier, um mehr über Kafka Consumer Group/Offset Management zu erfahren.

Der Status des Datenverbrauchs kann die folgenden Zustände annehmen:

1. **Inaktiver Konsum**

   - **Keine Historie des Datenexports**: Dieser Status wird durch einen orangefarbenen Punkt dargestellt, der darauf hinweist, dass keine von Citrix Analytics vorbereiteten Daten jemals erfolgreich in Ihre SIEM-Umgebung geflogen sind.



     Das kann daran liegen -

     – Fehlerhafte/unvollständige Datenquellenkonfiguration. Die Karte **Verfügbare Daten**

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

in Citrix Analytics kann verwendet werden, um zu überprüfen, ob genügend Datenquellen vorhanden sind und ob deren Datenverarbeitung aktiviert ist, um den Export zu ermöglichen.

- Mangelnde Benutzeraktivität. Mit der Schaltfläche **Ereignisse der letzten 7 Tage anzeigen** auf der Karte **Verfügbare Daten in Citrix Analytics** können Sie überprüfen, ob keine Benutzeraktivitäten stattgefunden haben. Darüber hinaus kann die Karte **Verfügbare Ereignisse für den SIEM-Verbrauch** verwendet werden, um zu überprüfen, ob Insight- oder Datenquellenereignisse von Citrix Analytics für die Übertragung in Ihr SIEM vorbereitet wurden.
- Falsches/unvollständiges SIEM-Setup. Stellen Sie sicher, dass die Phase der Kontoeinrichtung auf der Registerkarte **Konfiguration** erfolgreich abgeschlossen wurde. Wenn die Einrichtung abgeschlossen ist, ist in der Phase der Kontoeinrichtung ein grünes Häkchen sichtbar.

  Wenn sich der Status auch nach einer erfolgreichen Kontoeinrichtung nicht ändert, überprüfen Sie die weitere Problembehandlung, indem Sie Folgendes überprüfen:

  * Firewallprobleme oder falsch konfigurierte SIEM-Einstellungen —siehe SIEM-Umgebung einrichten.
  * Probleme mit Anmeldeinformationen bei der Einrichtung eines Kafka-Kontos oder Ihrer SIEM-Umgebung —siehe SIEM-Integrationmit Kafka.

- **Kein aktiver Verbrauch festgestellt**: Dieser Status weist darauf hin, dass mindestens in den letzten 10 Minuten keine Daten erfolgreich in Ihre SIEM-Umgebung übertragen wurden. Auf der Karte wird auch der Zeitstempel der letzten erfolgreichen Übertragung von Daten angezeigt. Wie bei **Kein Verlauf des Datenexports**können Sie dieses Problem beheben, indem Sie die Karten **Verfügbare Daten in Citrix Analytics** und **Verfügbare Ereignisse für SIEM-Verbrauch** verwenden. Wenn die Benutzeraktivität ausreichend ist und die Anzahl der verfügbaren Ereignisse steigt, ist es eine gute Idee, sich auf den letzten erfolgreichen Zeitstempel zu konzentrieren, um zu überprüfen, ob nach diesem Zeitstempel Firewalländerungen oder Kennwortrotationen stattgefunden haben.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Vor mehr als 7 Tagen exportiert**: Dieser Status gibt an, dass der aktive Verbrauch auf Ihrem SIEM zuletzt vor über einer Woche festgestellt wurde. Ähnlich wie bei den beiden oben genannten Zuständen verwenden Sie die Karten **Verfügbare Daten in Citrix Analytics** und **Verfügbare Ereignisse für den SIEM-Verbrauch**, um Probleme mit Ihrem SIEM-Setup zu beheben, wenn dies der erkannte Datenverbrauchsstatus ist.

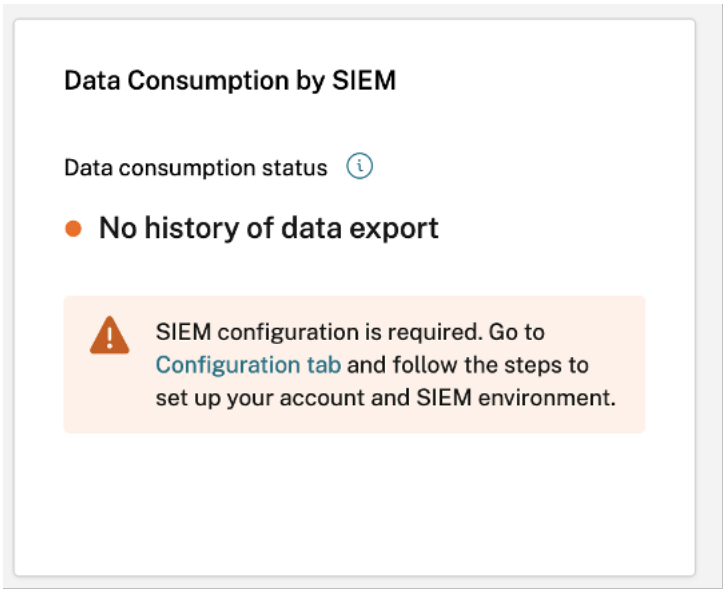
> **Hinweis**
>
> **Kafka-Aufbewahrungsrichtlinie**: In den Kafka-Themen von Citrix Analytics werden

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> Ereignisse nur für maximal 7 Tage gespeichert. Um einen möglichen Datenverlust zu vermeiden oder zu verhindern, wird empfohlen, ein Datenabfrageintervall einzurichten, das 7 Tage nicht überschreitet.

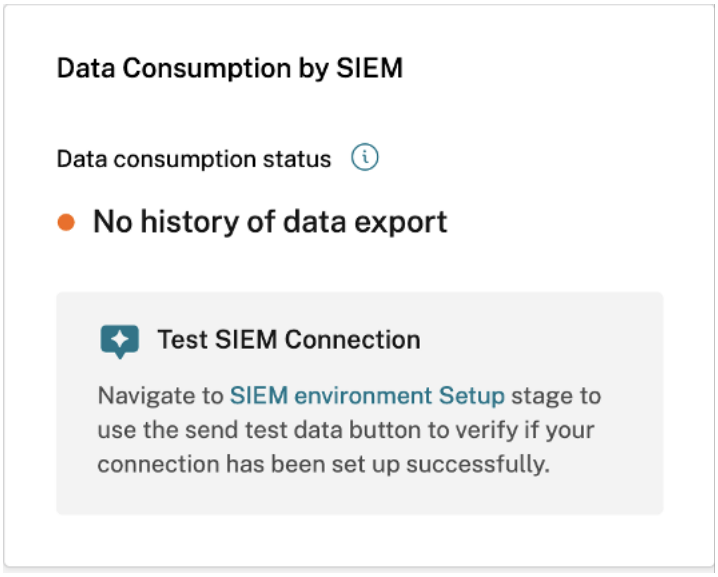
Bei inaktivem Verbrauch können Sie sich die folgenden Warnmeldungen anzeigen lassen, die Ihnen bei der Problembehebung helfen.

Wie im Fall **Keine Historie des Datenexports** hervorgehoben, fließen keine Daten in die SIEM-Umgebung, wenn das SIEM-Setup nicht abgeschlossen ist. Daher wird der Benutzer zur Registerkarte **Konfiguration** weitergeleitet, um die Kontoeinrichtung abzuschließen, wie im folgenden Screenshot gezeigt:



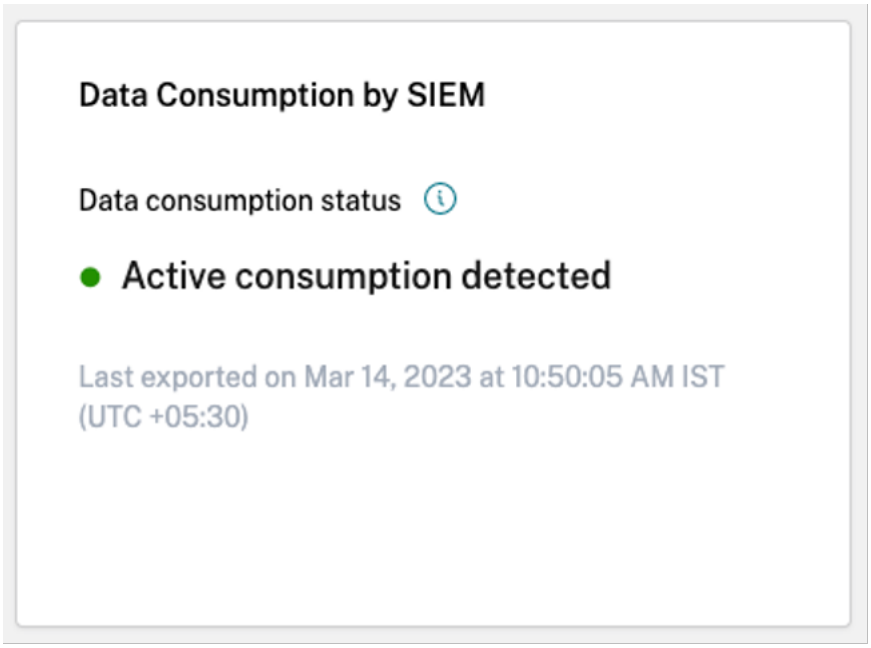
Wenn das SIEM-Setup abgeschlossen ist, kann es immer noch vorkommen, dass die Daten nicht aktiv fließen, wie im Status **Kein aktiver Verbrauch erkannt** oder vor **mehr als 7 Tagen exportiert** dargestellt wird. Daher wird dem Benutzer dringend empfohlen, zum Abschnitt **Testereignisgenerierung** zu gehen, um die SIEM-Verbindung zu testen, wie in der folgenden Warnmeldung hervorgehoben.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



2. **Aktiver Konsum**

   - **Aktiver Verbrauch erkannt**: Dieser Status zeigt an, dass auf Ihrem SIEM ein aktiver Verbrauch festgestellt wurde.

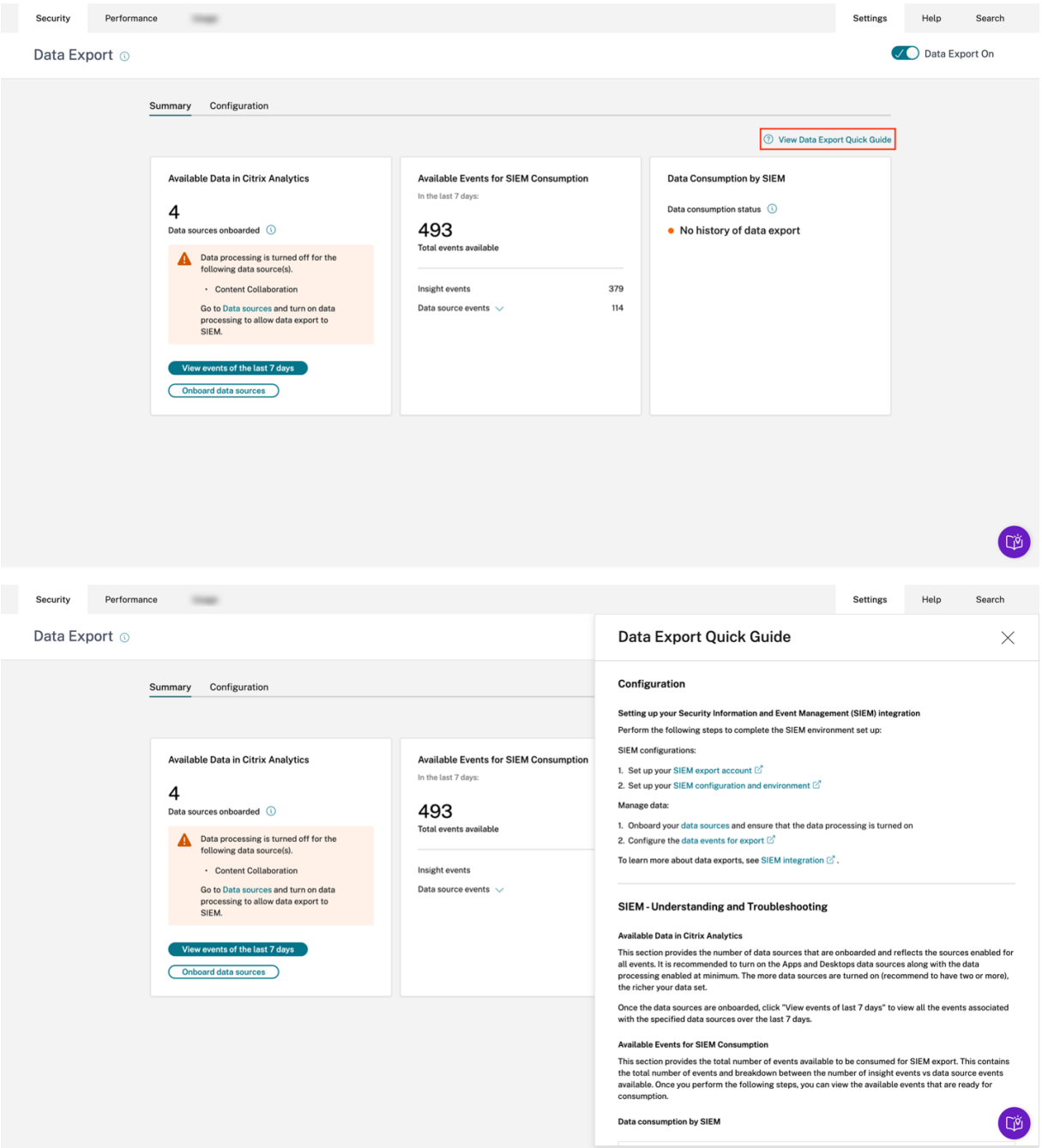


Kurzanleitung zum Datenexport

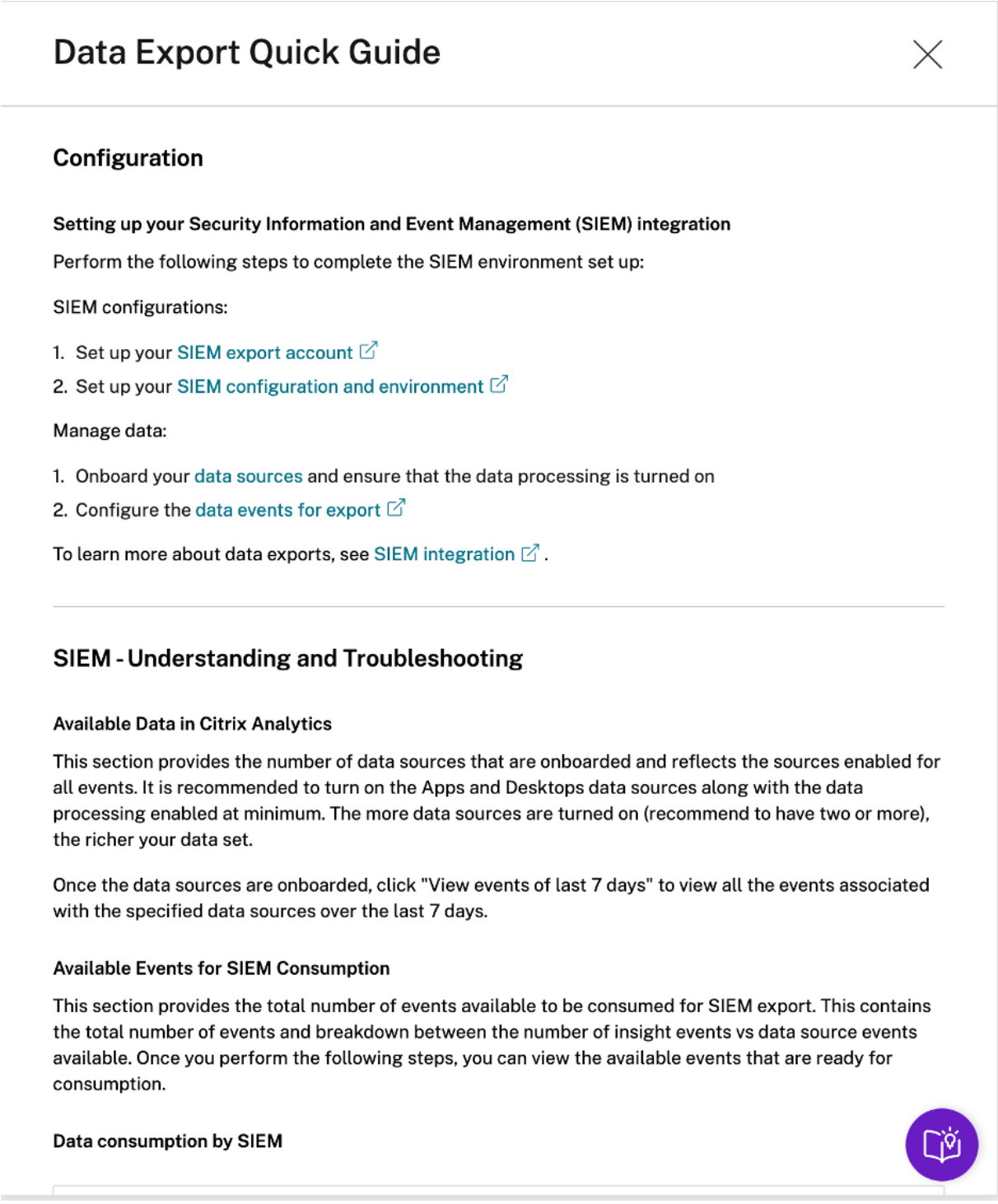
Die Registerkarte **Zusammenfassung** wird durch die **Kurzanleitung zum Datenexport** ergänzt, um die Bereitstellung, Verwaltung und Fehlerbehebung Ihrer SIEM-Setups zu vereinfachen. Die Kurzanleitung bietet nicht nur eine umfassende Anleitung zur Ansicht "Datenexport für Sicherheit", sondern

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

enthält auch nützliche Tipps zur Einrichtung und Verwaltung Ihrer SIEM-Umgebung, indem sie Links zu der entsprechenden Dokumentation enthält.



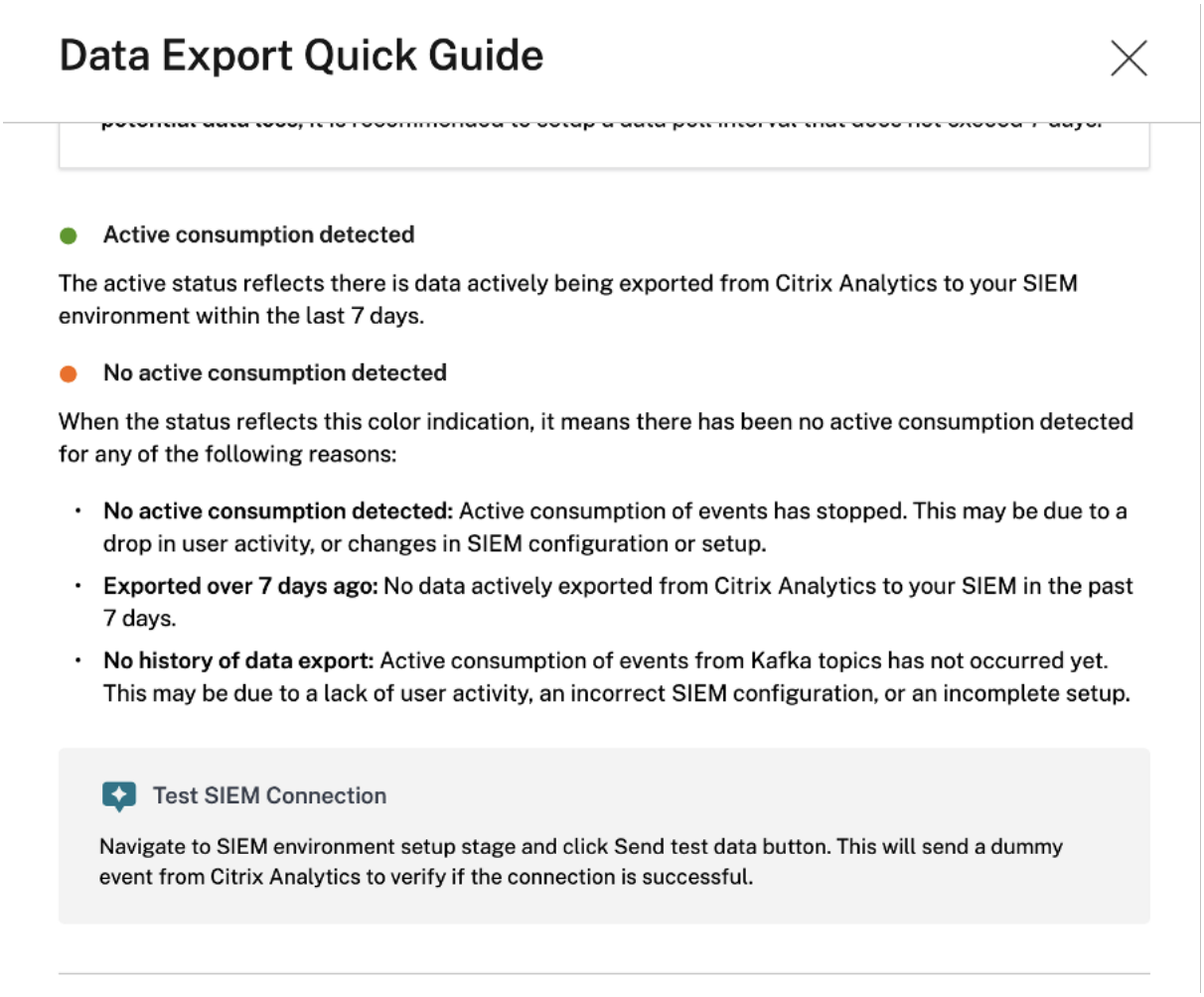
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



In der Kurzanleitung gibt es auch einen Abschnitt **SIEM-Verbindung testen**, der den Benutzer innerhalb der Einrichtungsphase der SIEM-Umgebung zur Phase “SIEM-Verbindung testen”weiterleitet. Auf diese Weise kann der Benutzer untersuchen, ob die SIEM-Integration selbst defekt ist, wodurch die Möglichkeit von Problemen mit der Verarbeitung der Ereignisse durch Citrix Analytics for Security ausgeschlossen wird. Der Benutzer kann dann die SIEM-Verbindung reparieren, um den Datenfluss

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

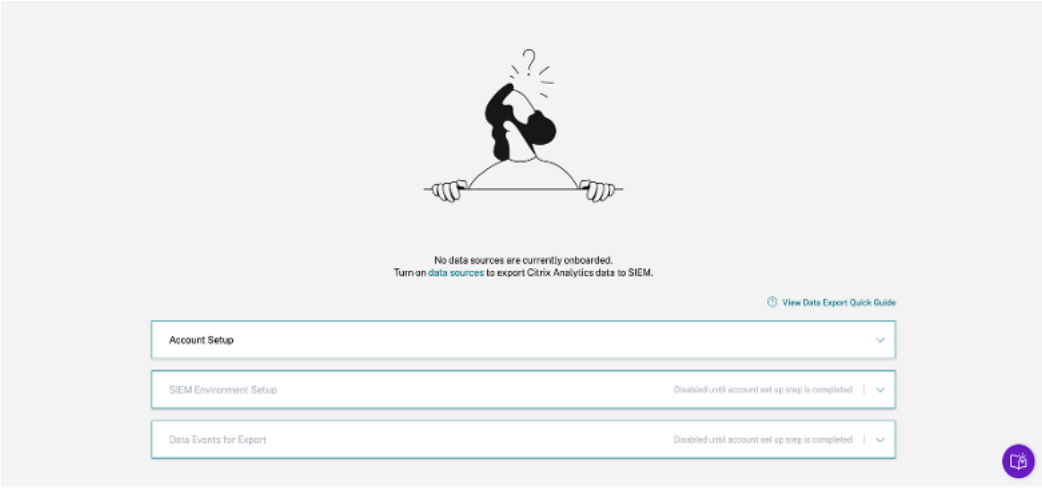
zu aktivieren.



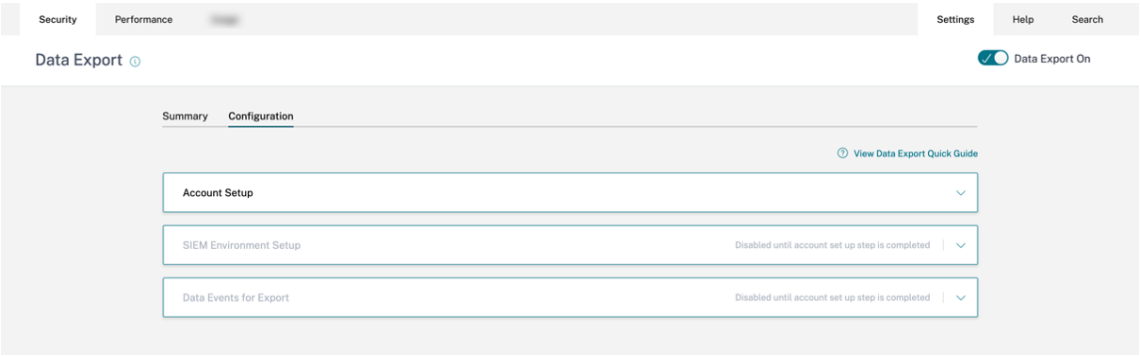
Die Registerkarte „ **Konfiguration** “führt Administratoren zwar durch die Einrichtung der Bereitstellung, bietet aber auch nützliche Tipps, Warnmeldungen und häufig auftretende Fallstricke bei der Einrichtung ihres SIEM. Entsprechende Warnungen werden angezeigt, wenn:

- Citrix Analytics stellt fest, dass keine Datenquellen integriert wurden. Es wird empfohlen, Apps and Desktops zu integrieren, um Telemetrie basierend auf Benutzeraktivitäten zu erfassen. In Ermangelung der integrierten Datenquelle wird kein Datenfluss beobachtet, obwohl Ihr SIEM-Setup möglicherweise erfolgreich durchgeführt wurde.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

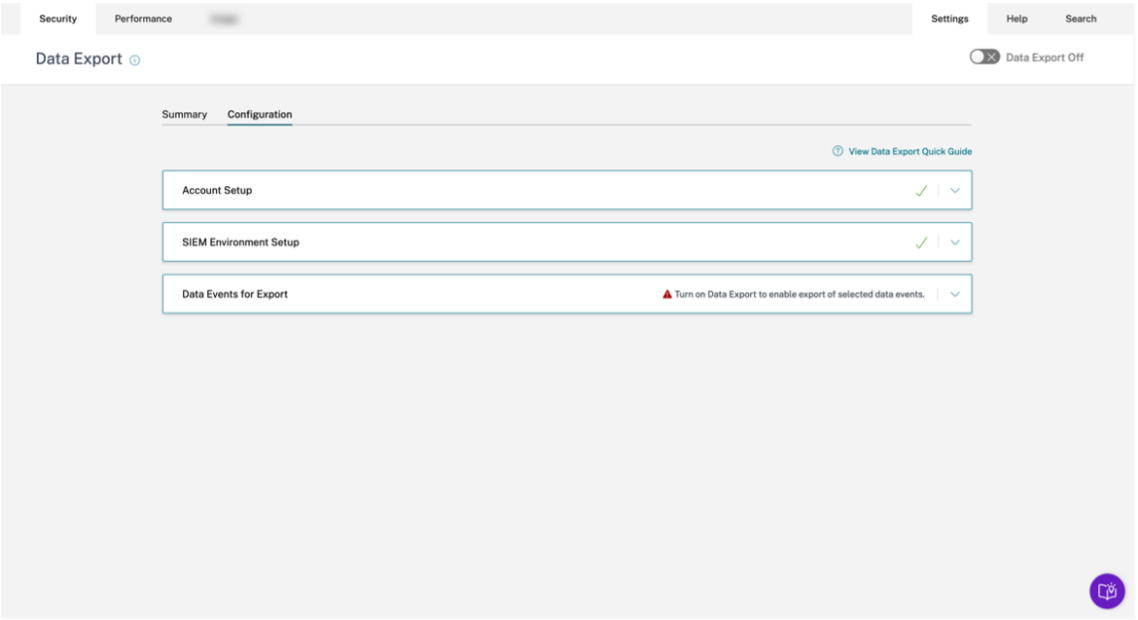


- Wie in der folgenden Abbildung dargestellt, sind die Phasen SIEM-Umgebungseinrichtung und Datenereignisse für den Export deaktiviert, bis die Kontoeinrichtung erfolgreich abgeschlossen ist.

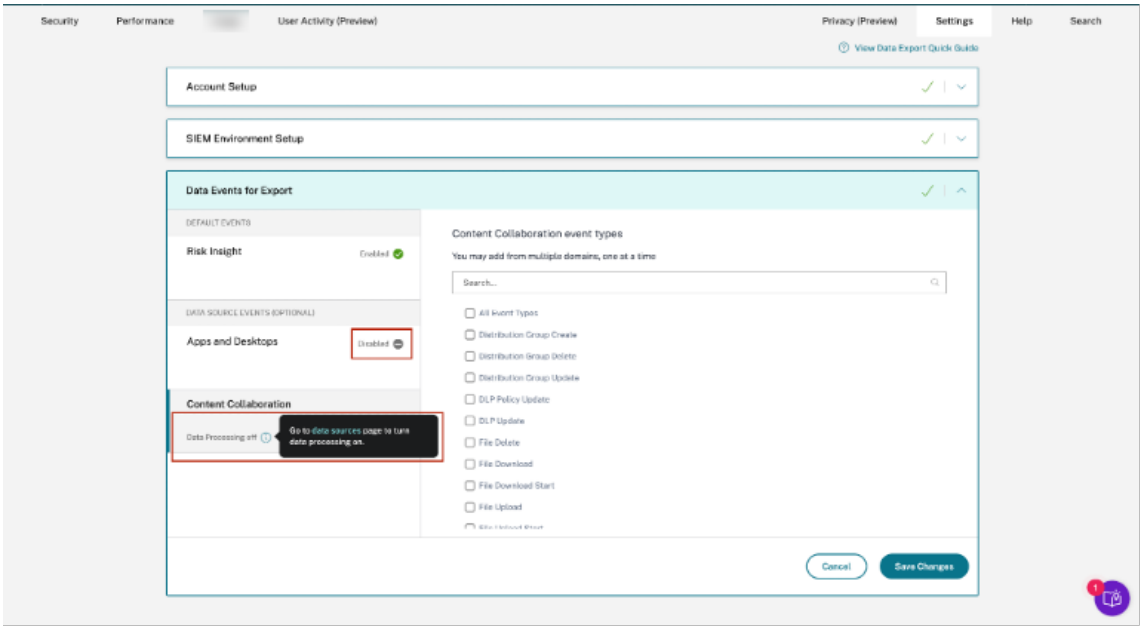


- Datenexporte wurden deaktiviert. Die Warnung in der Phase "Datenereignisse für den Export" dient als Erinnerung daran, dass Datenexporte alle Änderungen vornehmen können.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



- Wenn in der Phase „Datenereignisse für Export“der Datenexport für eine bestimmte Datenquelle deaktiviert ist, fließen keine Datenquellenereignisse an SIEM. Sie müssen dies aktivieren, indem Sie die Typen der gewünschten Datenquellenereignisse konfigurieren und auswählen. Stellen Sie außerdem sicher, dass die Datenverarbeitung für die jeweilige Datenquelle aktiviert ist, um sicherzustellen, dass die Daten Citrix Analytics erreichen.



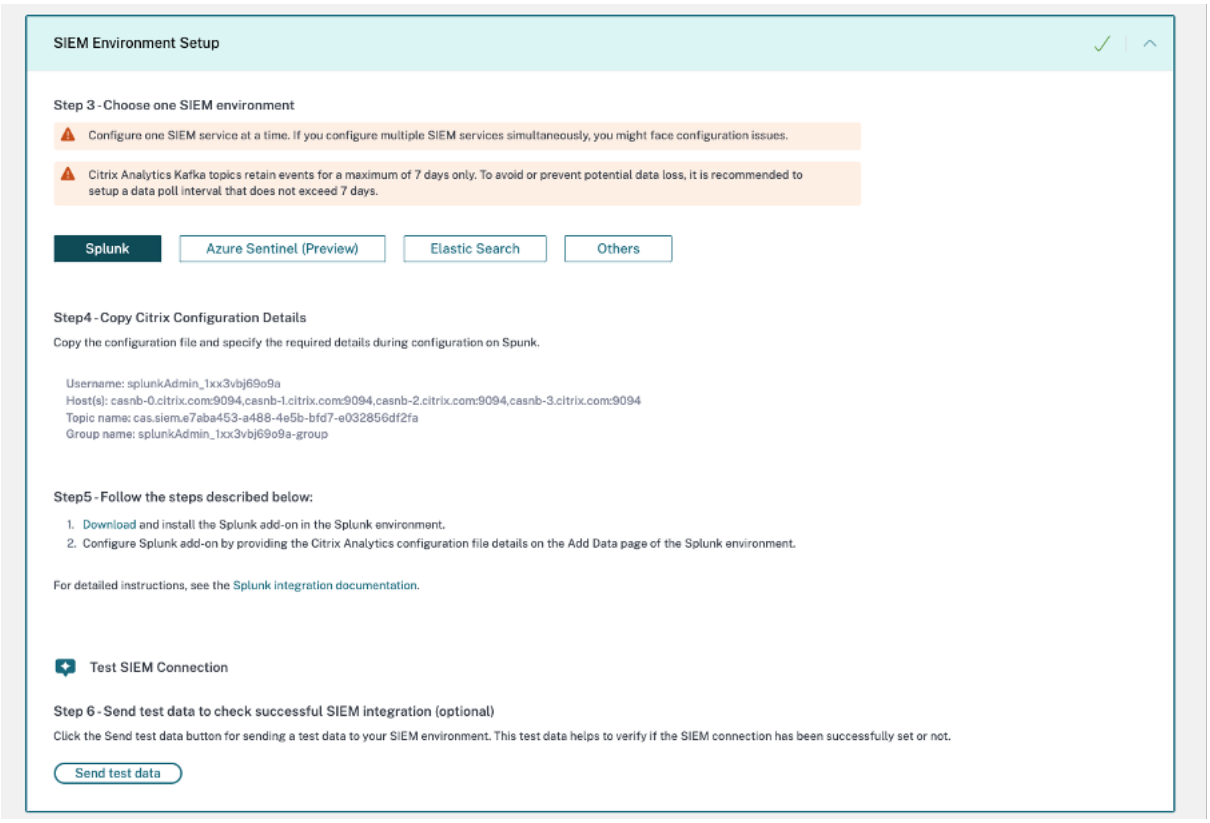
Generierung von Testereignissen

Die Generierung von Testereignissen ist Teil der **Einrichtungsphase der SIEM-Umgebung**, um die Problembehebung zu verbessern. Sobald ein Benutzer das SIEM-Setup abgeschlossen hat, bietet die

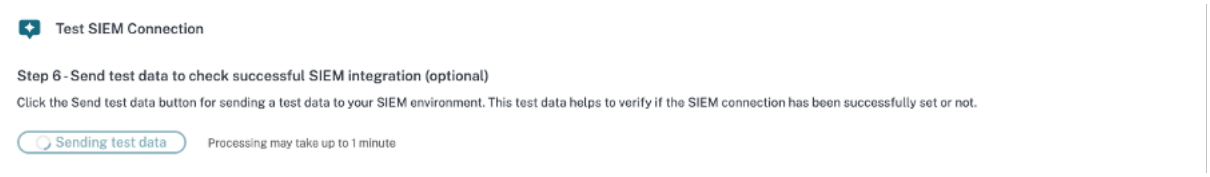
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Generierung von Testereignissen eine Möglichkeit, die SIEM-Verbindung schnell zu testen, indem ein Testereignis direkt an das Kafka-Thema des Kunden für den SIEM-Datenexport gesendet wird.

Außerdem können neue Benutzer ihre SIEM-Integration mit Citrix Analytics schnell testen, ohne explizit eine neue Datenquelle integrieren und anschließend Benutzeraktivitäten generieren zu müssen.

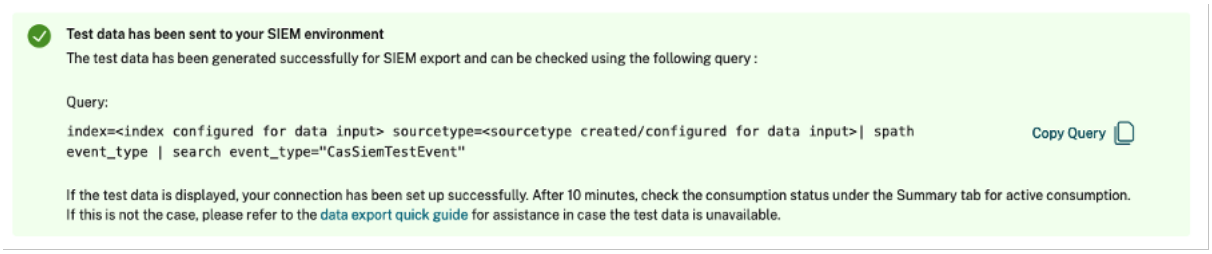


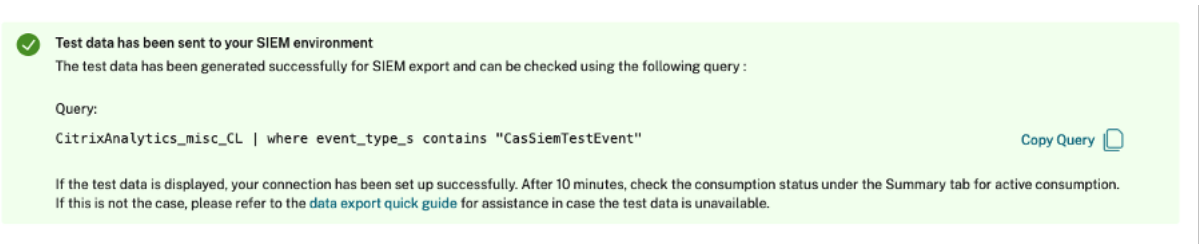
Um diese Funktion zu testen, muss der Benutzer auf die Schaltfläche **Testdaten senden** klicken. Dadurch wird ein Dummytestereignis generiert und an das SIEM-Datenexport-Kafka-Thema des Kunden gesendet. Dieser Prozess zur Generierung von Testereignissen kann bis zu 1 Minute dauern, wie im folgenden Screenshot gezeigt:



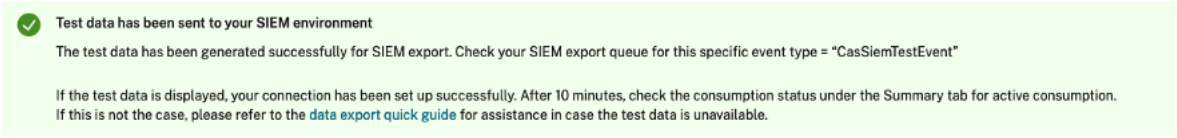
Wenn die Testereignisdaten erfolgreich in das Kunden-Kafka-Thema geschrieben wurden, wird eine Erfolgsmeldung angezeigt, die darauf hinweist, dass die SIEM-Verbindung erfolgreich ist. Abhängig von Ihrer ausgewählten Umgebung (Splunk und Sentinel) können Administratoren die Abfrage kopieren und ihre SIEM-Umgebungen auf das Testereignis überprüfen.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

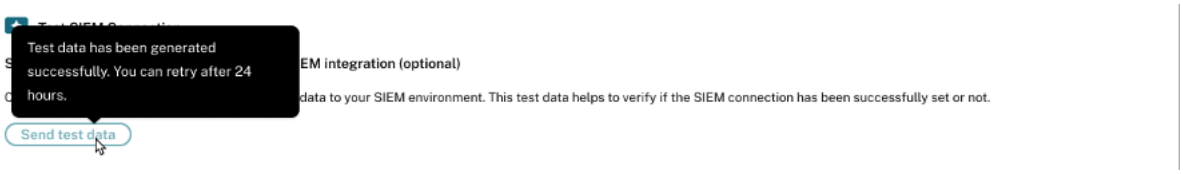




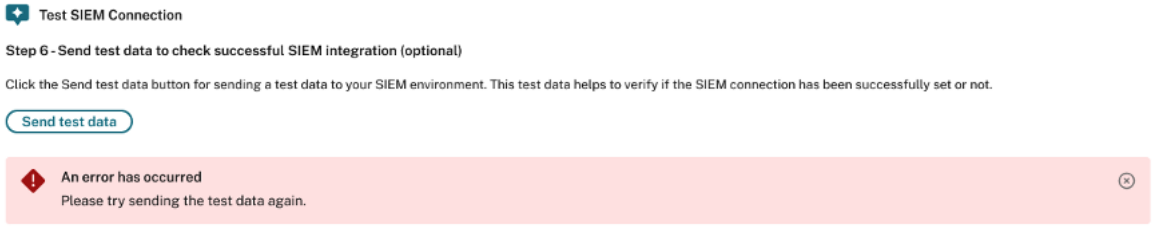
Für Elasticsearch und andere Umgebungen wird die folgende Erfolgsmeldung angezeigt.



> **Hinweis:**
>
> Sobald ein Testereignis generiert wurde, ist die Schaltfläche **Testdaten senden** für die nächsten 24 Stunden deaktiviert, und die Benutzer sehen das folgende Popup, wenn sie mit der Maus über die Schaltfläche fahren. 24 Stunden nach dem letzten Erfolgszeitstempel wird die Schaltfläche aktiviert, sodass die Benutzer die Funktionalität erneut testen können.



Wenn die Testereignisdaten nicht erfolgreich in das Kunden-Kafka-Thema geschrieben wurden, wird eine Fehlermeldung angezeigt, wie im folgenden Screenshot dargestellt. Der Benutzer kann die Daten erneut senden, um die Verbindung zu testen.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

SIEM-E-Mail-Warnung

Citrix Analytics sendet E-Mail-Benachrichtigungen, um die Administratoren über Szenarien zu informieren, die zu einer Unterbrechung des Datenflusses in ihrer SIEM-Umgebung führen könnten. Es enthält situationsbezogene Informationen über Aktivitäten, die zu vorübergehenden/permanenten sicherheitsbedingten Datenverlusten führen können. Es hilft auch dabei, sich im Self-Service-Prozess zur Fehlerbehebung für den SIEM-Datenexport zurechtzufinden.

Einige wichtige Eigenschaften dieser Reihe von E-Mail-Benachrichtigungen, die Ihnen helfen, sie in Ihrem Posteingang zu finden:

- Die E-Mail wird an Citrix Cloud-Administratoren, Security-Volladministratoren, schreibgeschützte Sicherheitsadministratoren und schreibgeschützte Sicherheits- und Leistungsadministratoren verteilt.
- Der Absender ist Citrix Cloud **donotreplynotifications@citrix.com**.
- Die Betreffzeile lautet:
  - **SIEM-Datenexport-Warnung —Das Kennwort wurde für E-Mail-Benachrichtigungen zum Zurücksetzen** des Kennworts zurückgesetzt.
  - **SIEM-Datenexport-Warnung —Der Datenfluss wurde aufgrund von E-Mail-Benachrichtigungen aufgrund von Datenflussunterbrechungen gestoppt** .

Wie aktiviere ich E-Mail-Benachrichtigungen?

Wenn Sie ein Citrix Cloud-Administrator mit benutzerdefinierten Zugriffsberechtigungen (Security Full Admin, Security Read Only Admin, Security und Performance Read Only) zur Verwaltung von Security Analytics sind, sind die E-Mail-Benachrichtigungen immer für Ihr Citrix Cloud-Konto aktiviert. Standardmäßig werden die wöchentlichen E-Mail-Benachrichtigungen an die Standardliste der Citrix Sicherheitsadministratoren gesendet. Sie können auch die Verteilerliste ändern, die diese Warnung erhält. Weitere Informationen finden Sie unter .

Wenn Sie ein Citrix Cloud-Administrator mit benutzerdefinierten Zugriffsberechtigungen (Security Full Admin, Security Read Only Admin, Security und Performance Read Only) zur Verwaltung von Security Analytics sind, sind die E-Mail-Benachrichtigungen für Ihr Citrix Cloud-Konto immer aktiviert.

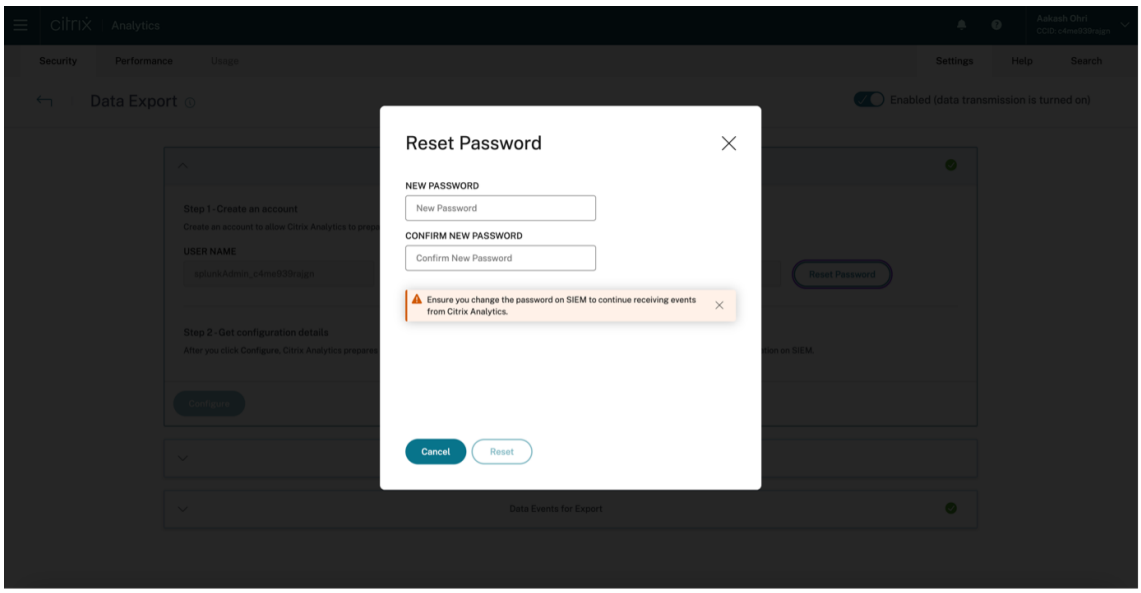
Arten von SIEM-E-Mail-Benachrichtigungen

1. **E-Mail-Benachrichtigung zum Zurücksetzen des SIEM-Kennworts**

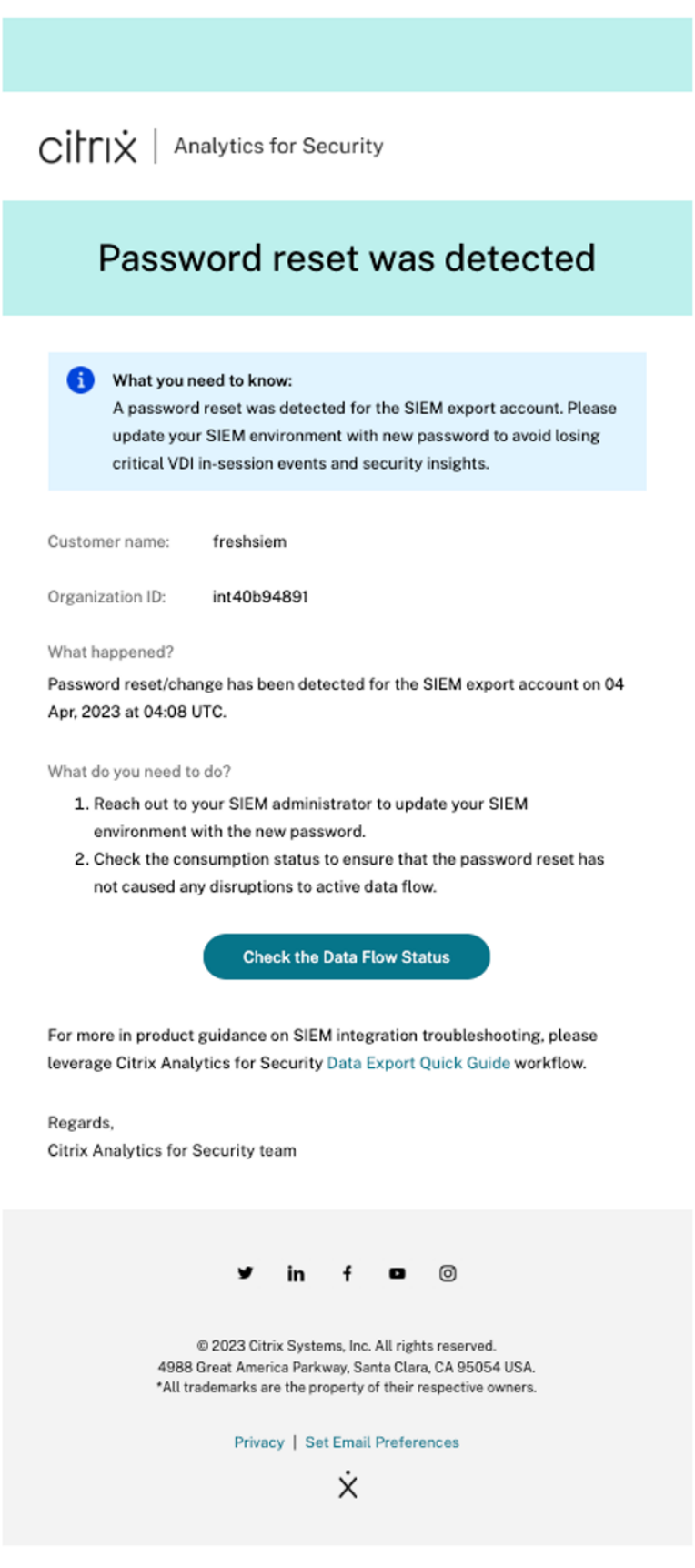
   Die Warnmeldung zum Zurücksetzen des SIEM-Kennworts wird empfangen, wenn das Kontokennwort über die Seite Datenexporte zurückgesetzt wird. Das Zurücksetzen des

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

SIEM-Kennworts allein auf der Citrix Analytics-Benutzeroberfläche kann dazu führen, dass das Kennwort nicht mit dem auf Ihrem SIEM konfigurierten Kennwort übereinstimmt. Dies führt zu einer Unterbrechung des Datenflusses. Diese E-Mail-Benachrichtigung enthält den Zeitpunkt, zu dem das Kennwort zurückgesetzt wurde. Wenn der Datenfluss unterbrochen wird, können Sie auf der Registerkarte **Zusammenfassung** überprüfen, ob der Zeitstempel „Zuletzt exportiert am“in der Nähe des Zeitstempels für das Zurücksetzen des Kennworts liegt, und somit die erforderlichen Kennwortänderungen weiterleiten. Dies verkürzt den Debugging-Prozess und hilft Ihnen, in kürzester Zeit zu einem erfolgreichen Datenfluss in Ihre SIEM-Umgebung zurückzukehren.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.



citrix | Analytics for Security

Password reset was detected

What you need to know:
A password reset was detected for the SIEM export account. Please update your SIEM environment with new password to avoid losing critical VDI in-session events and security insights.

Customer name: freshsiem

Organization ID: int40b94891

What happened?

Password reset/change has been detected for the SIEM export account on 04 Apr, 2023 at 04:08 UTC.

What do you need to do?

1. Reach out to your SIEM administrator to update your SIEM environment with the new password.
2. Check the consumption status to ensure that the password reset has not caused any disruptions to active data flow.

Check the Data Flow Status

For more in product guidance on SIEM integration troubleshooting, please leverage Citrix Analytics for Security Data Export Quick Guide workflow.

Regards,
Citrix Analytics for Security team

© 2023 Citrix Systems, Inc. All rights reserved.
4988 Great America Parkway, Santa Clara, CA 95054 USA.
*All trademarks are the property of their respective owners.

Privacy | Set Email Preferences

2. **Unterbrechung des Datenflusses für 24 Stunden E-Mail-Benachrichtigung**

   Diese E-Mail-Warnung wird gesendet, wenn der Datenfluss vom Citrix Analytics Service in Ihre SIEM-Umgebung für mehr als 24 Stunden unterbrochen ist. Die E-Mail enthält den Zeitpunkt, zu dem das letzte Ereignis exportiert wurde, sowie hilfreiche Tipps zur Fehlerbehebung, mit denen der Datenfluss wiederhergestellt werden kann. Dies wäre der richtige Zeitpunkt, um den Datenfluss schnell wieder aufzunehmen, damit keine sicherheitsrelevanten Daten verloren gehen.

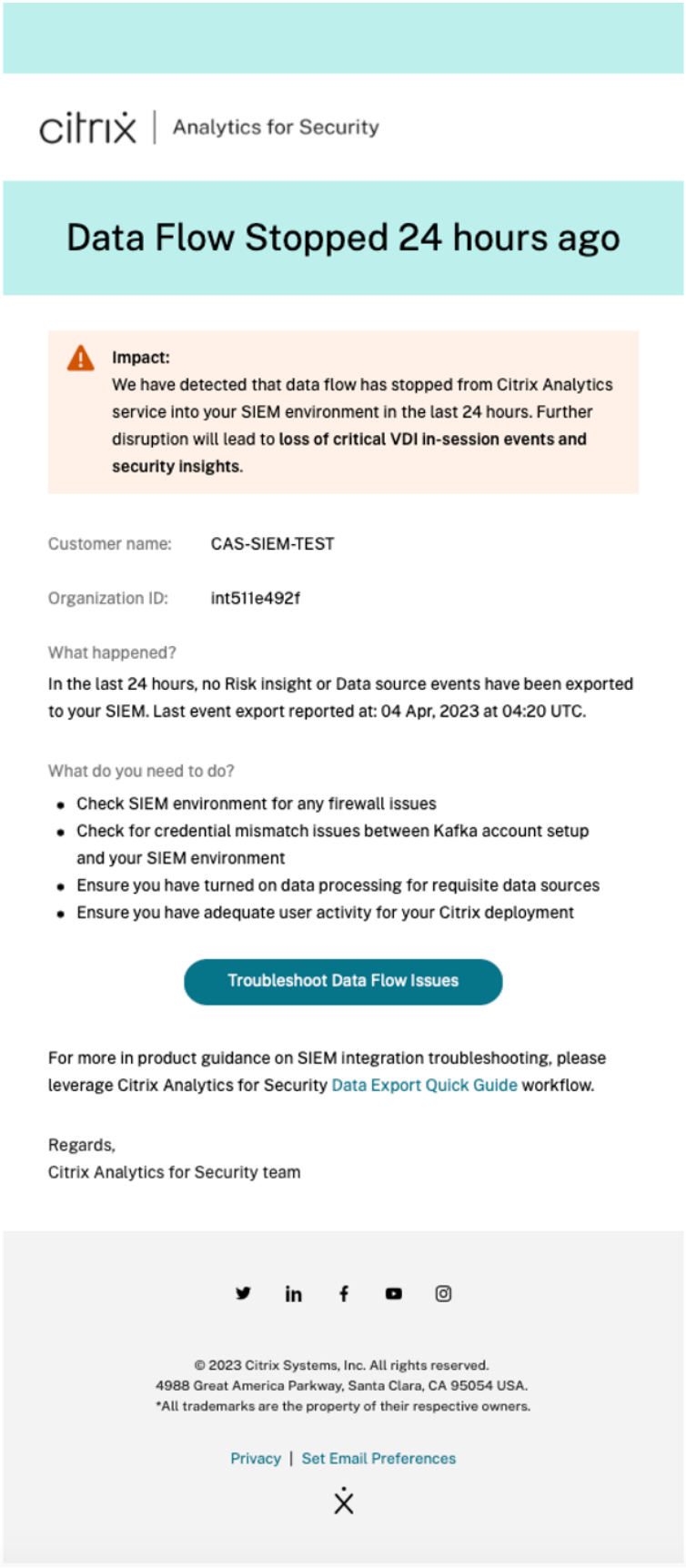
3. **Unterbrechung des Datenflusses für 7 Tage E-Mail-Benachrichtigung**

   Diese E-Mail-Warnung wird gesendet, wenn der Datenfluss vom Citrix Analytics Service in Ihre SIEM-Umgebung für mehr als 7 Tage unterbrochen ist. Da die Aufbewahrungsfrist für das Kafka-Thema des Kunden 7 Tage beträgt, ist es wichtig, die Tipps zur Fehlerbehebung zu befolgen und die Hilfe der Kurzanleitung auf der Seite **Datenexporte** in Anspruch zu nehmen, um keine weiteren Daten zu verlieren. In dieser E-Mail wird vor einem dauerhaften Verlust sicherheitsrelevanter Informationen gewarnt.

4. **Unterbrechung des Datenflusses für 30 Tage E-Mail-Benachrichtigung**

   Diese E-Mail-Warnung wird gesendet, wenn der Datenfluss vom Citrix Analytics Service in Ihre SIEM-Umgebung für mehr als 30 Tage unterbrochen ist. Inzwischen hat der Kunde die sicherheitsrelevanten Daten verloren, und es ist unerlässlich, die Funktionen zur Fehlerbehebung zu nutzen, um den Datenfluss so schnell wie möglich wiederherzustellen.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



citrix | Analytics for Security

Data Flow Stopped 24 hours ago

Impact:
We have detected that data flow has stopped from Citrix Analytics service into your SIEM environment in the last 24 hours. Further disruption will lead to **loss of critical VDI in-session events and security insights.**

Customer name: CAS-SIEM-TEST

Organization ID: int511e492f

What happened?

In the last 24 hours, no Risk insight or Data source events have been exported to your SIEM. Last event export reported at: 04 Apr, 2023 at 04:20 UTC.

What do you need to do?

- Check SIEM environment for any firewall issues
- Check for credential mismatch issues between Kafka account setup and your SIEM environment
- Ensure you have turned on data processing for requisite data sources
- Ensure you have adequate user activity for your Citrix deployment

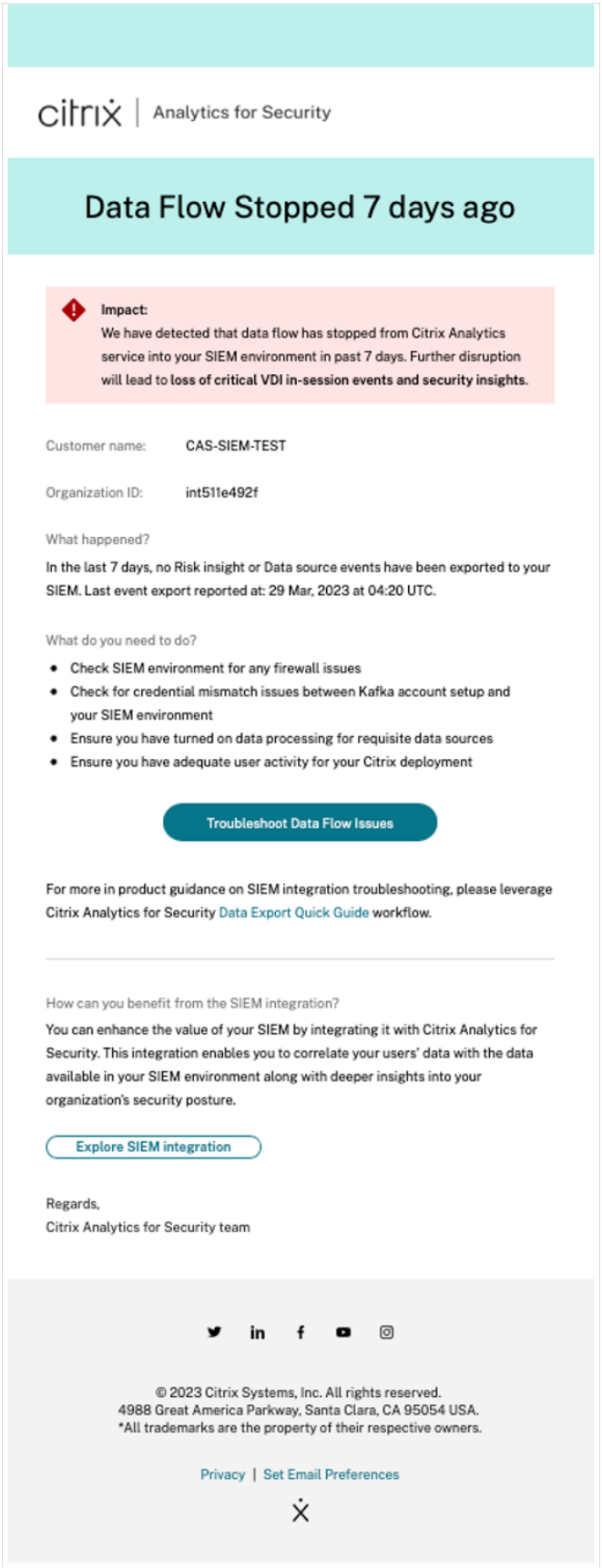
Troubleshoot Data Flow Issues

For more in product guidance on SIEM integration troubleshooting, please leverage Citrix Analytics for Security Data Export Quick Guide workflow.

Regards,
Citrix Analytics for Security team

© 2023 Citrix Systems, Inc. All rights reserved.
4988 Great America Parkway, Santa Clara, CA 95054 USA.
*All trademarks are the property of their respective owners.

Privacy | Set Email Preferences



citrix | Analytics for Security

Data Flow Stopped 7 days ago

Impact:
We have detected that data flow has stopped from Citrix Analytics service into your SIEM environment in past 7 days. Further disruption will lead to **loss of critical VDI in-session events and security insights.**

Customer name: CAS-SIEM-TEST

Organization ID: int511e492f

What happened?

In the last 7 days, no Risk insight or Data source events have been exported to your SIEM. Last event export reported at: 29 Mar, 2023 at 04:20 UTC.

What do you need to do?

- Check SIEM environment for any firewall issues
- Check for credential mismatch issues between Kafka account setup and your SIEM environment
- Ensure you have turned on data processing for requisite data sources
- Ensure you have adequate user activity for your Citrix deployment

Troubleshoot Data Flow Issues

For more in product guidance on SIEM integration troubleshooting, please leverage Citrix Analytics for Security Data Export Quick Guide workflow.

How can you benefit from the SIEM integration?

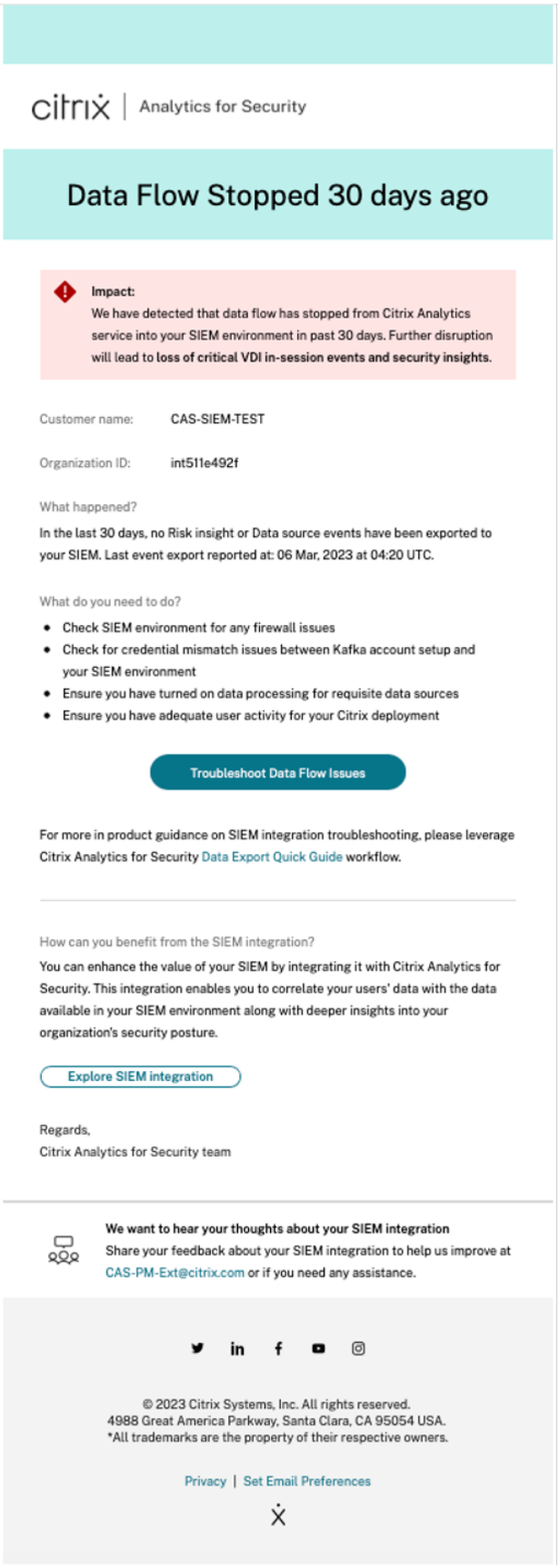
You can enhance the value of your SIEM by integrating it with Citrix Analytics for Security. This integration enables you to correlate your users' data with the data available in your SIEM environment along with deeper insights into your organization's security posture.

Explore SIEM integration

Regards,
Citrix Analytics for Security team

© 2023 Citrix Systems, Inc. All rights reserved.
4988 Great America Parkway, Santa Clara, CA 95054 USA.
*All trademarks are the property of their respective owners.

Privacy | Set Email Preferences



citrix | Analytics for Security

Data Flow Stopped 30 days ago

Impact:
We have detected that data flow has stopped from Citrix Analytics service into your SIEM environment in past 30 days. Further disruption will lead to **loss of critical VDI in-session events and security insights.**

Customer name: CAS-SIEM-TEST

Organization ID: int511e492f

What happened?

In the last 30 days, no Risk insight or Data source events have been exported to your SIEM. Last event export reported at: 06 Mar, 2023 at 04:20 UTC.

What do you need to do?

- Check SIEM environment for any firewall issues
- Check for credential mismatch issues between Kafka account setup and your SIEM environment
- Ensure you have turned on data processing for requisite data sources
- Ensure you have adequate user activity for your Citrix deployment

Troubleshoot Data Flow Issues

For more in product guidance on SIEM integration troubleshooting, please leverage Citrix Analytics for Security Data Export Quick Guide workflow.

How can you benefit from the SIEM integration?

You can enhance the value of your SIEM by integrating it with Citrix Analytics for Security. This integration enables you to correlate your users' data with the data available in your SIEM environment along with deeper insights into your organization's security posture.

Explore SIEM integration

Regards,
Citrix Analytics for Security team

We want to hear your thoughts about your SIEM integration
Share your feedback about your SIEM integration to help us improve at CAS-PM-Ext@citrix.com or if you need any assistance.

© 2023 Citrix Systems, Inc. All rights reserved.
4988 Great America Parkway, Santa Clara, CA 95054 USA.
*All trademarks are the property of their respective owners.

Privacy | Set Email Preferences

Beispiel für Sigma-Signaturen für Security Insights

December 12, 2023

Diese Seite enthält Beispielabfragen, mit denen Administratoren mithilfe von Citrix Security Analytics aussagekräftige Ergebnisse erzielen können.

Diese Beispiele decken Risiken der folgenden Kategorien ab:

- Kompromittierte Endpunkte
- Insider-Bedrohungen
- Exfiltration von Daten

Wie benutzt man diese Beispiele

Zeigen Sie die Datenquelle an und schalten Sie die Datenverarbeitung ein

Um die Datenquelle anzuzeigen, klicken Sie in der Citrix Analytics-GUI auf **Einstellungen > Datenquellen > Sicherheit**. Die **App-Site-Karte Apps und Desktops** —**Workspace** wird auf der Seite **Datenquellen** angezeigt. Klicken Sie auf **Datenverarbeitung einschalten**, damit Citrix Analytics mit der Verarbeitung von Daten für diese Datenquelle beginnen kann.

Citrix Analytics for Security sendet die folgenden zwei Arten von Risikoerkenntnissen an Ihren SIEM-Service:

- Ereignisse mit Risikoeinblicken (Standardexporte)
- Datenquellenereignisse (optionale Exporte)

Als Teil Ihrer SIEM-Umgebung sind die Risiko-Insight Event-Datenquellen verfügbar und standardmäßig immer aktiviert. Weitere Informationen finden Sie unter Datenereignisse, die aus Citrix Analytics for Security in Ihren SIEM-Dienst exportiert wurden.

Sie können entweder CAS- oder Sigma-Signaturen verwenden, um bestimmte Benutzerereignisse in Ihren Datenquellen zu überprüfen. CAS-Abfragen sind über die Self-Service-Suchseite auf Ihrer Citrix Analytics-GUI zugänglich. Die Sigma-Signaturen sind in einem einfachen oder benutzerfreundlichen Format geschrieben, wodurch sie mit verschiedenen SIEM-Umgebungen kompatibel sind.

CAS-Abfragen verwenden

Sie können die CAS-Abfrage auf der Seite **Self-Service-Suche** verwenden, um Benutzerereignisse aus verschiedenen Datenquellen zu suchen und zu filtern. Klicken Sie in Ihrer Citrix Analytics-GUI auf

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Suchen und geben Sie die Abfrage in das Suchfeld ein. Weitere Informationen finden Sie unter So verwenden Sie die Self-Service-Suche.

Sie können auch benutzerdefinierte Risikoindikatoren mit den vorhandenen Vorlagen erstellen. Um einen benutzerdefinierten Risikoindikator zu erstellen, navigieren Sie zu **Sicherheit > Benutzerdefinierte Risikoindikatoren > Indikator erstellen**. Weitere Informationen finden Sie unter Erstellen eines benutzerdefinierten Risikoindikators.

Sigma-Signaturen verwenden

Sigma ist ein benutzerfreundliches, offenes Signaturformat für die Erstellung textbasierter Abfragen, mit denen Analysten Protokollereignisse beschreiben können, sodass Erkennungen einfacher zu schreiben sind. Es gibt verschiedene Möglichkeiten, eine Sigma-Signatur in die Abfragesprache Ihres SIEM-Tools zu konvertieren.

- Sie können die von Sigma angebotenen CLI-Tools und Python-SDKs verwenden. Weitere Informationen zur Sigma-Signatur finden Sie unter Verwendung von Regeln.
- Sie können öffentliche Tools wie die Sigma Translation Engine von uncoder.io verwenden, die ein kostenloses Kontingent bietet.

Informationen zu den verschiedenen Risikoeinblicken finden Sie in den folgenden Anwendungsfällen für benutzerdefinierte Indikatoren:

- Nicht genehmigter Browser
- Nicht genehmigtes Betriebssystem
- Nicht genehmigte Workspace-App-Versionen
- Nicht autorisierte Betriebssysteme außerhalb der Zulassungsliste
- Nicht autorisierte IP-Adresse oder Subnetze
- Nicht autorisierte virtuelle Apps
- Ungewöhnliche Desktop-Namen
- Bestimmte Anwendung überwachen
- Drucken aus SaaS-Apps
- Verwendung der Zwischenablage in SaaS-Apps

Kompromittierte Endpunkte

November 16, 2023

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Nicht genehmigter Browser

Dies passiert, wenn ein Benutzer versucht, von einem Browsertyp oder einer Version aus auf Inhalte zuzugreifen, die nach den IT-Richtlinien des Unternehmens oder aufgrund von Sicherheitslücken nicht zulässig sind.

Details

Datenquelle: Apps und Desktops (Workspace-App)

CAS-Abfrage

```
Event-Type = "Session.Logon" AND Browser-Name !~ "<Browser-Name>"
<!--NeedCopy-->
```

Das Session.Logon-Ereignis wird ausgelöst, wenn ein Benutzer seine Anmeldeinformationen eingibt und sich bei seiner App- oder Desktopsitzung anmeldet.

Sigma-Signatur

```
author: Citrix
date: 2023/01/31
description: This occurs when a user accesses content from an
    authorized browser which might cause an undesirable event or action
    through the internet.
detection:
  condition: index_selection and selection and not filter
  filter:
  - browser_name|contains: '<Browser-Name>'
  index_selection:
    source: cas_siem_consumer://<env>_<tenant_identifier>
  selection:
  - occurrence_event_type: Session.logon
logsource:
  product: citrixanalytics
  service: security
title: Access from unauthorized browser
<!--NeedCopy-->
```

Nicht genehmigte Betriebssysteme

Dies passiert, wenn ein Benutzer versucht, auf ein Gerät mit einem Betriebssystemtyp oder einer Version zuzugreifen, die nach den IT-Richtlinien Ihres Unternehmens oder aufgrund von Sicherheitslücken nicht zulässig ist.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Details

Datenquelle: Apps und Desktops (Workspace-App)

CAS-Abfrage

```
Event-Type = "Session.Logon" AND OS-Name ~ "<OS-Name>" AND OS-Version =
    "<OS-Version>" AND OS-Extra-Info = "<OS-Extra-Info>"
<!--NeedCopy-->
```

Sigma-Signatur

```
author: Citrix
date: 2023/01/31
description: This occurs when a user attempts to access apps from
   servers with blocked listed operating systems.
detection:
  condition: index_selection and selection
  filter_null: []
  index_selection:
    source: cas_siem_consumer://<env>_<tenant_identifier>
  selection:
    occurrence_event_type: Session.logon
    os_name|contains: '<OS-Name>'
    os_version: '<OS-Version>'
    os_extra_info: '<OS-Extra-Info>'
logsource:
  product: citrixanalytics
  service: security
title: Unauthorized operating systems in block list
<!--NeedCopy-->
```

Nicht autorisierte IP-Adresse oder Subnetze

Dies passiert, wenn ein Benutzer versucht, von einer IP-Adresse oder einem Bereich aus zuzugreifen, die oder der von den IT-Richtlinien Ihres Unternehmens als nicht autorisiert gekennzeichnet ist.

Details

Datenquelle: Apps und Desktops (Workspace-App)

CAS-Abfrage

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
Event-Type = "Session.Logon" AND Client-IP = "<XX.YY.ZZ.*>"
<!--NeedCopy-->
```

Sigma-Signatur

```
author: Citrix
date: 2023/01/31
description: This occurs when a user accessing content from an
    unauthorized IPs which might cause an undesirable event or action
    through the internet.
detection:
  condition: selection and not filter_null and filter
  filter:
  - client_ip: '<IP>'
  filter_null:
  - client_ip: null
  selection:
  - occurrence_event_type: Session.Logon
logsource:
  product: citrixanalytics
  service: security
title: Access from unauthorized IP
<!--NeedCopy-->
```

Nicht autorisierte Betriebssysteme außerhalb der Zulassungsliste

Dies passiert, wenn ein Benutzer versucht, auf Anwendungen von Servern zuzugreifen, die Betriebssysteme außerhalb der Zulassungsliste hosten.

Details

Datenquelle: Apps und Desktops (Workspace-App)

CAS-Abfrage

```
Event-Type = "Session.Logon" AND OS-Name !~ "<OS-Name>" AND OS-Version
    != "<OS-Version>" AND OS-Extra-Info != "<OS-Extra-Info>"
<!--NeedCopy-->
```

Sigma-Signatur

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
author: Citrix
date: 2023/01/31
description: Unauthorized operating systems outside allow list
detection:
  condition: selection and not filter_null and not filter_os and not
     filter_os_version and not filter_os_extra
  filter_os:
  - os_name|contains: '<OS INFO>'
  filter_os_version:
  - os_version: '<OS Version>'
  filter_os_extra:
  - os_extra_info: '<OS Extra Info>'
  filter_null:
  - os_name: null
  - os_version: null
  - os_extra_info: null
  selection:
  - occurrence_event_type: Session.Logon
logsource:
  product: citrixanalytics
  service: security
title: Unauthorized operating systems outside allow list
<!--NeedCopy-->
```

Nicht genehmigte Workspace-App-Versionen

Dies passiert, wenn ein Benutzer versucht, auf eine Workspace-App-Version zuzugreifen, die keine unterstützte Clientversion ist. In solchen Fällen müssen Benutzer ihren Client auf eine unterstützte Version aktualisieren. Weitere Informationen finden Sie unter Support von Client-Versionen.

Details

Datenquelle: Apps und Desktops (Workspace-App)

CAS-Abfrage

```
Event-Type = "Session.Logon" AND Client-Type IN ("Windows", "Macintosh"
   , "Unix/Linux") AND Workspace-App-Version != "20*" AND Workspace-App
   -Version != "21*"
<!--NeedCopy-->
```

Sigma-Signatur

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
author: Citrix
date: 2023/01/31
description: Unsupported Workspace app versions
detection:
  condition: selection and not filter_null and filter_product and not
     filter_product_version
  filter_product:
  - product: ['Windows', 'Mac', '<Other type>']
  filter_product_version:
  - product_version|contains: ['<Product Version1>', '<Product Version2
     >']
  filter_null:
  - product: null
  - product_version: null
  selection:
  - occurrence_event_type: Session.Logon
logsource:
  product: citrixanalytics
  service: security
title: Unsupported Workspace app versions
<!--NeedCopy-->
```

Insider-Bedrohungen

November 16, 2023

Ungewöhnliche Desktop-Namen

Dies tritt auf, wenn der Benutzer versucht, einen Desktop zu starten, der nicht als normal angesehen wird.

Details

Datenquelle: Apps und Desktops (Workspace-App)

CAS-Abfrage

```
Event-Type = "Session.Logon" AND Session-Launch-Type = "desktop" AND
   App-Name ~ "<Desktop Name>"
<!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Sigma-Signatur

```
author: Citrix
date: 2023/01/31
description: Unusual desktop names
detection:
  condition: selection1 and selection2 and not filter_null and
     filter_app_name
  filter_app_name:
  - app_name|contains: '<App Name>'
  filter_null:
  - app_name: null
  selection1:
  - occurrence_event_type: Citrix.EventMonitor.AppStart
  selection2:
  - launch_type: 'desktop'
logsource:
  product: citrixanalytics
  service: security
title: Unusual desktop names
<!--NeedCopy-->
```

Spezifischen Prozess überwachen

Dies passiert, wenn der Benutzer eine veröffentlichte Anwendung startet, die sich in der Überwachungsliste befindet. Der Zweck könnte darin bestehen, die Nutzung bestimmter veröffentlichter Anwendungen zu überwachen.

Details

Datenquelle: Apps und Desktops (Sitzungsaufzeichnung)

CAS-Abfrage

```
Event-Type = "Citrix.EventMonitor.AppStart" AND App-Name IN ("<App-Name
   -1>", "<App-Name-2>")
<!--NeedCopy-->
```

Sigma-Signatur

```
author: Citrix
date: 2023/01/31
description: Monitor specific process
detection:
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
  condition: selection and not filter_null and filter_app_name
  filter_app_name:
  - app_name: ['<App-Name1>', '<App-Name2>']
  filter_null:
  - app_name: null
  selection:
  - occurrence_event_type: Citrix.EventMonitor.AppStart
logsource:
  product: citrixanalytics
  service: security
title: Monitor specific process
<!--NeedCopy-->
```

Nicht autorisierte virtuelle Apps

Dies tritt auf, wenn der Benutzer auf nicht autorisierte virtuelle Apps zugreift.

Details

Datenquelle: Apps und Desktops (Workspace-App)

CAS-Abfrage

```
Event-Type = "App.Start" AND App-Name IN ("<App-Name1>", "<App-Name2>")
<!--NeedCopy-->
```

Sigma-Signatur

```
date: 2023/01/31
description: Unauthorized virtual apps
detection:
  condition: selection and not filter_null and filter_app_name
  filter_app_name:
  - app_name: ['<App-Name1>', '<App-Name2>']
  filter_null:
  - app_name: null
  selection:
  - occurrence_event_type: App.Start
logsource:
  product: citrixanalytics
  service: security
title: Unauthorized virtual apps
<!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Datenexfiltration

November 16, 2023

Drucken aus SaaS-Apps

Dies tritt auf, wenn eine Datei aus einer SaaS-Anwendung gedruckt wird, aus der das Drucken nicht zulässig ist. Es erkennt potenzielle Datenexfiltration durch Druckvorgänge in SaaS-Anwendungen.

Details

Datenquelle: Apps und Desktops (Citrix Enterprise Browser)

CAS-Abfrage

```
Event-Type = "App.SaaS.File.Print" AND SaaS-App-Name = "<App-Name>"
<!--NeedCopy-->
```

Sigma-Signatur

```
author: Citrix
date: 2023/01/31
description: Printing from SaaS apps
detection:
  condition: selection and not filter_null and filter_saas_app_name
  filter_saas_app_name:
  - saas_app_name: '<App-Name>'
  filter_null:
  - saas_app_name: null
  selection:
  - occurrence_event_type: App.SaaS.File.Print
logsource:
  product: citrixanalytics
  service: security
title: Printing from SaaS apps
<!--NeedCopy-->
```

Verwendung der Zwischenablage in SaaS-Apps

Dies tritt auf, wenn eine Aktivität zum Ausschneiden, Kopieren oder Einfügen von einer SaaS-Anwendung aus ausgeführt wird. Es erkennt potenzielle Datenexfiltrationen aus SaaS-Anwendungen

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

in Ihrem Unternehmen, indem es die Zwischenablage überwacht.

Details

Datenquelle: Apps und Desktops (Citrix Enterprise Browser)

CAS-Abfrage

```
Event-Type = "App.SaaS.Clipboard" AND Clipboard-Result = "success" AND
    Clipboard-Operation IN ( "copy" , "cut" )
<!--NeedCopy-->
```

Sigma-Signatur

```
author: Citrix
date: 2023/01/31
description: Clipboard usage on SaaS apps
detection:
  condition: selection and not filter_null and
     filter_clipboard_details_result and filter_clipboard_operation
  filter_clipboard_details_result:
  - clipboard_details_result: 'success'
  filter_clipboard_operation:
  - clipboard_operation: ['cut', 'copy', '<Other Operation>']
  filter_null:
  - clipboard_operation: null
  - clipboard_details_result: null
  selection:
  - occurrence_event_type: App.SaaS.Clipboard
logsource:
  product: citrixanalytics
  service: security
title: Clipboard usage on SaaS apps
<!--NeedCopy-->
```

Benutzerdashboard

February 9, 2024

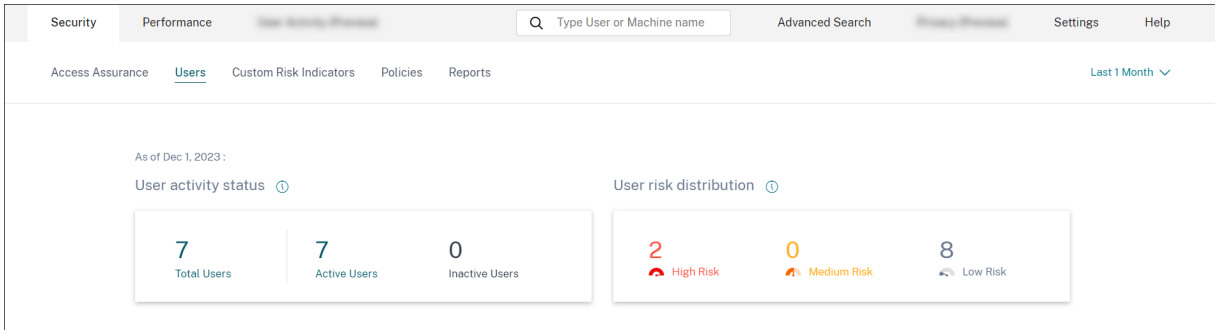
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Übersicht

Das **Benutzerdashboard** ist der Ausgangspunkt für die Analyse des Benutzerverhaltens und die Bedrohungsprävention.

Dieses Dashboard bietet Einblick in Benutzerverhaltensmuster in einer Organisation. Mithilfe dieser Daten können Sie proaktiv Verhalten überwachen, erkennen und kennzeichnen, das nicht der Norm entspricht, wie z. B. Phishing- oder Ransomware-Angriffe.

Um das Benutzer-Dashboard anzuzeigen, gehen Sie zu **Sicherheit > Benutzer**. Das Benutzer-Dashboard enthält die folgenden Abschnitte:



- **Benutzeraktivstatus**: Verteilung der Gesamtzahl der aktiven und inaktiven Benutzer.
- **Verteilung des Benutzerrisikos**: Verteilung der aktiven, inaktiven Benutzer und der Gesamtzahl der Benutzer sowie Verteilung der Benutzer mit hohem, mittlerem und niedrigem Profil auf der Grundlage ihres höchsten berechneten Risikowerts im ausgewählten Zeitraum.
- **Top-Benutzer**: Top-Benutzer werden nach ihrem Risikowert sortiert und nach „Alle Benutzer“, „Privilegierten Benutzern“und „Watchlist-Benutzern“segmentiert.
- **Risikokategorien**: Zeigt die Risikokategorien an, die Citrix Analytics unterstützt. Risikoindikatoren mit ähnlichen Verhaltensmustern werden in Kategorien eingeteilt.
- **Risikoindikatoren und Maßnahmen**: Verteilung der Risikoindikatoren und Maßnahmen, dargestellt über einen ausgewählten Zeitraum, auf alle Benutzer in Ihrer Organisation.
- **Zugriffsübersicht**: Fasst die Gesamtzahl der Versuche zusammen, die Benutzer unternommen haben, auf die Ressourcen innerhalb Ihrer Organisation zuzugreifen.
- **Richtlinien und Aktionen**: Zeigt die fünf wichtigsten Richtlinien und Aktionen an, die auf Benutzerprofile angewendet wurden.
- **Risikoindikatoren**: Zeigt die fünf wichtigsten Risikoindikatoren in Ihrem Unternehmen an.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Status der Benutzeraktivität

Gesamtzahl der Benutzer in Ihrer Organisation, die die Datenquellen verwenden, für die Sie Analytics aktiviert haben. Sie haben möglicherweise eine Risikobewertung, die mit ihrem Konto verknüpft ist oder auch nicht. Diese Kachel zeigt die Anzahl der aktiven Benutzer. Aktive Benutzer sind Benutzer, bei denen Ereignisse innerhalb des ausgewählten Zeitraums erkannt wurden. Sie können auf das Dropdownmenü mit dem Status der Benutzeraktivität klicken, um die Verteilung der Gesamtzahl der Benutzer in aktive und inaktive Benutzer anzuzeigen.

- Benutzer insgesamt: Gesamtzahl der Benutzer im ausgewählten Zeitraum.
- Aktive Benutzer: Benutzer, deren Ereignisse im ausgewählten Zeitraum erkannt wurden.
- Inaktive Benutzer: Benutzer, für die im ausgewählten Zeitraum keine Ereignisse erkannt wurden.

Die Gesamtzahl der Benutzer im Benutzer-Dashboard kann **höher** sein als die Anzahl der riskanten Benutzer, da nicht erwartet wird, dass alle Benutzer riskant sind.

> **Hinweis**
>
> Auf der Seite **Benutzer** wird die Gesamtzahl der Benutzer der letzten 30 Tage unabhängig vom ausgewählten Zeitraum angezeigt.

Facetten

Filtern Sie die Benutzerereignisse basierend auf den folgenden Kategorien:

- **Risikobewertung**: Benutzerereignisse, die auf Einstufungen mit hohem, mittlerem Risiko, niedrigem Risiko und Nullrisiko basieren.
- **Benutzer**: Benutzerereignisse basierend auf Administratorrechten, Executive-Rechten und Watchlist-Benutzern.
- **Ermittelte Datenquellen**: Benutzerereignisse basierend auf der Datenquelle, die Sie eingebunden haben.

Suchfeld

Verwenden Sie das Suchfeld, um nach Ereignissen für die Benutzer zu suchen. Sie können Operatoren in Ihrer Abfrage verwenden, um den Fokus Ihrer Suche einzugrenzen. Informationen zu den gültigen Operatoren, die Sie in Ihrer Abfrage verwenden können, finden Sie unter Self-Service-Suche.

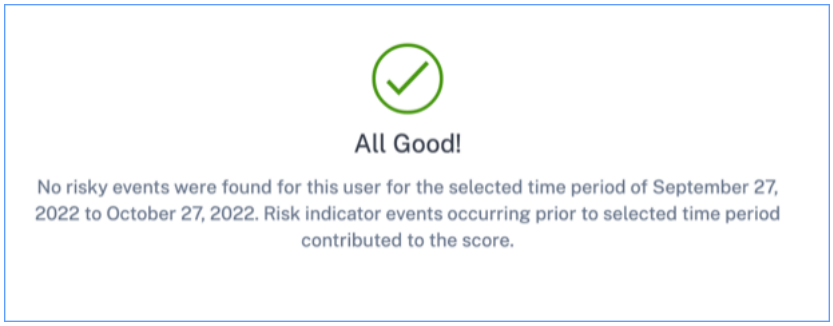
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Neuestes Ergebnis

Der Risiko-Score bestimmt das Risiko, das ein Benutzer für eine Organisation für einen bestimmten Zeitraum darstellt. Der Risiko-Score-Wert ist dynamisch und variiert basierend auf der Analyse des Benutzerverhaltens. Basierend auf der neuesten Risikobewertung kann ein Benutzer in eine der folgenden Kategorien fallen: Benutzer mit hohem Risiko, Benutzer mit mittlerem Risiko, Benutzer mit geringem Risiko und Benutzer mit Nullrisikobewertung.

User

Liste aller von Analytics entdeckten Benutzer. Wählen Sie einen Benutzernamen aus, um die Benutzerinformationen und die Risikozeitleiste für den Benutzer anzuzeigen. Möglicherweise hat der Benutzer einen Risikoindikator ausgelöst. Wenn mit diesem Benutzer keine riskanten Ereignisse verbunden sind, wird die folgende Meldung angezeigt.



Wenn mit einem Benutzer gefährliche Ereignisse verbunden sind, sehen Sie die Risikoindikatoren auf seiner Risikozeitleiste. Wählen Sie den Benutzer aus, um seinen Risikozeitplananzuzeigen.

Ein Benutzer kann als `privileged` markiert und zur Watchlist hinzugefügt werden.

Datenquelle entdeckt

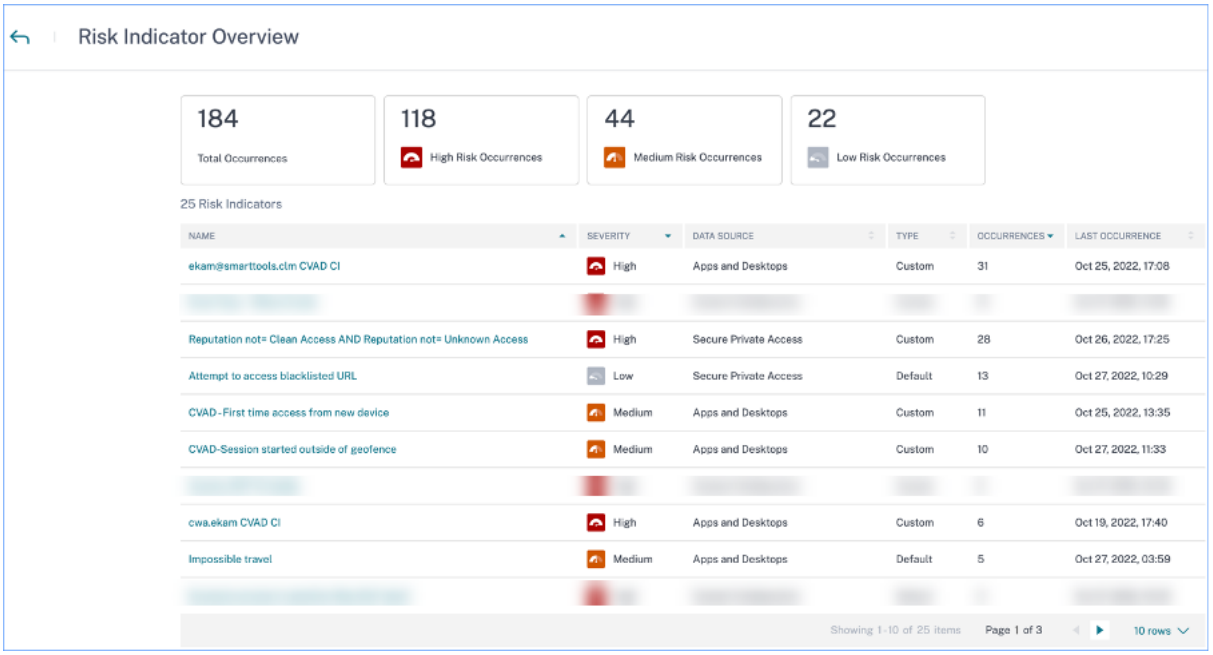
Die einem Benutzer zugeordnete Datenquelle. Wenn ein Benutzer die Datenquelle aktiv verwendet, erhält Analytics die Benutzerereignisse von dieser Datenquelle. Um Benutzerereignisse zu empfangen, müssen Sie die Datenverarbeitung auf der Datenquell-Sitekarte aktivieren, die auf der Seite **Datenquellen** verfügbar ist.

Ausgelöste Indikatoren

Gibt die Anzahl der Risikoindikatoren an, die für die ausgewählte Dauer von Benutzern ausgelöst wurden. Klicken Sie auf die Kachel **Ausgelöste Indikatoren**, um die Details der Risikoindikatoren anzuzeigen. Die Tabelle mit den Risikoindikatoren enthält die folgenden Angaben:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

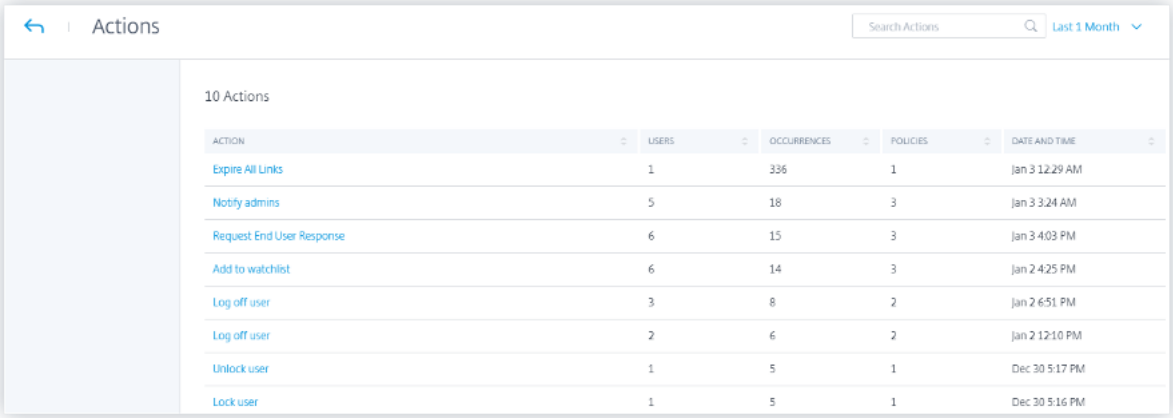
- **Name**: Der Name des Risikoindikators.
- **Schweregrad**: Der Schweregrad des mit dem Ereignis verbundenen Risikos. Das Risiko kann hoch, mittel oder niedrig sein.
- **Datenquelle**: Die Datenquelle, für die die Risikoindikatorvorlage gilt.
- **Typ**: Art des Risikoindikators. Ein Risikoindikator kann Standard oder benutzerdefiniertsein.
- **Vorkommen:**Die Häufigkeit, mit der ein Risikoindikator für einen Benutzer ausgelöst wird. Wenn Sie den Zeitraum auswählen, ändern sich die Vorkommnisse des Risikoindikators basierend auf der Zeitauswahl.
- **Letztes Vorkommen**: Zeigt das Datum und die Uhrzeit des letzten Vorfalls an.



Angewendete Maßnahmen

Gibt die Anzahl der Aktionen an, die für die ausgewählte Dauer benutzerübergreifend angewendet wurden. Dazu gehören die manuell von den Administratoren ausgeführten Aktionen und die richtliniengesteuerten Aktionen. Klicken Sie auf die Kachel **Angewendete Aktion**, um die Aktionsdetails anzuzeigen. In diesem Abschnitt werden die Aktionen nicht angezeigt, die Sie manuell auf die Benutzerprofile angewendet haben.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

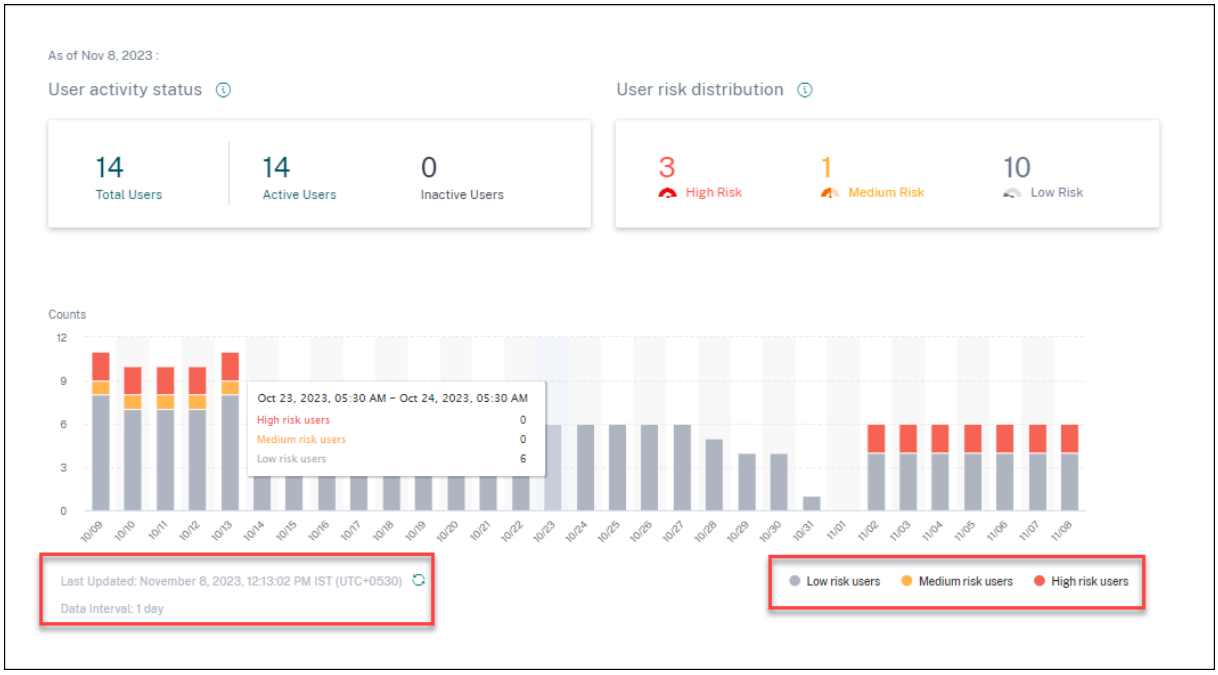


Die **Aktionstabelle** enthält die folgenden Informationen:

- **Aktion**: Name der Aktion, die gemäß der Richtlinie angewendet wurde.
- **Benutzer**: Anzahl der Benutzer, auf die die Aktion angewendet wurde.
- **Vorkommen**: Anzahl der Vorkommen der Aktion.
- **Datum und Uhrzeit**: Datum und Uhrzeit der angewendeten Aktion.

Bearbeitete Ereignisse

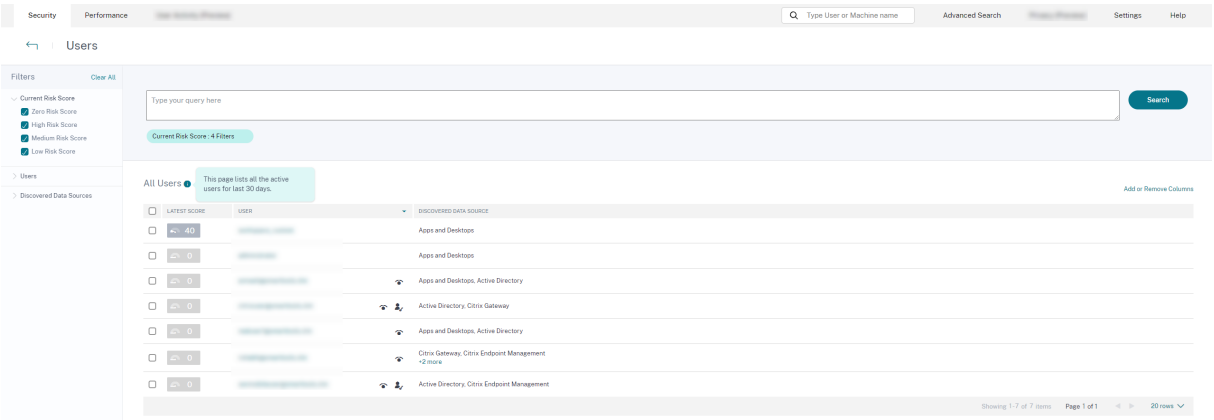
Gesamtzahl der Benutzerereignisse, die von Ihren verbundenen Datenquellen empfangen und von Analytics verarbeitet wurden.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Verteilung des Benutzerrisikos

Sie können die Anzahl der Benutzer mit hohen, mittleren und niedrigen Profilen auf der Grundlage ihrer höchsten berechneten Risikobewertung im ausgewählten Zeitraum anzeigen. Unter den Gesamtzahlen zeigt ein Balkendiagramm, wie sich die Verteilung der Benutzer mit niedrigem, mittlerem und hohem Risiko im Laufe der Zeit verändert hat.



Das Risikoniveau ist in drei Farbcodes unterteilt.

- **Rot** —Steht für Benutzer mit hohem Risiko.
- **Orange** —Steht für Benutzer mit mittlerem Risiko.
- **Grau** —Steht für Benutzer mit geringem Risiko.

Sie können die Anzahl riskanter Benutzer (hoch, mittel und niedrig) für einen bestimmten Zeitraum anzeigen, während Sie mit der Maus auf die Farbleisten zeigen. Sie können die zuletzt aktualisierten Details (Datum und Uhrzeit) mit den Datenintervallinformationen anzeigen. Klicken Sie auf eine Farbleiste, um die Risikobenutzer in diesem Zeitraum anzuzeigen. Klicken Sie auf die Aktualisierungsoption, um die aktualisierten Daten zu erhalten.

Riskante Benutzer

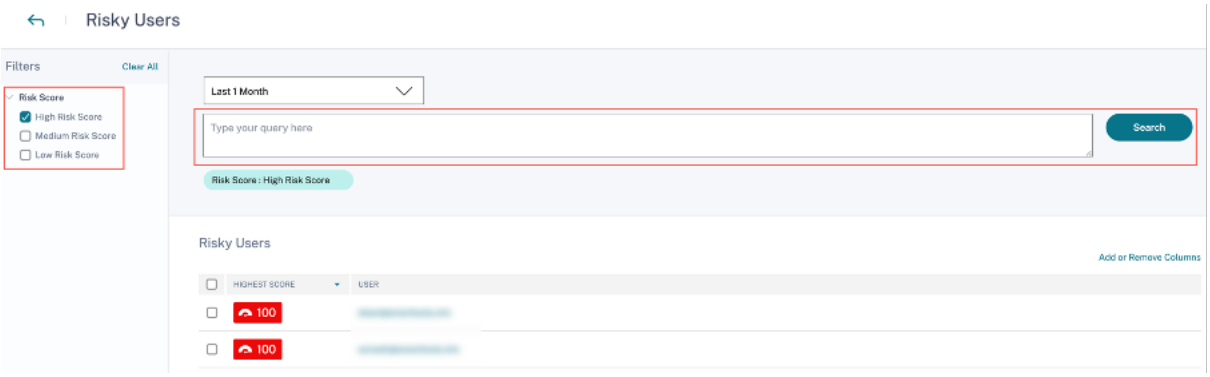
Riskante Benutzer sind Benutzer, denen riskante Ereignisse zugeordnet sind und die mindestens einen Risikoindikator ausgelöst haben. Das Risiko, das ein Benutzer für einen bestimmten Zeitraum für das Netzwerk darstellt, wird durch die mit dem Benutzer verbundene Risikobewertung bestimmt. Der Risiko-Score-Wert ist dynamisch und basiert auf Analysen des Benutzerverhaltens.

Das Risiko jedes Benutzers wird im Laufe der Zeit auf der Grundlage der Benutzeraktivitäten regelmäßig aktualisiert. Daher kann es sein, dass ein Benutzer zu einem bestimmten Zeitpunkt ein mittleres oder hohes Risiko hat, das Risiko jedoch später auf ein niedrigeres Risikoniveau sinkt. Basierend auf der Risikobewertung kann ein riskanter Benutzer in eine der folgenden Kategorien fallen:

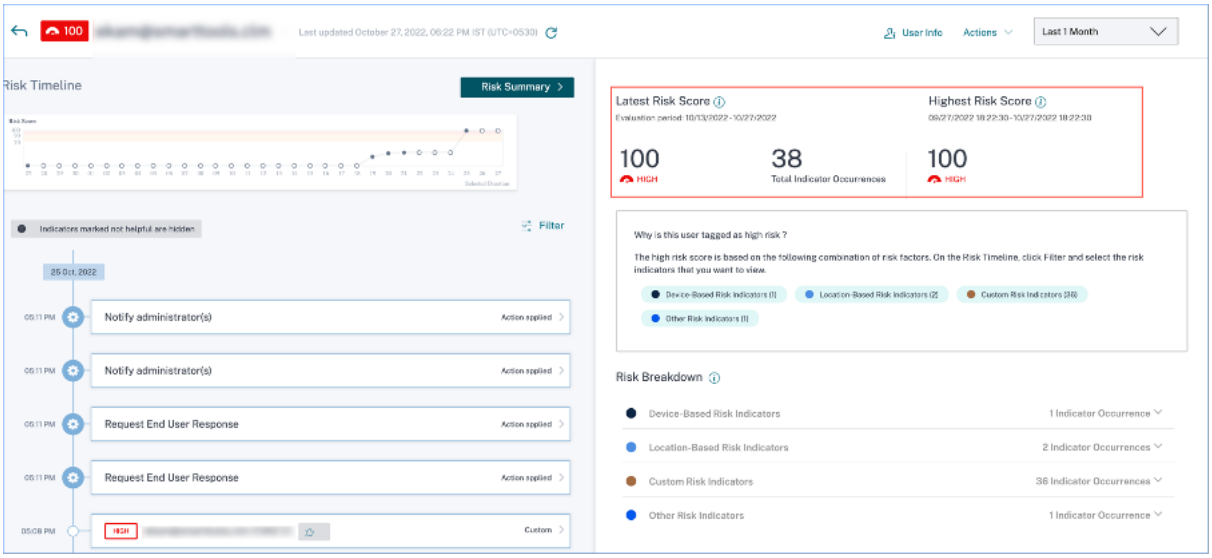
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Hohes Risiko
- Mittleres Risiko
- Niedriges Risiko

Auf der Seite **Riskante Benutzer** können Sie die Facetten verwenden, um nach den mit dem ausgewählten Zeitraum verknüpften Risikoniveaus zu filtern, und die Suchleiste, um nach einem oder mehreren bestimmten Benutzern zu suchen.



Klicken Sie auf die E-Mail-ID des Benutzers, um die Seite mit der **Risikozeitleiste** für diesen bestimmten ausgewählten Benutzer anzuzeigen. Auf dieser Seite werden die Risikoindikatoren zusammen mit den Angaben zur **neuesten** und **höchsten Risikobewertung** auf der Grundlage des ausgewählten Zeitraums angezeigt.

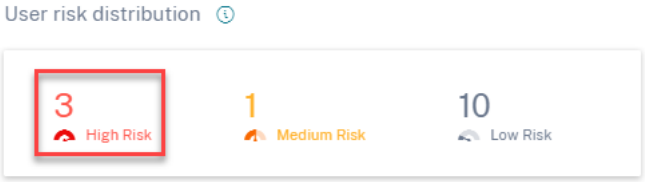


Hohes Risiko

Benutzer mit Risikowerten zwischen 90 und 100. Diese Benutzer haben mehrere Verhaltensweisen an den Tag gelegt, die auf moderate bis schwere Risikofaktoren zurückzuführen sind und eine unmittelbare Bedrohung für das Unternehmen darstellen könnten.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

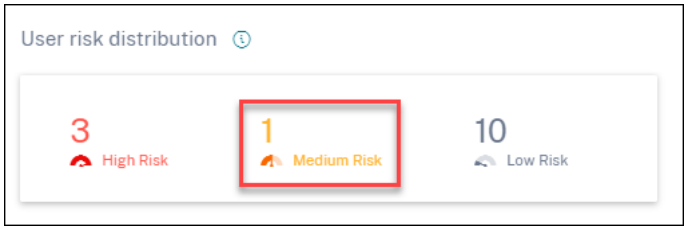
Im **Benutzerdashboard** können Sie die Anzahl der Benutzer mit hohem Risiko auf der Grundlage der höchsten berechneten Risikobewertung im ausgewählten Zeitraum anzeigen.



Klicken Sie auf die Option **Hohes Risiko**, um die Seite **Riskante Benutzer** aufzurufen. Auf der Seite werden die Details zu den Benutzern mit hohem Risiko angezeigt.

Mittleres Risiko

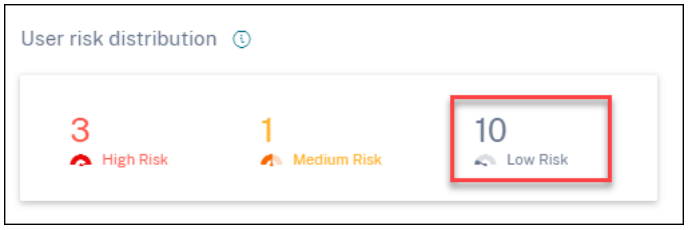
Benutzer mit Risikowerten zwischen 70 und 89. Diese Benutzer haben in der Regel eine oder mehrere Aktivitäten, die potenziell verdächtig und/oder anomal erscheinen und die es wert sein könnten, genau beobachtet zu werden.



Klicken Sie auf die Option **Mittleres Risiko**, um die Seite **Riskante Benutzer** aufzurufen. Auf der Seite werden die Details zu Benutzern mit mittlerem Risiko angezeigt.

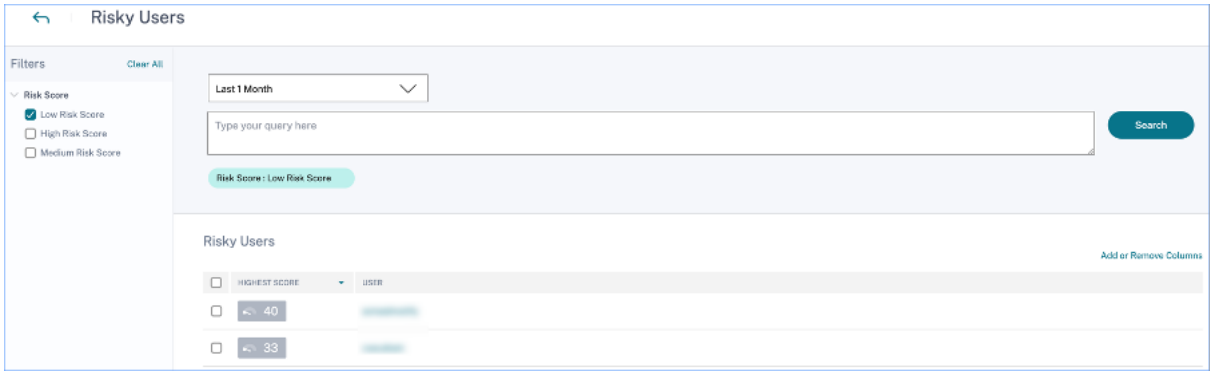
Niedriges Risiko

Benutzer mit Risikowerten zwischen 1 und 69. Bei diesen Benutzern gibt es mindestens einen Risikoindikator, der ein ungewöhnliches oder unerwartetes Verhalten widerspiegelt, der jedoch nicht ausreicht, um eine seriösere Risikoklassifizierung zu rechtfertigen.



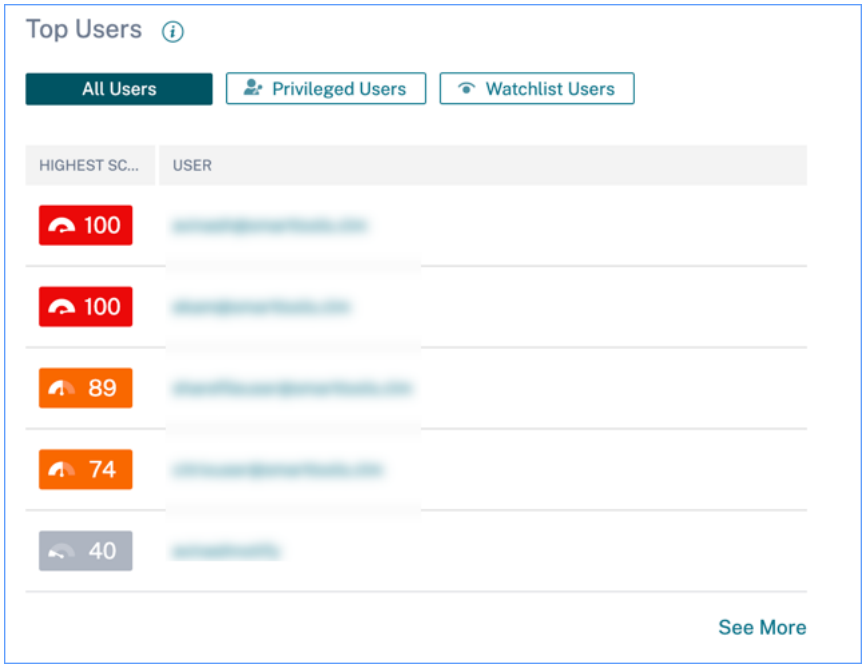
Klicken Sie auf die Option **Niedriges Risiko**, um die Seite **Riskante Benutzer** aufzurufen. Auf der Seite werden die Details zu Benutzern mit geringem Risiko angezeigt.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Top-Nutzer

Sie können sich die Top-Benutzer in verschiedenen Benutzerkategorien anzeigen lassen, sortiert nach den höchsten Risikobewertungen für den ausgewählten Zeitraum. In der folgenden Tabelle mit den häufigsten **Benutzern** werden die fünf Benutzer mit dem höchsten Risiko (alle Benutzer, Benutzer mit bevorzugter Berechtigung und Beobachtungsliste) anhand ihrer für den ausgewählten Zeitraum berechneten Risikobewertung und nicht anhand der neuesten Risikobewertung angezeigt.



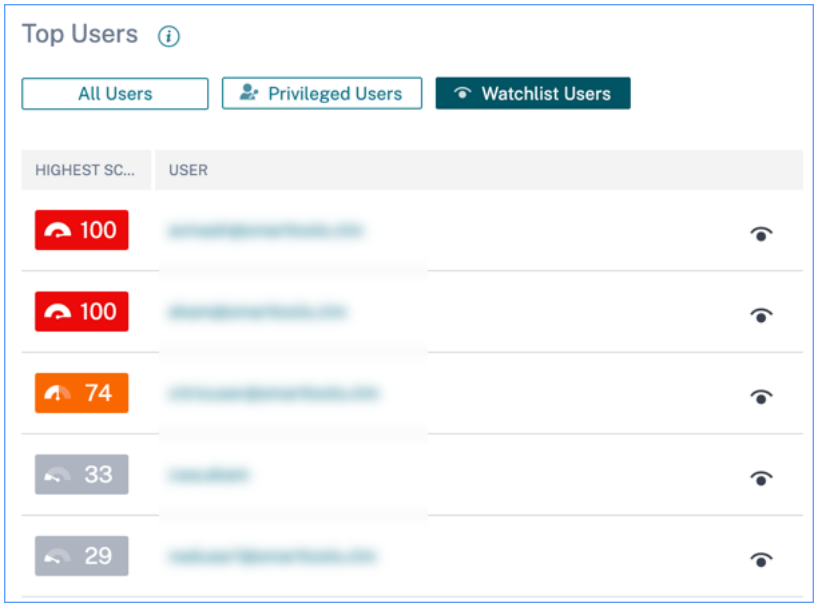
> **Hinweis**
>
> In früheren Versionen wurde in der Tabelle Top-Benutzer unabhängig vom ausgewählten Zeitraum immer die aktuelle Risikobewertung angezeigt.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Nutzer der Watchlist

Liste der Benutzer, die genau auf potenzielle Bedrohungen überwacht werden. Sie können beispielsweise Benutzer überwachen, die keine Vollzeitmitarbeiter in Ihrem Unternehmen sind, indem Sie diese Benutzer zur Watchlist hinzufügen. Sie können auch Benutzer überwachen, die häufig einen bestimmten Risikoindikator auslösen. Sie fügen entweder manuell einen Benutzer zur Watchlist hinzu oder definieren Richtlinien, um Benutzer zur Watchlist hinzuzufügen.

Wenn Sie Benutzer zur Watchlist hinzugefügt haben, können Sie sich die fünf besten Benutzer auf der Watchlist anhand der höchsten Punktzahl anzeigen lassen.



Klicken Sie im Bereich **Alle Benutzer** auf den Link **Mehr** anzeigen, um die Seite **Benutzer** aufzurufen. Auf der Seite wird die Liste aller Benutzer in der Watchlist angezeigt.

> **Hinweis**
>
> Im **Benutzer-Dashboard** und auf der Seite **Benutzer** wird die Anzahl der Benutzer in der Watchlist unabhängig vom ausgewählten Zeitraum für die letzten 13 Monate angezeigt. Wenn Sie einen Zeitraum auswählen, ändern sich die Vorkommnisse des Risikoindikators basierend auf der Zeitauswahl.

Mehr erfahren: Watchlist

Risiko-Kategorien

Das **Ringdiagramm "Risikokategorien** "fasst die Anzahl der Indikatorvorkommen nach Risikokategorien im ausgewählten Zeitraum zusammen. Wenn Sie mit der Maus über jedes Diagrammsegment fahren, werden eindeutige Benutzerzahlen angezeigt, wodurch wiederum auf die entsprechende

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

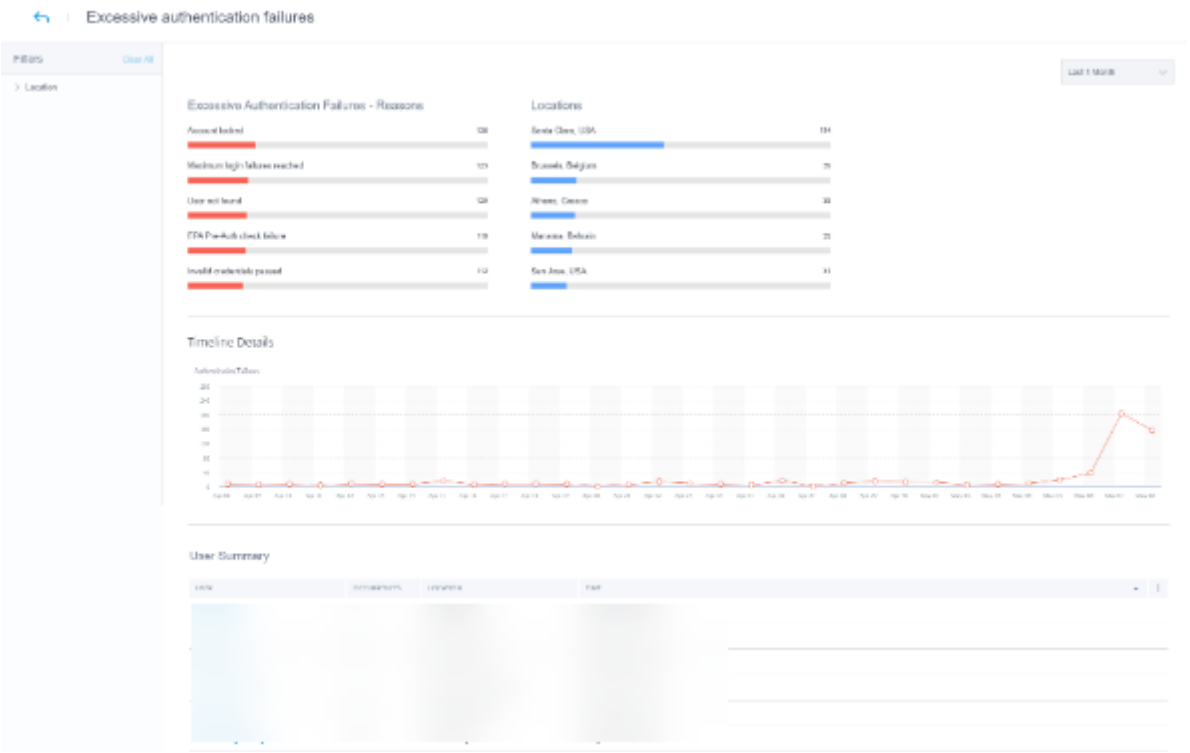
Übersichtsseite der **Risikoindikator-Kategorie** verwiesen wird. Die Risikokategorisierung wird durch standardmäßige und benutzerdefinierte Risikoindikatoren unterstützt.

Der Zweck des Dashboards **für Risikokategorien besteht** darin, Citrix Virtual Apps and Desktops und Citrix DaaS-Administratoren die Verwaltung von Benutzerrisiken zu ermöglichen und die Diskussionen mit ihren Sicherheitspartnern zu vereinfachen, ohne dass Sicherheitskenntnisse auf Expertenebene erforderlich sind. Es ermöglicht die Umsetzung der Sicherheitsdurchsetzung auf organisatorischer Ebene und ist nicht nur auf Sicherheitsadministratoren beschränkt.

Anwendungsfall

Bedenken Sie, dass Sie ein Administrator für Citrix Virtual Apps and Desktops sind und die Anwendungszugriffsrechte von Mitarbeitern in Ihrem Unternehmen verwalten. Wenn Sie zum Abschnitt **Risikokategorien** > **Kompromittierte Benutzer** > **Übermäßige Authentifizierungsfehler - NetScaler Gateway-Risikoindikator** gehen, können Sie beurteilen, ob die Mitarbeiter, denen Sie Zugriff gewährt haben, kompromittiert wurden. Wenn Sie weiter navigieren, können Sie genauere Einblicke in diesen Risikoindikator erhalten, z. B. die Fehlergründe, Anmeldeorte, Timeline-Details und Benutzerzusammenfassung. Wenn Sie Unstimmigkeiten zwischen den Benutzern, denen Zugriff gewährt wurde, und den Benutzern, die kompromittiert wurden, feststellen, können Sie den Sicherheitsadministrator darüber informieren. Diese rechtzeitige Benachrichtigung des Sicherheitsadministrators trägt zur Durchsetzung der Sicherheit auf organisatorischer Ebene bei.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



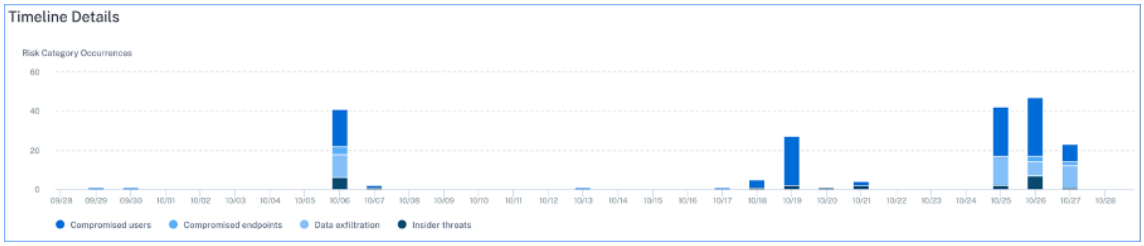
Wie analysiert man das Dashboard Risikokategorien?

Wenn Sie im Dashboard **Risikokategorien** die Option **Mehr** anzeigen auswählen, werden Sie auf die Seite weitergeleitet, auf der Details zu den Risikokategorien zusammengefasst sind. Diese Seite enthält die folgenden Details:

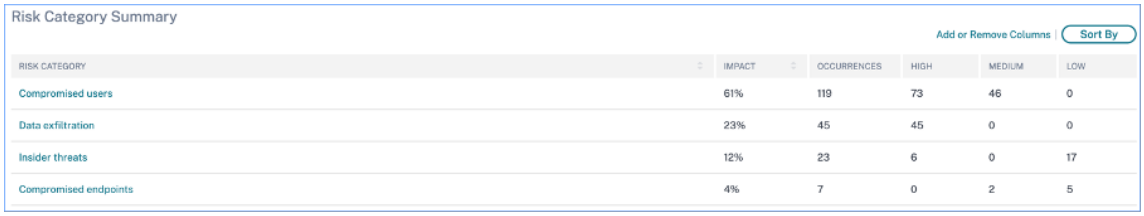
- **Risikokategoriebericht**: Stellt die Gesamtrisikoindikatorvorkommen jeder Kategorie für einen ausgewählten Zeitraum dar.

- **Details zur Zeitleiste**: Bietet eine grafische Darstellung des Gesamtrisikoindikators jeder Risikokategorie für einen ausgewählten Zeitraum. Wenn Sie zum Ende dieses Abschnitts navigieren, können Sie nach Risikokategorien sortieren, um genauere Einblicke in die Risikoindikatoren zu erhalten.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



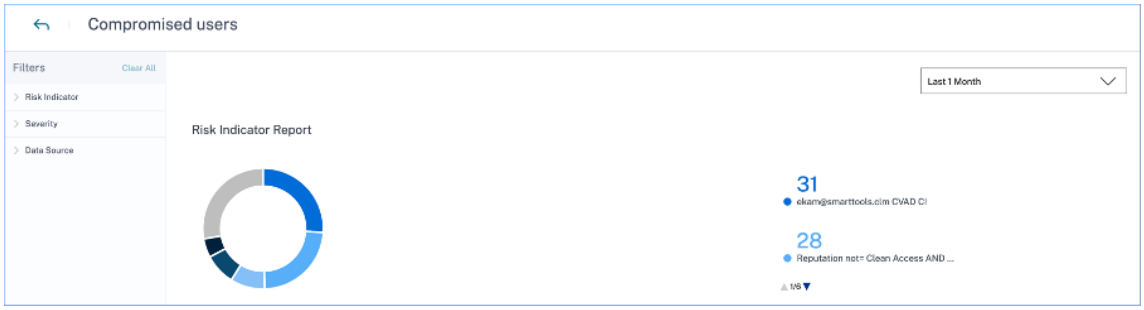
- **Zusammenfassung der Risikokategorie**: Dieser Abschnitt enthält Details wie die Auswirkungen, das Auftreten und den Schweregrad der mit jeder Kategorie verbundenen Risikoindikatoren. Wählen Sie eine beliebige Risikokategorie aus, um Details zu den mit dieser Kategorie verbundenen Risikoindikatoren anzuzeigen. Wenn Sie beispielsweise die Kategorie **Kompromittierte Benutzer** auswählen, werden Sie zur Seite **Kompromittierte Benutzer** weitergeleitet.



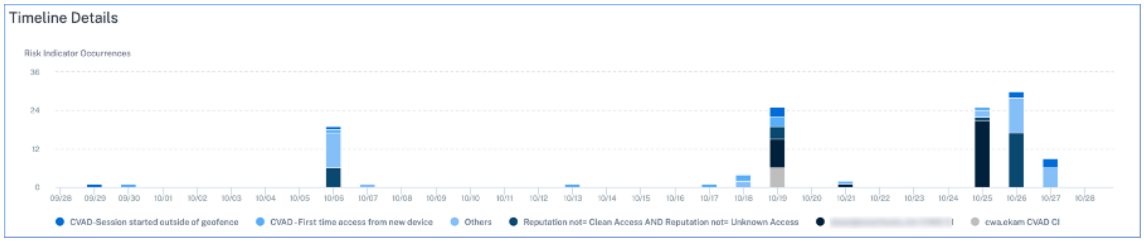
RISK CATEGORY	IMPACT	OCCURRENCES	HIGH	MEDIUM	LOW
Compromised users	61%	119	73	46	0
Data exfiltration	23%	45	45	0	0
Insider threats	12%	23	6	0	17
Compromised endpoints	4%	7	0	2	5

Auf der Seite **Kompromittierte Benutzer** werden die folgenden Details angezeigt:

- **Risikoindikatorbericht**: Zeigt die Risikoindikatoren an, die für einen ausgewählten Zeitraum zur Kategorie Kompromittierte Benutzer gehören. Es zeigt auch die Gesamtereignisse der Risikoindikatoren an, die während des ausgewählten Zeitraums ausgelöst wurden.



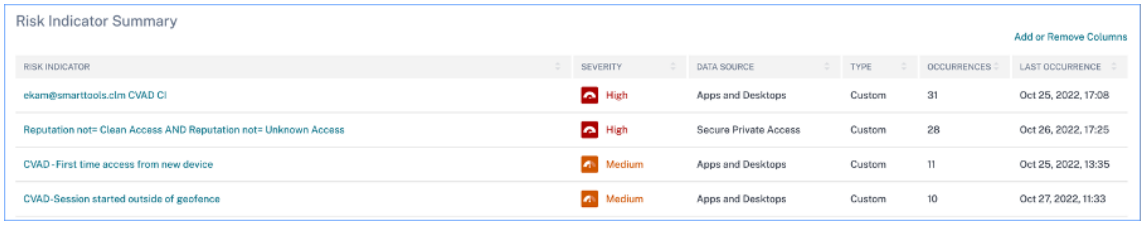
- **Timeline-Details**: Bietet eine grafische Darstellung des Risikoindikators für einen ausgewählten Zeitraum.



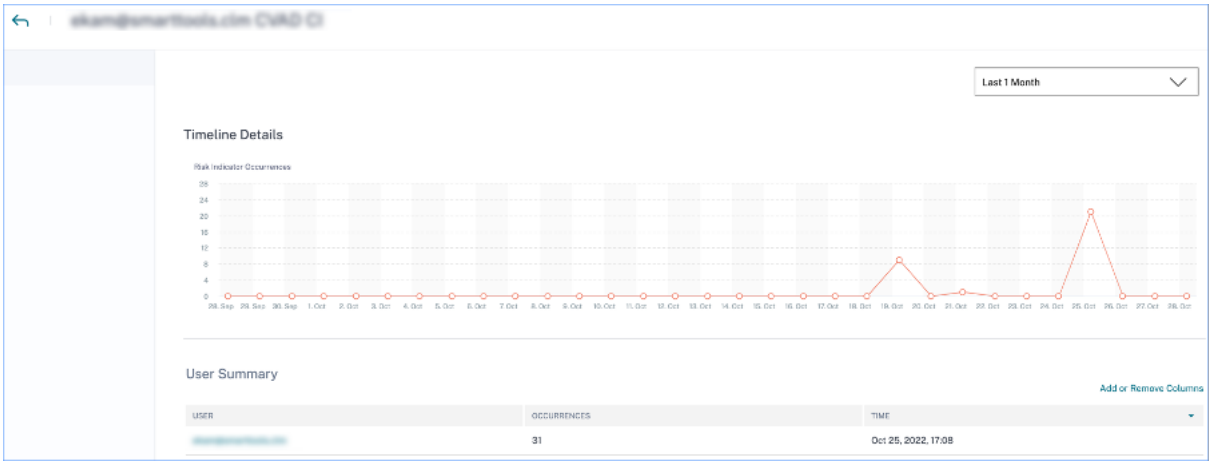
- **Zusammenfassung des Risikoindikators**: Zeigt eine Zusammenfassung der Risikoindikatoren an, die unter der Kategorie Kompromittierte Benutzer generiert wurden. In diesem Abschnitt

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

werden auch der Schweregrad, die Datenquelle, der Risikoindikatortyp, das Auftreten und das letzte Auftreten angezeigt.



Wenn Sie einen Risikoindikator auswählen, werden Sie zu der Seite weitergeleitet, auf der die Details dieses Indikators zusammengefasst sind. Wenn Sie beispielsweise den Risikoindikator **Erster Zugriff über ein neues Gerät** auswählen, werden Sie auf die Seite weitergeleitet, auf der Details zu diesem Indikator zusammengefasst sind. Die Zusammenfassung enthält Zeitleistendetails über das Auftreten dieses Ereignisses sowie eine Benutzerzusammenfassung, in der die Benutzer, die diesen Risikoindikator ausgelöst haben, das Auftreten von Risikoindikatoren und der Zeitpunkt des Ereignisses aufgeführt sind. Wenn Sie einen Benutzer auswählen, werden Sie zur Risikozeitleiste des Benutzers weitergeleitet.



> **Hinweis**
>
> Citrix Analytics gruppiert Standardrisikoindikatoren unter der entsprechenden Risikokategorie. Für benutzerdefinierte Risikoindikatoren müssen Sie auf der Seite **Indikator erstellen** eine Risikokategorie auswählen. Weitere Informationen finden Sie unter Benutzerdefinierte Risikoindikatoren.

Arten von Risikokategorien

Exfiltration von Daten In dieser Kategorie werden Risikoindikatoren zusammengefasst, die durch Schadsoftware oder durch Mitarbeiter ausgelöst werden, die unbefugte Datenübertragungen oder Datendiebstähle zu oder von einem Gerät in einem Unternehmen durchführen. Sie können Einblicke in alle Datenexfiltrationsaktivitäten erhalten, die während eines bestimmten Zeitraums stattgefunden

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

haben, und die mit dieser Kategorie verbundenen Risiken mindern, indem Sie proaktiv Aktionen auf Benutzerprofile anwenden.

Die Risikokategorie Datenexfiltration gruppiert die folgenden Risikoindikatoren:

Datenquellen	Indikatoren für Benutzerrisiken
Citrix Virtual Apps and Desktops von Citrix und Citrix DaaS	Potenzielle Datenexfiltration

Insider-Bedrohungen Diese Kategorie gruppiert Risikoindikatoren, die von Mitarbeitern innerhalb einer Organisation ausgelöst werden. Da Mitarbeiter einen höheren Zugriff auf unternehmensspezifische Anwendungen haben, besteht für Unternehmen ein höheres Risiko von Sicherheitsrisiken. Riskante Aktivitäten können absichtlich von einem böswilligen Insider verursacht werden oder auf ein menschliches Versagen zurückzuführen sein. In beiden Szenarien sind die Auswirkungen auf die Sicherheit auf das Unternehmen schädlich. Diese Kategorie bietet Einblicke in alle Aktivitäten von Insider-Bedrohungen, die in einem bestimmten Zeitraum stattgefunden haben. Mithilfe dieser Erkenntnisse können Sie die mit dieser Kategorie verbundenen Risiken mindern, indem Sie proaktiv Aktionen auf Benutzerprofile anwenden.

Die Risikokategorie Insider-Bedrohungen fasst die folgenden Risikoindikatoren zusammen:

Datenquellen	Indikatoren für Benutzerrisiken
Citrix Secure Private Access	Versuch, auf eine URL auf der Sperrliste zuzugreifen
Citrix Secure Private Access	Übermäßiger Datendownload
Citrix Secure Private Access	Zugriff auf riskante Website
Citrix Secure Private Access	Ungewöhnliches Uploadvolumen

Kompromittierte Benutzer In dieser Kategorie werden Risikoindikatoren zusammengefasst, bei denen Benutzer ungewöhnliche Verhaltensmuster wie verdächtige Anmeldungen und Anmeldefehler aufweisen. Alternativ können die ungewöhnlichen Muster darauf zurückzuführen sein, dass die Benutzerkonten kompromittiert wurden. Sie können Einblicke in alle kompromittierten Benutzerereignisse erhalten, die während eines bestimmten Zeitraums stattgefunden haben, und die mit dieser Kategorie verbundenen Risiken mindern, indem Sie proaktiv Aktionen auf Benutzerprofile anwenden.

In der Risikokategorie „Gefährdete Benutzer“werden die folgenden Risikoindikatoren zusammengefasst:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Datenquellen	Indikatoren für Benutzerrisiken
Citrix Gateway	Fehler beim Scannen der Endpunktanalyse
Citrix Gateway	Übermäßige Authentifizierungsfehler
Citrix Gateway	Unmögliche Reisen
Citrix Gateway	Anmeldung von verdächtiger IP
Citrix Gateway	Ungewöhnlicher Authentifizierungsfehler
Citrix Virtual Apps and Desktops von Citrix und Citrix DaaS	Verdächtige Anmeldung
Citrix Virtual Apps and Desktops von Citrix und Citrix DaaS	Unmögliche Reisen
Microsoft Graph Security	Azure AD-Identitätsschutz-Risikoindikatoren
Microsoft Graph Security	Microsoft Defender for Endpoint Risikoindikatoren

Kompromittierte Endpunkte Diese Kategorie gruppiert Risikoindikatoren, die ausgelöst werden, wenn Geräte unsicheres Verhalten aufweisen, das auf einen Kompromiss hindeuten könnte.

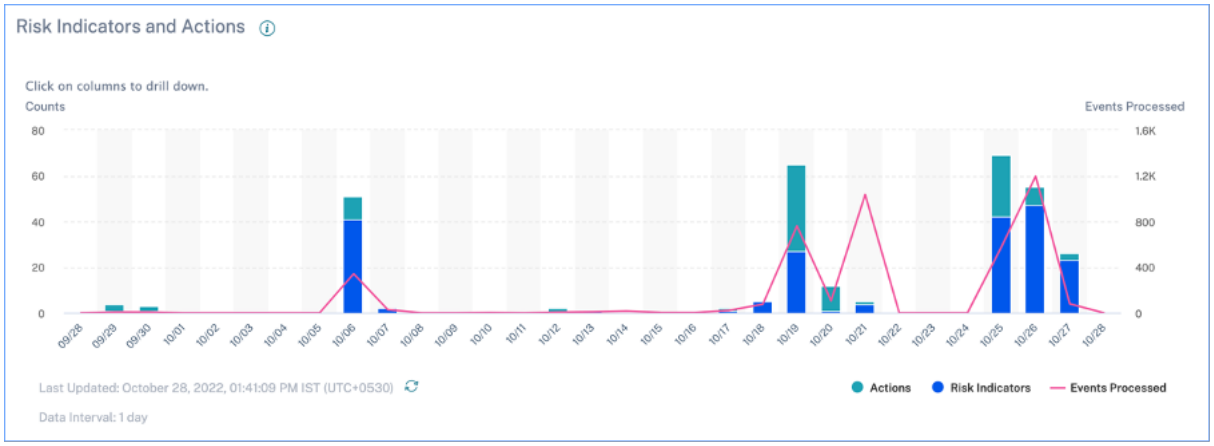
Die Risikokategorie Kompromittierte Endpunkte fasst die folgenden Risikoindikatoren zusammen:

Datenquellen	Indikatoren für Benutzerrisiken
Citrix Endpoint Management	Nicht verwaltetes Gerät erkannt
Citrix Endpoint Management	Jailbreak oder gerootetes Gerät erkannt
Citrix Endpoint Management	Gerät mit Apps auf der Sperrliste erkannt

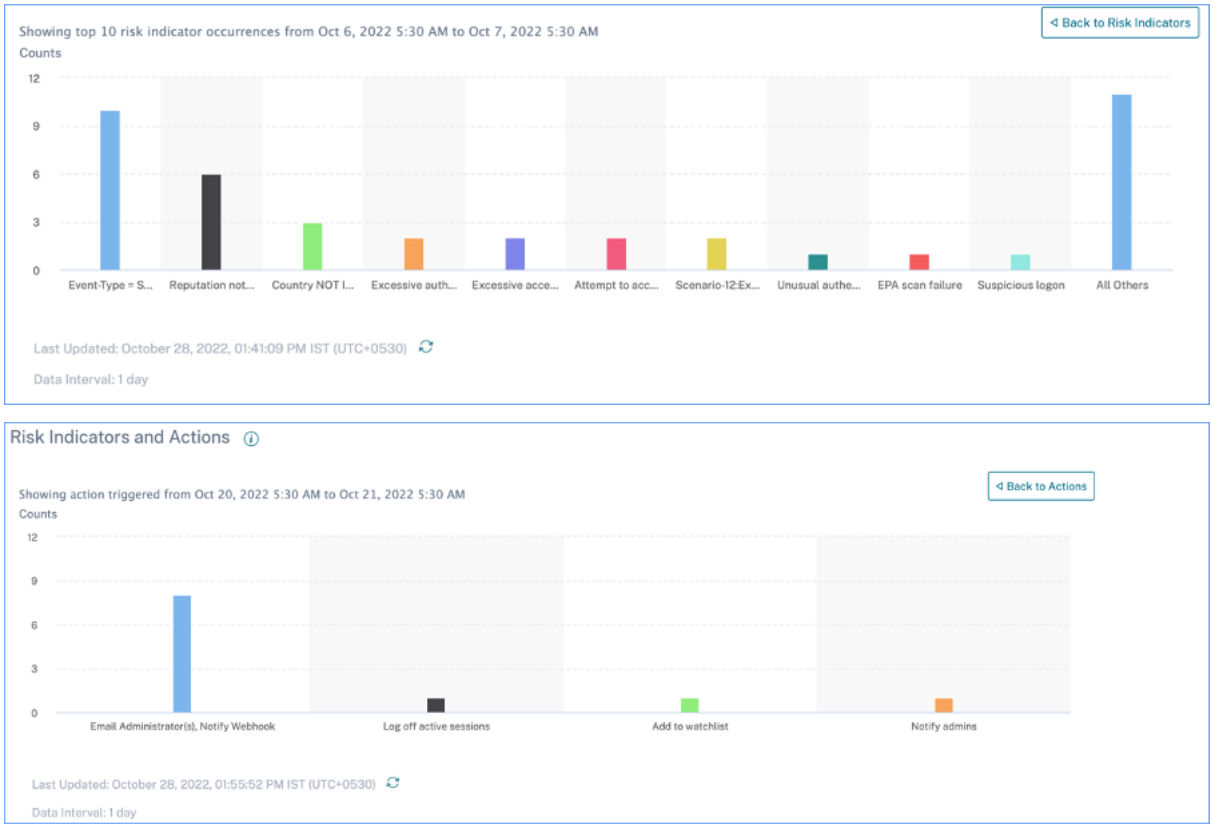
Risikoindikatoren und Maßnahmen

Sie können die ausgelösten Risikoindikatoren und die angewandten Aktionen für Ihre Benutzer für den ausgewählten Zeitraum einsehen. Das neue Balkendiagramm mit **Risikoindikatoren und Maßnahmen** zeigt die Anzahl der Indikatoren, Aktionen und Ereignisse im Zeitverlauf detailliert an, wobei der Gesamtzeitbereich und das Balkenintervall aus dem ausgewählten Zeitraum abgeleitet wurden.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Wenn Sie auf ein Balkensegment für Indikatoren oder Aktionen klicken, erhalten Sie eine detaillierte Darstellung der Anzahl pro Indikator bzw. Aktion.



Wenn Sie in der Indikator-Drilldown-Liste auf eine einzelne Indikatorleiste klicken, wird die entsprechende Seite mit den Risikoindikatoren für den ausgewählten Zeitraum aufgerufen.

Access-Zusammenfassung

Dieses Dashboard fasst alle Gateway-Zugriffsereignisse für einen ausgewählten Zeitraum zusammen. Es zeigt die Anzahl des Gesamtzugriffs, des erfolgreichen Zugriffs und des fehlgeschlagenen Zugriffs

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

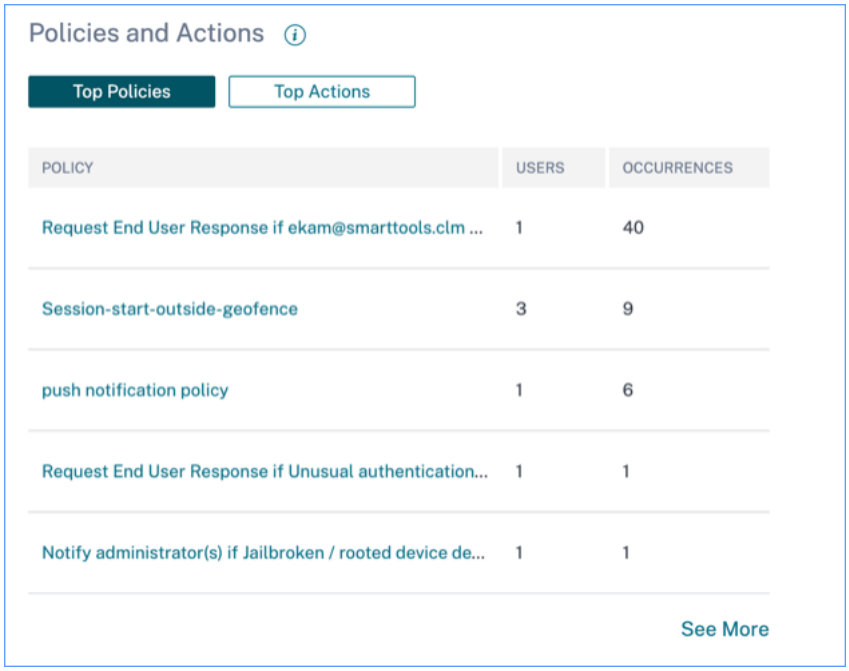
über NetScaler Gateway.

Klicken Sie auf die Zeiger in der Grafik, um die Seite Self-Service-Suche nach Gateway anzuzeigen. Für erfolgreiche Anmeldeszenarien werden Gateway-Zugriffsereignisse nach dem Statuscode auf der Seite sortiert.

Richtlinien und Aktionen

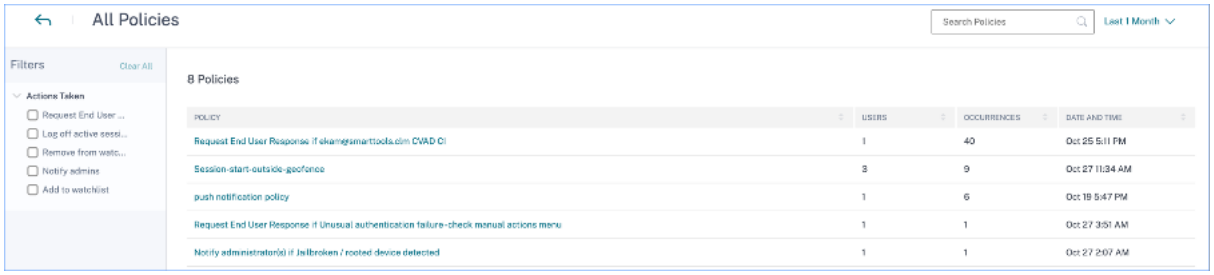
Zeigt die fünf wichtigsten Richtlinien und Aktionen an, die für einen ausgewählten Zeitraum auf Benutzerprofile angewendet wurden. Klicken **Sie im Bereich**Richtlinien und Aktionen**auf den Link Weitere** Informationen, um detaillierte Informationen zu den Richtlinien und Aktionen zu erhalten.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Top-Richtlinien

Die fünf wichtigsten konfigurierten Richtlinien werden basierend auf der Anzahl der Vorkommen bestimmt. Wenn Sie sich im Abschnitt "**Top-Richtlinien** "des Dashboards befinden und **Mehr anzeigen**auswählen, werden Sie zur Seite **Alle Richtlinien** weitergeleitet.



Alle Richtlinien Diese Seite enthält ausführliche Informationen zu allen konfigurierten Richtlinien. Wenn Sie eine Richtlinie auswählen, werden Sie zur Seite Self-Service-Suche nach Richtlinien weitergeleitet. Im linken Bereich können Sie basierend auf den angewendeten Aktionen filtern.

Wenn Sie einen Benutzernamen auswählen, werden Sie zur Risikozeitleiste weitergeleitet. Die richtlinienbasierte Aktion wird zur Risikozeitleiste des Benutzers hinzugefügt. Wenn Sie die Aktion auswählen, werden ihre Details im rechten Bereich des Risikozeitplans angezeigt.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

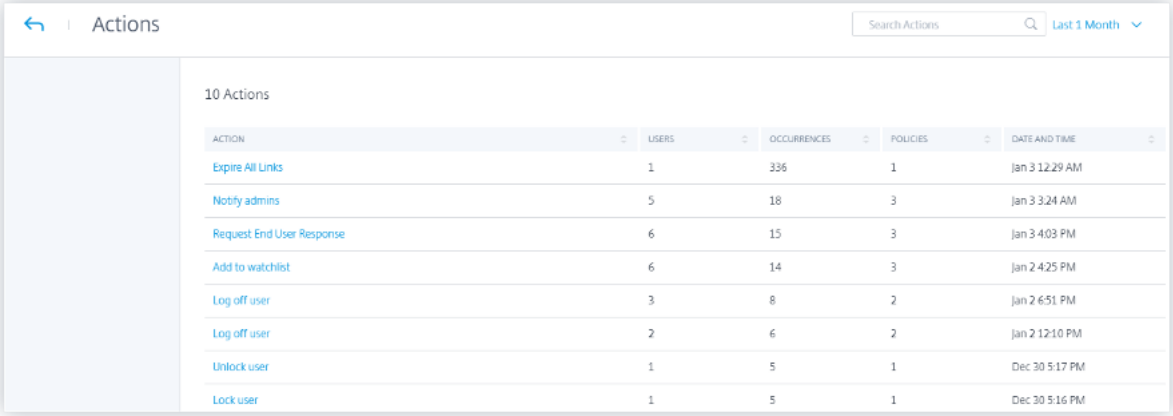
Top Aktionen

Die fünf wichtigsten Aktionen, die mit den Richtlinien verknüpft sind, die auf die Benutzerprofile angewendet wurden. In diesem Abschnitt werden die Aktionen nicht angezeigt, die Sie manuell auf die Benutzerprofile angewendet haben. Die Top-Aktionen werden durch die Anzahl der Vorkommen bestimmt.

Klicken Sie auf **Mehr** anzeigen, um alle richtlinienbasierten Aktionen auf der Seite **Aktionen** anzuzeigen.

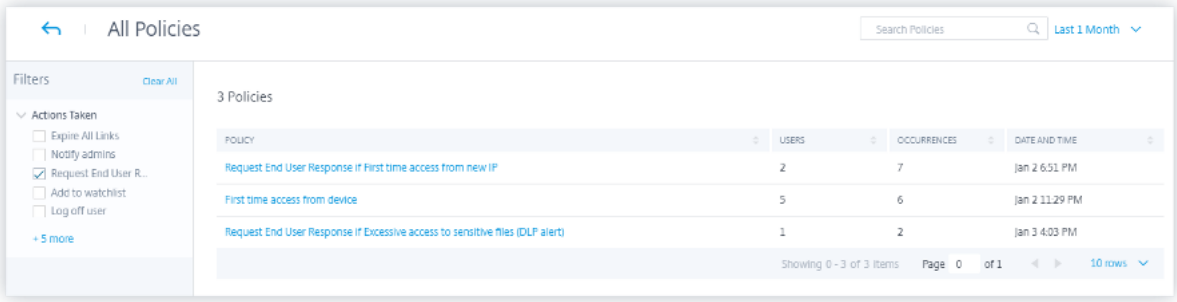
Aktionen Die Seite enthält eine Liste aller richtlinienbasierten Aktionen, die für den ausgewählten Zeitraum auf Ihre Benutzer angewendet wurden. Sie sehen die folgenden Informationen an:

- Name der Aktion, die gemäß der Richtlinie angewendet wird
- Anzahl der Benutzer, auf die die Aktion angewendet wurde
- Anzahl der Vorkommen der Aktion
- Anzahl der mit der Aktion verknüpften Richtlinien
- Datum und Uhrzeit der angewendeten Aktion



Klicken Sie auf eine Aktion, um alle zugehörigen Richtlinien anzuzeigen. Diese Richtlinien werden basierend auf der Anzahl der Vorkommen sortiert. Klicken Sie beispielsweise auf der Seite **Aktionen** auf **Endbenutzerantwort anfordern** . Auf der Seite **Alle Richtlinien** werden alle Richtlinien angezeigt, die mit der Aktion **Endbenutzer-Antwort anfordern** verknüpft sind.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Klicken Sie auf der Seite **Alle Richtlinien** auf eine Richtlinie, um die Benutzerereignisse anzuzeigen, auf die die Aktion angewendet wurde.

Risikoindikatoren

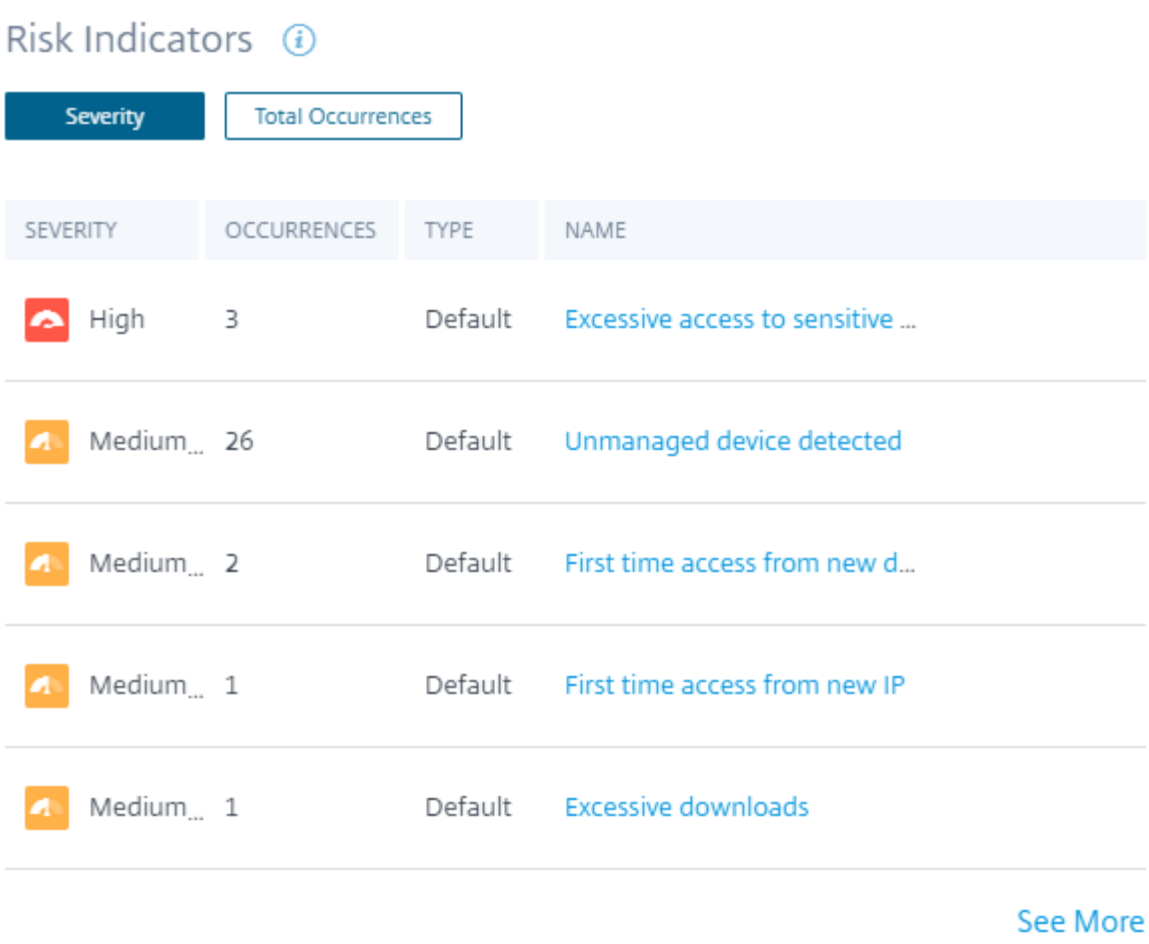
Fasst die fünf wichtigsten Risikoindikatoren für einen ausgewählten Zeitraum zusammen. Die Risikoindikatoren können Standard oder benutzerdefiniertsein. Für Standardrisikoindikatoren sammelt Citrix Analytics Daten aus den erkannten Datenquellen, auf denen die Datenverarbeitung aktiviert ist.

Für benutzerdefinierte Risikoindikatoren sammelt Citrix Analytics Daten aus den folgenden Datenquellen basierend auf den generierten riskanten Ereignissen:

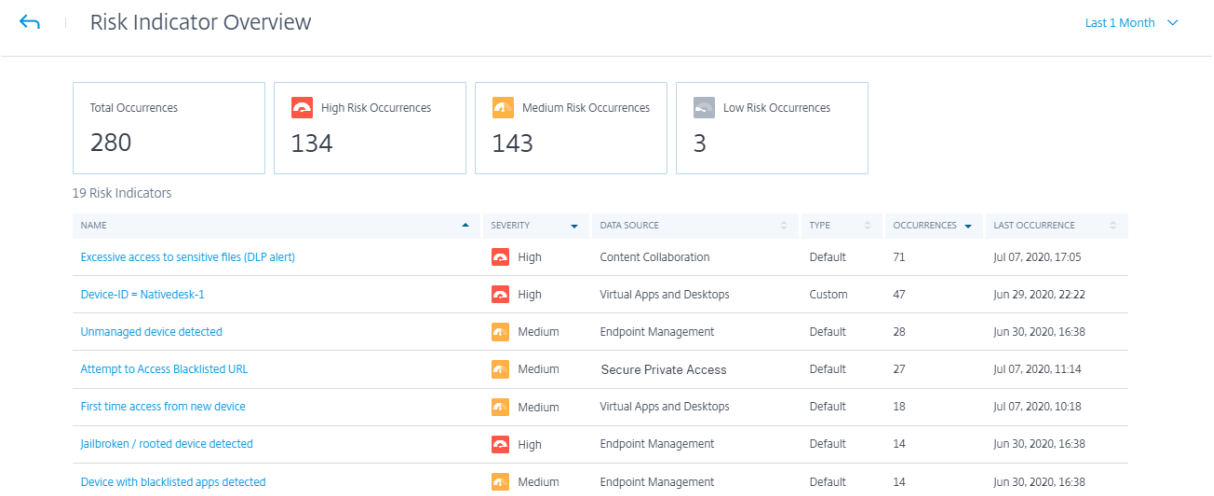
- Citrix Gateway
- Citrix Secure Private Access
- Citrix Virtual Apps and Desktops
- Citrix DaaS (früher Citrix Virtual Apps and Desktops Service)

Im Bereich **Risikoindikatoren** können Sie die fünf wichtigsten Risikoindikatoren anzeigen und nach Gesamtvorkommen oder Schweregrad sortieren.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Klicken Sie im Bereich **Risikoindikatoren** auf **Mehr anzeigen**, um die Seite **Risikoindikatorübersicht** anzuzeigen.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Dashboard zur Zugriffssicherung

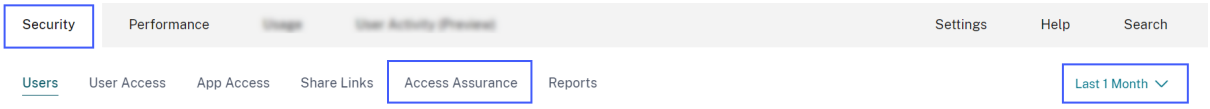
December 5, 2022

Angesichts der zunehmenden Anzahl von Telearbeit möchten Sie als Citrix IT-Administrator möglicherweise die Gewissheit haben, dass Ihre Benutzer von ihren gewohnten und sicheren Standorten aus auf Citrix Virtual Apps and Desktops oder Citrix DaaS (ehemals Citrix Virtual Apps and Desktops Service) zugreifen. Wenn sich Benutzer von unbekannten Standorten oder neuen Standorten aus angemeldet haben, können Sie ihre Anmeldedetails validieren und die erforderlichen Maßnahmen ergreifen, um Bedrohungen für Ihre Citrix IT-Umgebung zu mindern.

Das Access Assurance-Dashboard bietet einen Überblick über die Standorte und Netzwerke, von denen aus Ihre Benutzer auf virtuelle Apps oder virtuelle Desktops zugreifen. Citrix Analytics for Security empfängt diese Benutzeranmeldeereignisse von der Citrix Workspace-App, die auf den Geräten der Benutzer installiert ist. Weitere Informationen zu den unterstützten Versionen finden Sie in der Versionsmatrix der Citrix Workspace Workspace-App.

Das Dashboard ansehen

Um das Dashboard anzuzeigen, klicken Sie auf **Sicherheit > Zugriffsversicherung**. Wählen Sie den Zeitraum aus, für den Sie die Anmeldedetails anzeigen möchten.

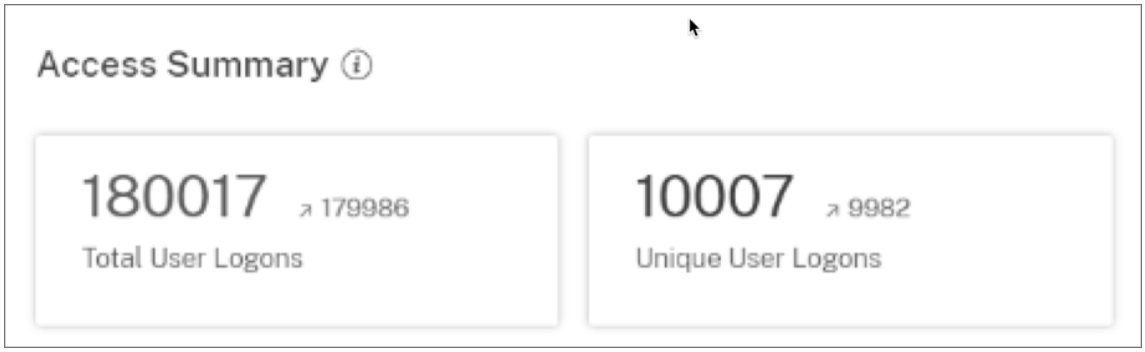


Zusammenfassung des Zugriffs

Der Übersichtsbereich des Dashboards enthält die folgenden Informationen für einen ausgewählten Zeitraum:

1. Gesamtzahl der Benutzeranmeldungen an den Standorten (weltweit).
2. Gesamtzahl der eindeutigen Benutzeranmeldungen an den Standorten (weltweit).

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Ort der Anmeldung

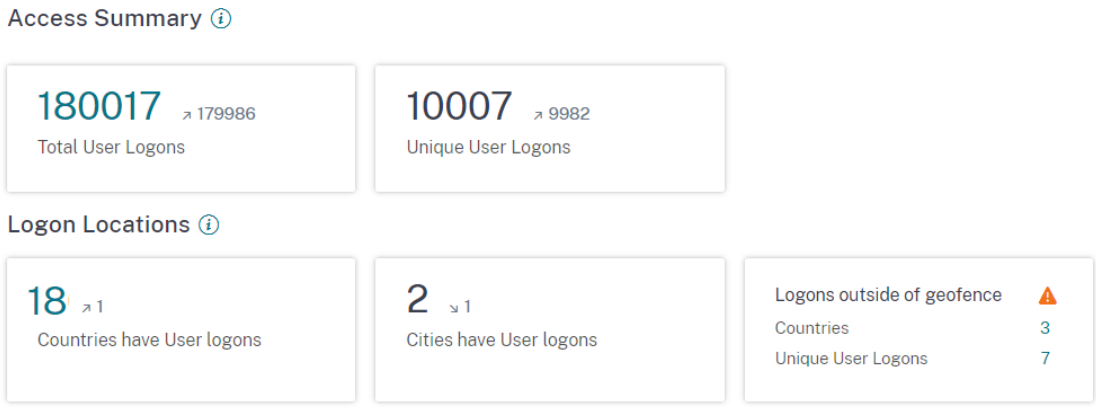
Der Abschnitt **Anmeldeorte** enthält die folgenden Informationen für einen ausgewählten Zeitraum:

- Gesamtzahl der Länder, aus denen sich die Benutzer angemeldet haben.
- Gesamtzahl der Städte, von denen aus sich die Benutzer angemeldet haben.
- Gesamtzahl der Länder und die eindeutigen Benutzeranmeldungen in den Geofencing-Gebieten. Um die Anmeldedetails aus den Geofencing-Bereichen anzuzeigen, aktivieren Sie Geofencing.
- Top 10 Standorte mit eindeutigen Benutzeranmeldungen. Manchmal stammen die wichtigsten Benutzeranmeldungen auch aus unbekannten Städten und Ländern und diese werden auf der Registerkarte **Unbekannte Standorte** aufgeführt. Die Liste der unbekannten Standorte ist auch eine Teilmenge der Top 10 Standorte. Informationen zu den Gründen, warum einige Standorte nicht identifiziert wurden, finden Sie unter Standorte, die als nicht verfügbar identifiziert wurden.

Sie können auch den Aufwärts- oder Abwärtstrend der gesamten Benutzeranmeldungen weltweit und der Gesamtzahl der eindeutigen Benutzeranmeldungen weltweit anzeigen. Für die 10 wichtigsten Standorte zeigt die Spalte **ABWEICHUNG** die Änderung (positiv (+) oder negativ (-)) in den Benutzeranmeldungen für jeden Standort an. Dieser Vergleich basiert auf dem ausgewählten Zeitraum und dem vorherigen Zeitraum gleicher Länge. Wenn Sie beispielsweise den Zeitraum **Letzter Monat**auswählen, werden der Trend der Benutzeranmeldung und die Abweichung zwischen dem letzten Monat und dem vorherigen mit dem letzten 1 Monat verglichen.

> **Hinweis:**
>
> Die Standortinformationen werden auf Stadt- und Länderebene bereitgestellt und stellen keine genaue Geolocation dar. Weitere Informationen zu Access Assurance und Geolocation finden Sie unter Häufig gestellte Fragen.

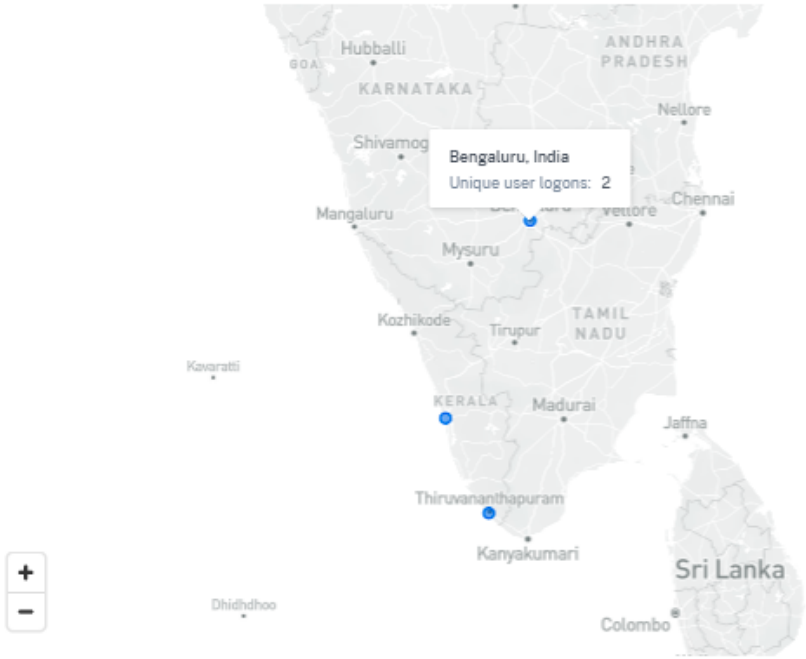
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



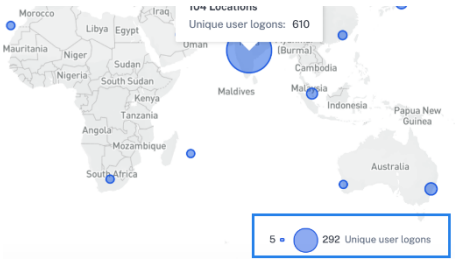
Wählen Sie in der Tabelle **Top 10 Unique Logon Locations** einen Speicherort aus, an dem die Benutzer und deren Zugriffsprofile und Anmeldedetailsangezeigt werden sollen.

Die Karte zeigt die Anzahl der eindeutigen Benutzer von verschiedenen Standorten für einen ausgewählten Zeitraum an. Bewegen Sie den Mauszeiger über die blaue Blase oder zoomen Sie auf eine Position, um die Gesamtzahl der eindeutigen Benutzeranmeldungen vom Standort aus anzuzeigen. Klicken Sie auf die blaue Blase, um die Zugangsdetails für einen Standort anzuzeigen.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



In der unteren rechten Ecke der Karte können Sie den Bereich der eindeutigen Benutzeranmeldungen anzeigen. Für einen ausgewählten Zeitraum gibt die kleine Blase die Mindestanzahl der eindeutigen Benutzeranmeldungen an den Standorten an. Die große Blase gibt die maximale Anzahl der eindeutigen Benutzeranmeldungen an den Standorten an.



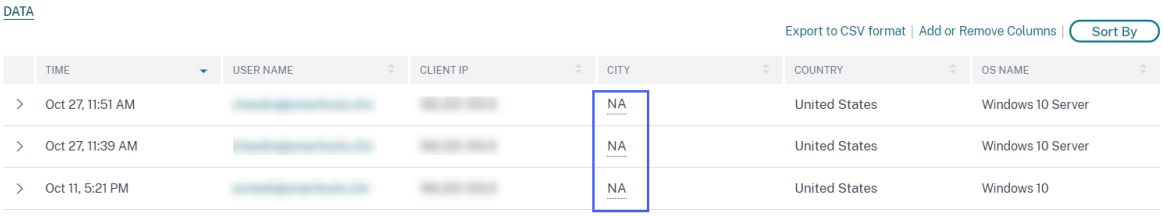
Standorte, die als nicht verfügbar identifiziert wurden

In der Tabelle **Top 10 Unique Logon Locations** sehen Sie möglicherweise, dass einige Standorte unbekannt oder nicht verfügbar sind. Klicken Sie auf einen unbekannten Speicherort, um die entsprechenden Benutzeranmeldedetails auf der Seite **Benutzeranmeldungen** anzuzeigen.

Auf der Seite **Benutzeranmeldungen** wird in der Tabelle **DATA** das **NA-Label** angezeigt, falls keine Landes- oder Stadtinformationen verfügbar sind.

Bewegen Sie den Mauszeiger über das **NA-Label**, um den Grund für die nicht verfügbaren Standortinformationen anzuzeigen.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Möglicherweise wird eines der folgenden Szenarien für die Nichtverfügbarkeit eines Standortes angezeigt:

Szenario	Gründe
Der Name der Stadt und der Ländername sind nicht verfügbar.	Eines der Folgenden 1. Die Benutzer verwenden eine nicht unterstützte Version der Citrix Workspace-App. Aktualisieren Sie den Client auf eine unterstützte Version, um die Standortinformationen anzuzeigen.
Standorte mit privaten IPs	Das Gerät des Benutzers befindet sich in einem privaten Netzwerk. In diesem Fall stehen die Standortinformationen für Citrix Analytics nicht zur Verfügung.
Der Ländername ist verfügbar, der Name der Stadt ist jedoch nicht verfügbar.	Das Gerät des Benutzers verwendet möglicherweise eine Unternehmens-IP. Die IP-Bereiche des Unternehmens sind im externen Geolokationsdienst verschleiert. Daher sind die Standortinformationen für Citrix Analytics nicht verfügbar.

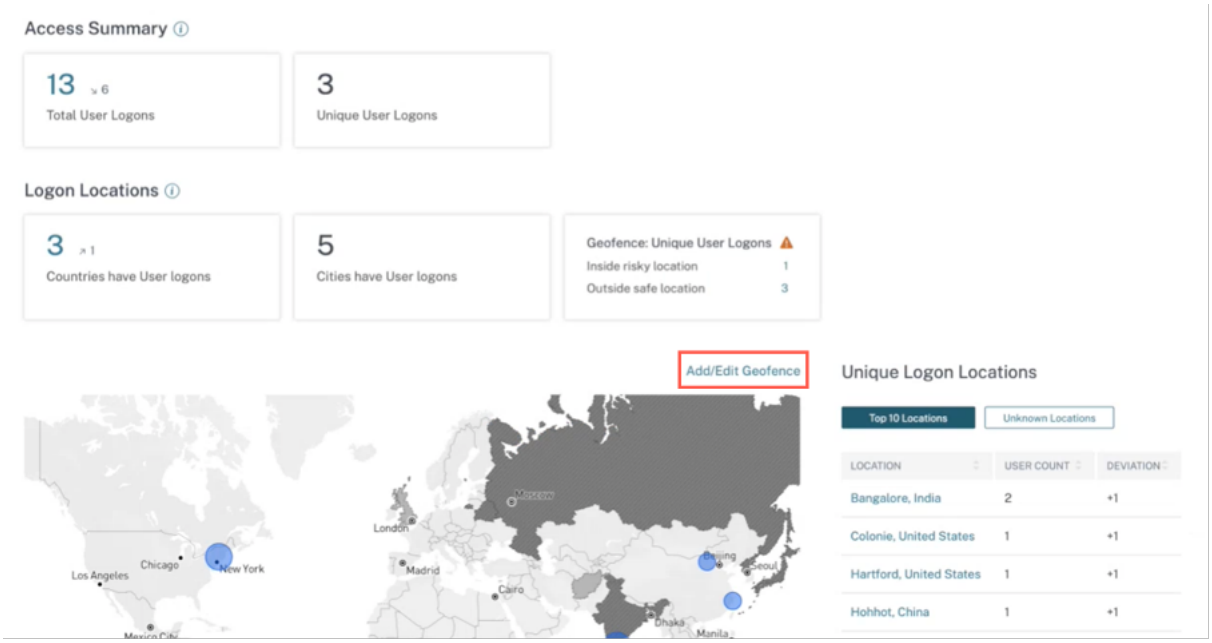
Geofencing aktivieren

Geofencing hilft Ihnen dabei, die Benutzer zu identifizieren, die von außerhalb von Safe Geofence und innerhalb riskanter Geofence-Bereiche auf virtuelle Apps oder virtuelle Desktops zugreifen. Um die Seite **Zugriffsübersicht** anzuzeigen, navigieren Sie zu **Sicherheit > Zugriffsabsicherung**.

Standardmäßig sind die **Geofence-Einstellungen** immer aktiviert. Um Ihren Geofence zu konfiguri-

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

eren, klicken Sie auf **Geofence hinzufügen/bearbeiten**.

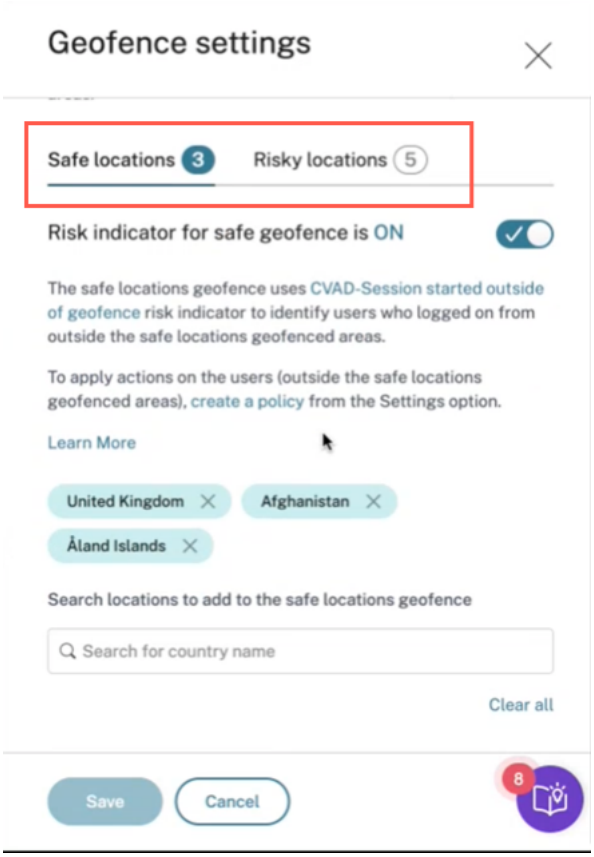


Das Fenster **Geofence-Einstellungen** wird mit zwei Registerkarten angezeigt:

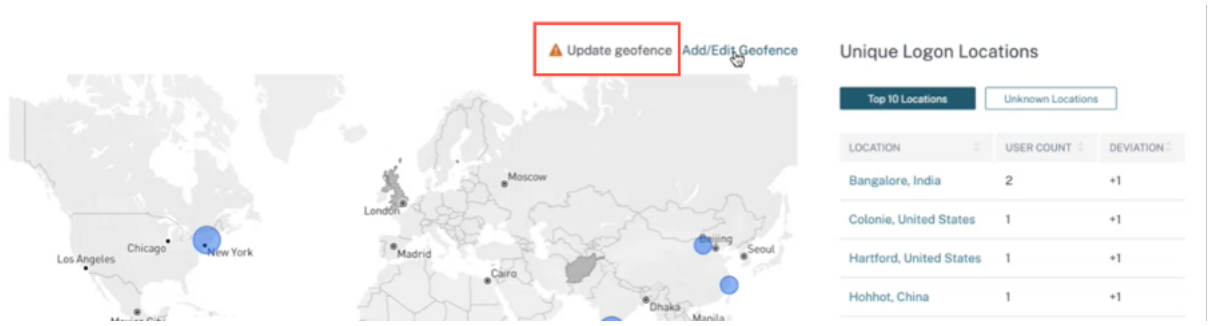
- **Sichere Standorte**: Sie können die Länder konfigurieren oder entfernen, die unter einen sicheren Standort fallen.
- **Riskante Standorte**: Sie können die Länder konfigurieren oder entfernen, die unter einen riskanten Standort fallen.

  Sie können auch die Gesamtzahl der auf jeder Registerkarte konfigurierten sicheren und riskanten Standorte anzeigen. Um ein Land aus einem Geofence für sichere Standorte oder Risikostandortgeofence zu löschen oder zu entfernen, klicken Sie auf das Schließen-Zeichen (X) neben dem Land. Klicken Sie auf **Speichern**, um die Geofence-Einstellungen zu speichern.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

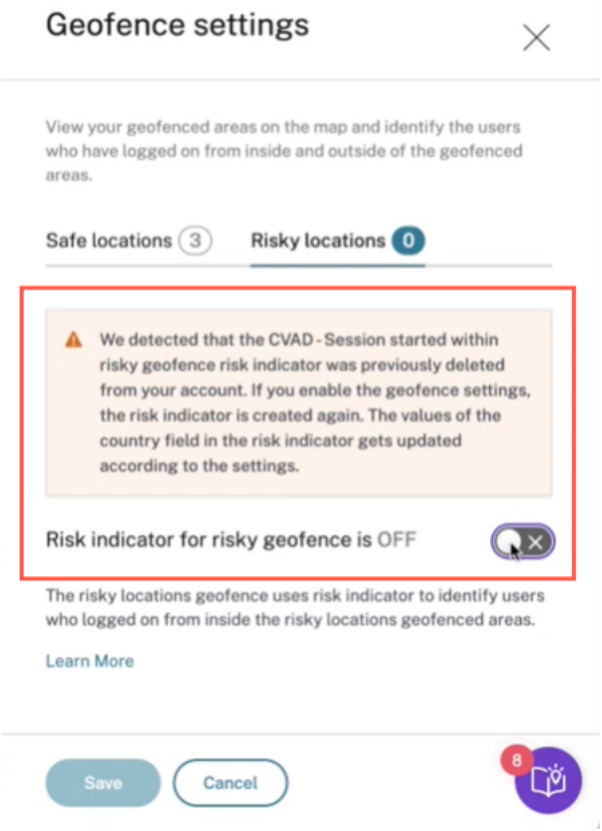


Sie können die Länder konfigurieren, die unter Geofence für riskante Standorte fallen. Wenn für Geofence riskante Standorte keine Risikoindikatoren hinzugefügt wurden oder die Risikoindikatoren gelöscht wurden, wird neben **Geofence hinzufügen/bearbeiten eine Warnmeldung zum Aktualisierenvon Geofence**angezeigt.



Um den Indikator neu zu erstellen, navigieren Sie zur Registerkarte **Riskante Standorte** und aktivieren Sie den Schalter **Risikoindikator für riskanten Geofence** .

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Der Indikator wird mit der Standardliste der riskanten Standorte erstellt.

Auf der Seite **Zugriffszusammenfassung** werden auch die sicheren und riskanten Geofences-Länder angezeigt.

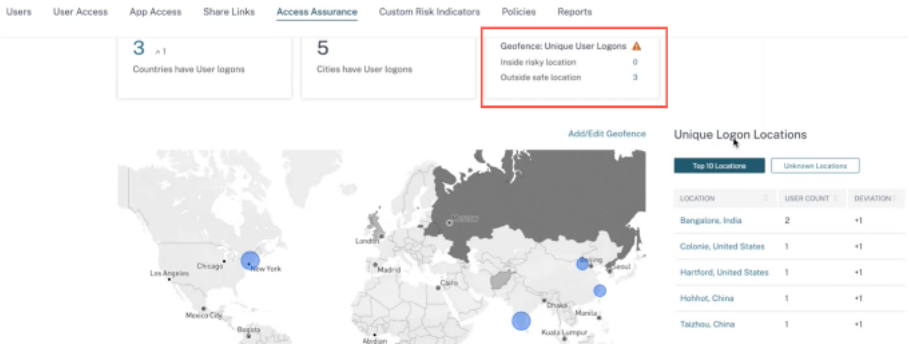
- Geofenced Safe-Länder sind mit einem hellgrauen Kreis gekennzeichnet.
- Geofencing, Riskante Länder sind mit einem dunkelgrauen Kreis gekennzeichnet.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

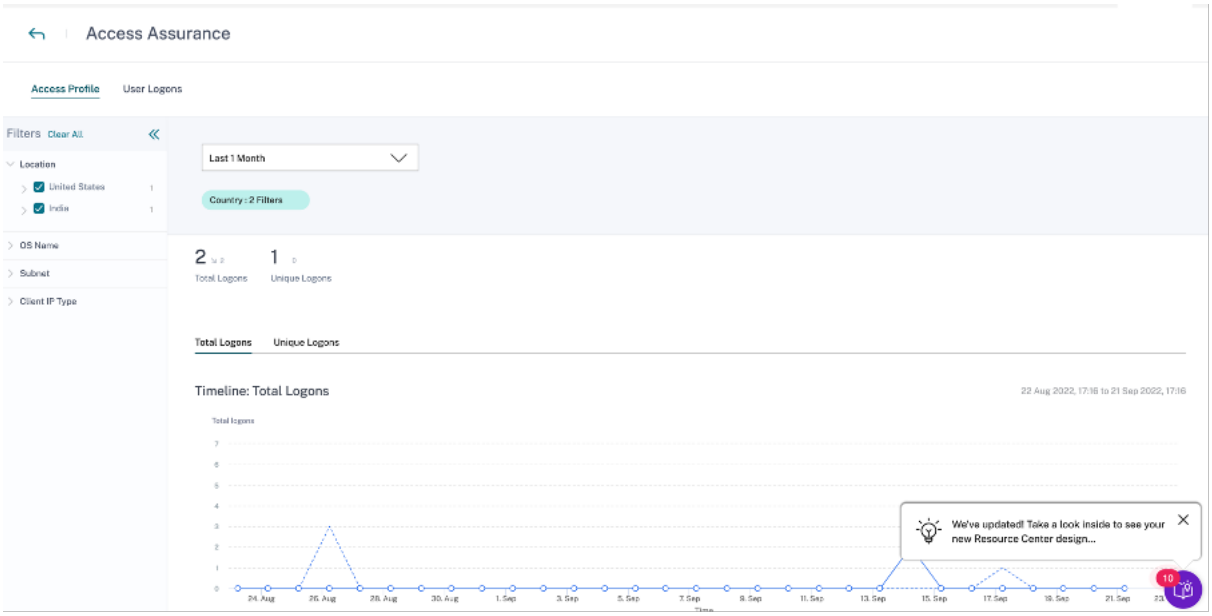
Geofence: Eindeutige Benutzeranmeldungen

Navigieren Sie zur Seite Zugriffszusammenfassung, um Geofence: Eindeutige Benutzeranmeldungen anzuzeigen. Die Karte zeigt die Anzahl der riskanten Standorte innerhalb und außerhalb sicherer Standorte an.

- **Innerhalb eines riskanten Standorts**: Identifizieren Sie Benutzer, die sich innerhalb der Geofencebereiche riskanter Standorte angemeldet haben.
- **Außerhalb des sicheren Standorts** Identifizieren Sie Benutzer, die sich von außerhalb der Geofencebereiche sicherer Standorte angemeldet haben.



Um eine detaillierte Zusammenfassung der gesamten Benutzeranmeldungen und der eindeutigen Benutzeranmeldungen zu erhalten, klicken Sie auf die Zahl neben Innerhalb eines riskanten Standorts oder Außerhalb eines sicheren Standorts.



Diese Funktion verwendet den folgenden vorkonfigurierten benutzerdefinierten Risikoindikator:

- **CVAD-Sitzung außerhalb von Geofence gestartet**: Zur Überwachung von Benutzeranmeldungen außerhalb von Safe Geofence.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Die CVAD-Sitzung wurde in riskantem Geofence gestartet**: Zur Überwachung von Benutzeranmeldungen innerhalb des riskanten Geofence.

Wenn Benutzeranmeldungen außerhalb des Geofence erkannt werden, wird der Risikoindikator ausgelöst und die außerhalb der Geofence-Richtlinie gestartete Sitzung wird auf diese Benutzer angewendet. Die Richtlinie löst die Aktion *Endbenutzerantwort anfordern* aus und basierend auf der Antwort des Benutzers können Sie geeignete Maßnahmen ergreifen, um Bedrohungen durch verdächtige Anmeldungen zu verhindern. Weitere Informationen finden Sie unter vorkonfigurierte benutzerdefinierte Risikoindikatoren.

> **Hinweise**
>
> - Wenn Sie in den **Geofence-Einstellungen**die Länder ändern, wird die *CVAD-Sitzung, die außerhalb des Geofence-Risikoindikators gestartet* wurde, ebenfalls aktualisiert.
> - Wenn Sie beispielsweise die Länder Australien und Indien als neue geofenced-Länder auswählen und speichern, wird die vorkonfigurierte Bedingung des Risikoindikators zusätzlich zu den USA (dem Standard-Geofence) mit den neuen Ländern aktualisiert. Sie können auch das Standardgeofenceland USA entfernen.
>
>   Vorkonfigurierter Zustand des Risikoindikators:
>
>   ```
>   Event-Type = \"Session.logon\" AND Country != \"\" AND Country
>    ~ \"\" AND Country != \"United States\"
>   ```
>
>   Nach dem Aktualisieren der **Geofence-Einstellungen** ist der Zustand des Risikoindikators:
>
>   ```
>   Event-Type = \"Session.logon\" AND Country != \"\" AND Country
>    ~ \"\" AND Country NOT IN (\"Australia\", \"United States\",
>   \"India\"
>   ```
>
> - Wenn die *außerhalb des Geofence-Risikoindikators gestartete CVAD-Sitzung* zuvor aus Ihrem Konto gelöscht wurde, wird durch Aktivieren der **Geofence-Einstellungen** der Risikoindikator erneut erstellt. Die Geofence-Länder des Risikoindikators werden über die **Geofence-Einstellungen**gesteuert.

Nach dem Aktivieren der **Geofence-Einstellungen**werden auf der Karte die geofencing-Bereiche und die eindeutigen Benutzeranmeldungen aus diesen Bereichen angezeigt.

Anmeldenetzwerk

Im Access Assurance-Dashboard können Sie jetzt die folgenden zusätzlichen Benutzerdetails anzeigen:

- Die Organisationen, die den IP-Adressen zugeordnet sind, von denen aus sich die Benutzer angemeldet haben. Zu diesen Organisationen gehören Einrichtungen wie Unternehmen,

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

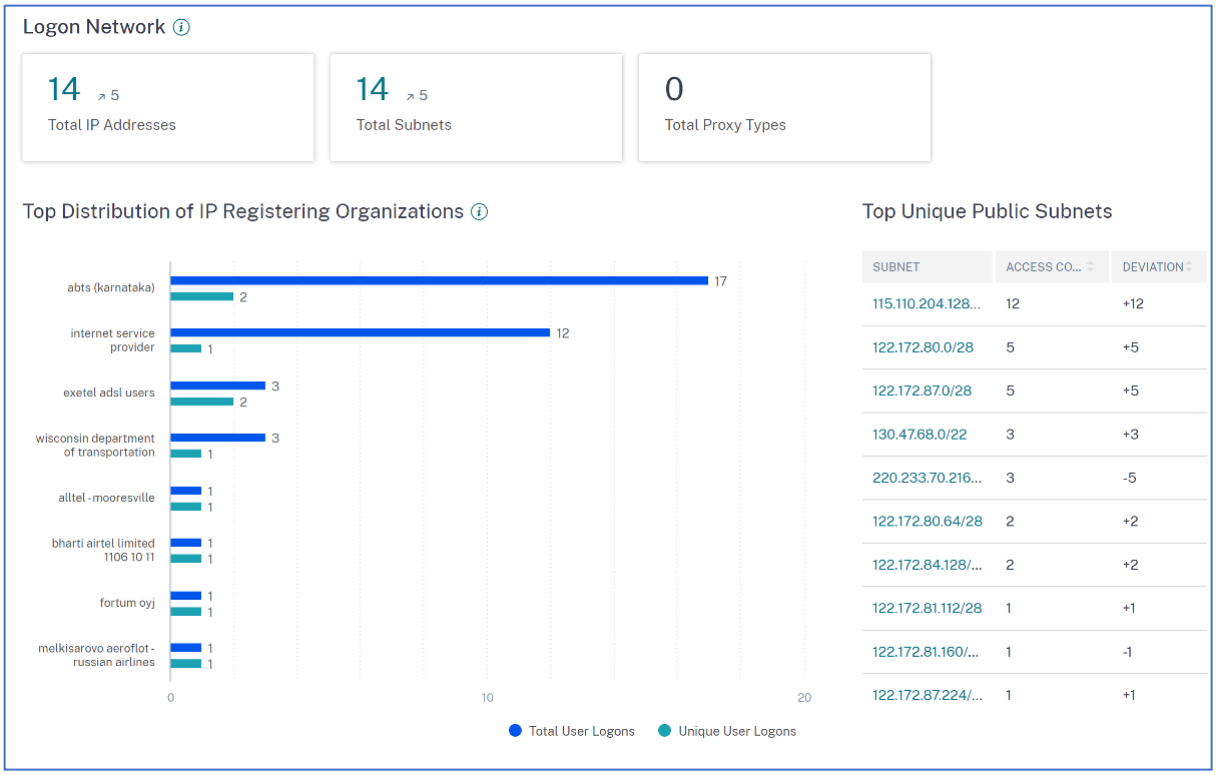
Regierungen, Bildungseinrichtungen und Internetdienstanbieter.

- Das gesamte eindeutige öffentliche Subnetz und das private Subnetz, von dem aus sich die Benutzer angemeldet haben.
- Die Details, die sich der Benutzer mit Proxys und privaten VPN-Diensten angemeldet hat.

Mithilfe dieser zusätzlichen Informationen können Sie als Administrator die Benutzeranmeldedaten überprüfen und sicherstellen, dass die Benutzeranmeldung den Sicherheitsanforderungen der Organisation entspricht.

Benutzernetzwerkdetails anzeigen

Navigieren Sie zu **Sicherheit > Access Assurance** und scrollen Sie nach unten, um Details unter **Logon Network**anzuzeigen.



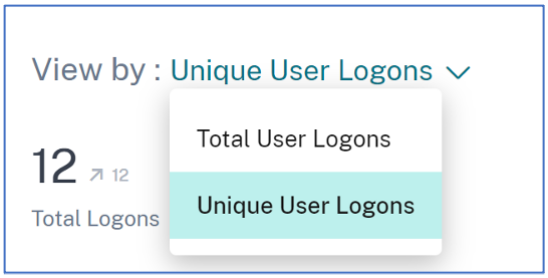
- **IP-Adressen insgesamt**: Gibt die Gesamtzahl der eindeutigen IP-Adressen an, die für die Anmeldung an virtuellen Sitzungen verwendet wurden.
- **Subnetze insgesamt**: Gibt die Gesamtzahl der Subnetze an, die für die Anmeldung an virtuellen Sitzungen verwendet wurden.
- **Gesamtzahl der Proxytypen**: Gibt die Gesamtzahl der Netzwerk- oder Protokolltypen an, die vom Server für den Proxy der Benutzerverbindung verwendet werden.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Unter **Top Distribution of IP Registration Organizations**können Sie sich einen Überblick über die Gesamtzahl der Benutzeranmeldungen und die eindeutigen Anmeldedetails jeder Organisation (ISP) anzeigen lassen. Sie können auf das Diagramm klicken, um die Details der Benutzer sowie deren Zugriffsprofile und Anmeldedetails anzuzeigen, die der ausgewählten Organisation zugeordnet sind.
- Unter **Gesamtzahl eindeutiger öffentlicher Subnetze**können Sie sich einen Überblick über die Subnetze, die Gesamtzahl der Benutzeranmeldungen aus jedem Subnetz und den Abweichungstrend in jedem Subnetz anzeigen lassen. Sie können auf jedes Subnetz klicken, um die Details der Benutzer sowie deren Zugriffsprofile und Anmeldedetails anzuzeigen, die mit dem ausgewählten Subnetz verknüpft sind.

Zugriffsprofile der Benutzer anzeigen

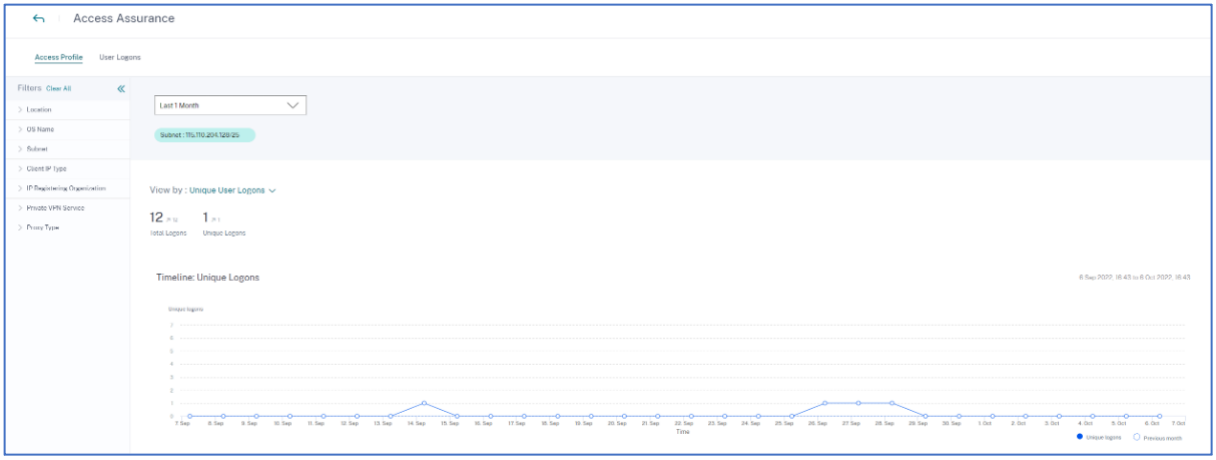
Wenn Sie eine Metrik (Standort, Organisation oder Subnetz) aufschlüsseln, bietet die Seite **Zugriffsprofil** eine Zusammenfassung der Zugriffe Ihrer Benutzer auf virtuelle Apps oder virtuelle Desktops von den ausgewählten Standorten aus. Sie können die Option „Einmaliges Anmelden“oder „Gesamtanmeldung“wählen, um die Trendanalyse für den ausgewählten Zeitraum anzuzeigen.



Sie können die wichtigsten Zugriffsereignisse für die ausgewählte Metrik (Standort, Organisation oder Subnetz) anzeigen. Diese Informationen helfen Ihnen, die Zugriffsmuster und die Details für die Bedrohungsuntersuchung und -analyse zu überprüfen.

Der Aufwärts- oder Abwärtstrend für die Gesamtzahl der Benutzeranmeldungen und der eindeutigen Benutzeranmeldungen wird auf der Grundlage des ausgewählten Zeitraums und des vorherigen Zeitraums gleicher Länge verglichen. Wenn Sie beispielsweise den Zeitraum als **Letzter Monat**auswählen, wird der Trend zwischen dem letzten Monat und dem vorherigen Monat mit dem letzten Monat verglichen.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Facetten

Für die Zugriffsereignisse können Sie folgende Facetten verwenden:

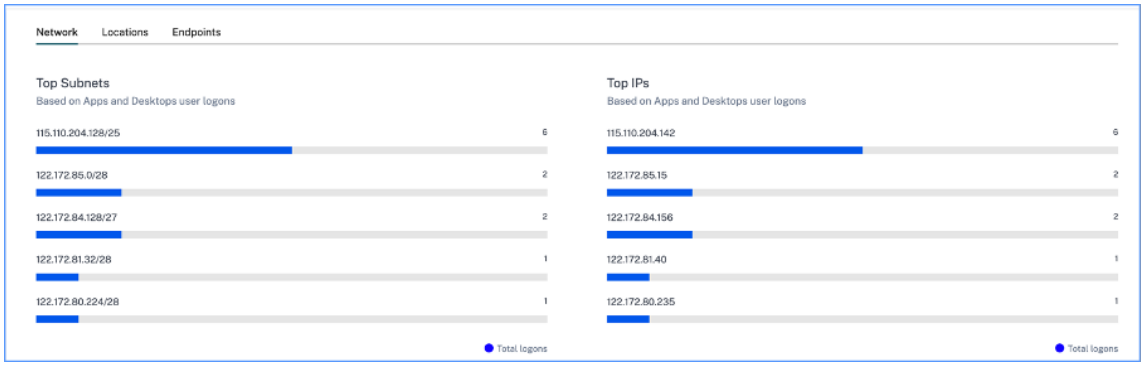
- **Ort**- Filtern Sie die Zugriffsereignisse nach Ländern und ihren Städten.
- **Betriebssystem**- Filtern Sie die Zugriffsereignisse nach den Betriebssystemen und deren Versionen.
- **Subnetz**—Filtert die Zugriffsereignisse nach den Subnetzen.
- **Client-IP-Typ**—Filtert die Zugriffsereignisse nach öffentlichen oder privaten Ereignissen.
- **IP-registrierende Organisation**—Filtert die Organisation, die der öffentlichen IP-Adresse zugeordnet ist.
- **Privater VPN-Dienst**—Filtert die Zugriffsereignisse nach den Namen der privaten VPN-Netzwerke.
- **Proxytyp**—Filtert die Zugriffsereignisse nach den Proxytyp-Klassifizierungen wie HTTP, Web, Tor und SOCKS.

> **Hinweis**
>
> Möglicherweise wird das Label “Nicht verfügbar”auch angezeigt, wenn Daten entweder nicht verfügbar oder nicht identifiziert sind.

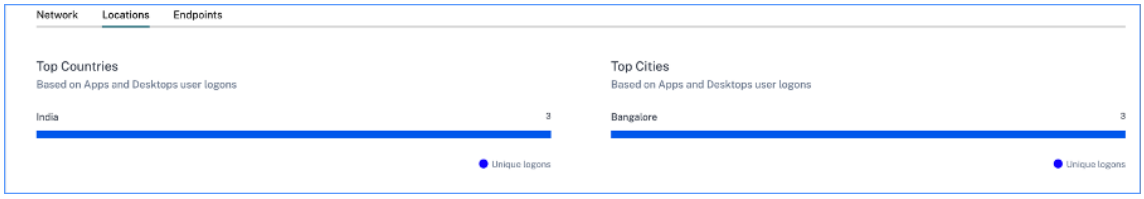
Zeigen Sie auf der Grundlage der angewendeten Filter die folgenden Informationen für die Gesamtzahl der Benutzeranmeldungen und eindeutigen Benutzeranmeldungen an:

- **Netzwerk**—Die wichtigsten Subnetze und die IP-Adressen, von denen aus sich die Benutzer bei virtuellen Apps oder virtuellen Desktops angemeldet haben.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



- **Standorte**—Die wichtigsten Länder und Städte, von denen aus sich die Benutzer bei virtuellen Apps oder virtuellen Desktops angemeldet haben.

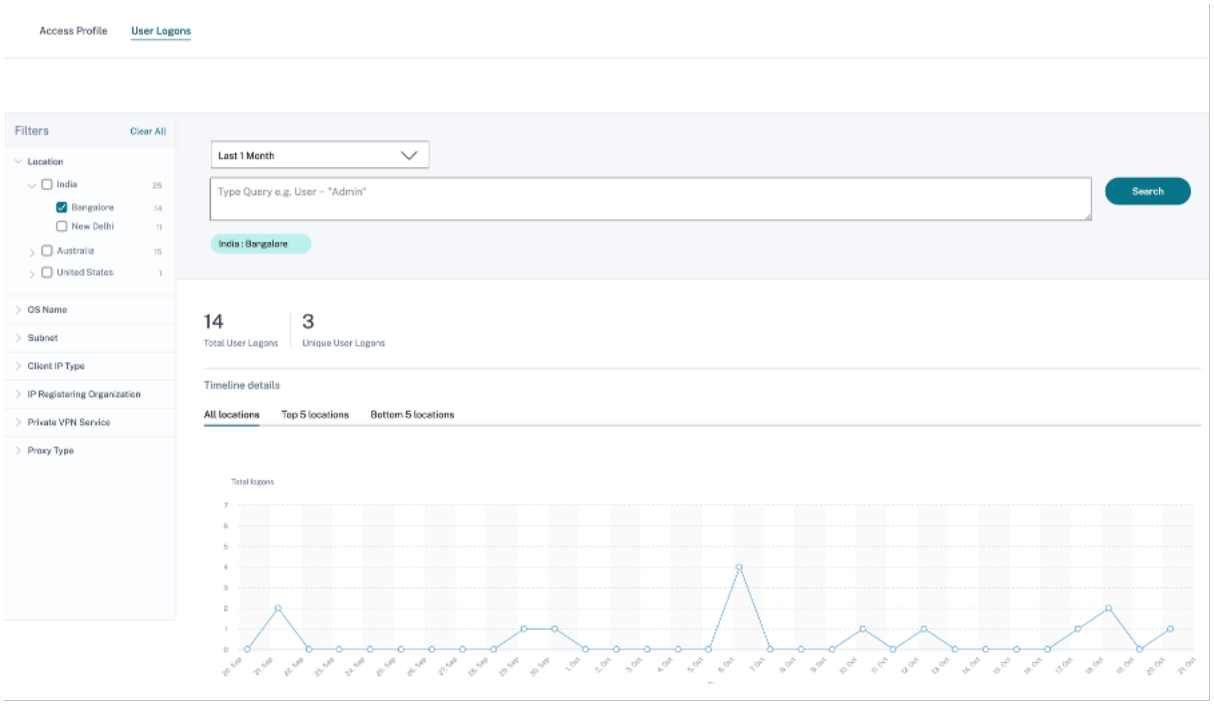


- **Endpunkte**—Die wichtigsten Geräte- und Betriebssystemnamen, die auf Benutzeranmeldungen von Apps und Desktops basieren.

Anmeldedetails von Benutzern anzeigen

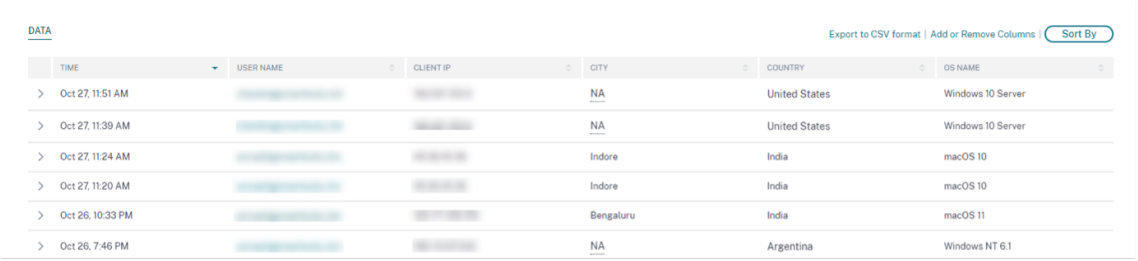
Auf der Seite **Benutzeranmeldungen** werden die Details der Benutzeranmeldungen an virtuellen Apps oder virtuellen Desktops von den ausgewählten Speicherorten aus angezeigt. Diese Informationen helfen Ihnen bei der Untersuchung und Analyse von Bedrohungen.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



In der Tabelle **DATA** werden die folgenden Anmeldedetails für die ausgewählten Standorte und den Zeitraum angezeigt:

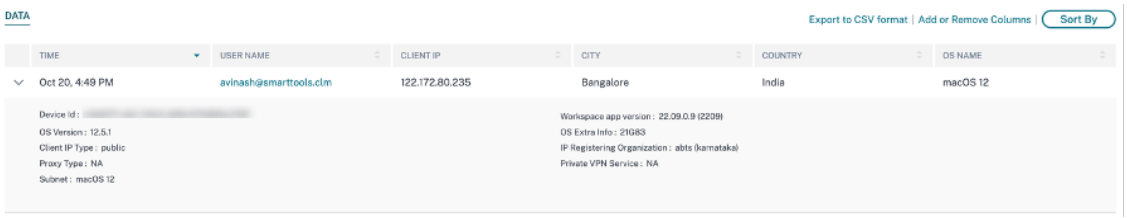
- **Zeit**. Das Datum und die Uhrzeit, zu der sich der Benutzer angemeldet hat.
- **Benutzername**. Die Identität des Nutzers.
- **Client-IP**. Die IP-Adresse des Benutzergeräts.
- **Client-IP-Typ**. Die Art der IP-Adresse des Benutzers, z. B. öffentlich oder privat.
- **Stadt und Land**. Die Standorte, von denen aus sich der Benutzer bei virtuellen Apps oder virtuellen Desktops angemeldet hat.
- **Geräte-ID**. Der Identitätscode des Benutzergeräts.
- **Name des Betriebssystems**. Das Betriebssystem auf dem Benutzergerät. Weitere Informationen finden Sie unter Self-Service-Suche nach Apps und Desktops.



Wenn du jedes Event erweiterst, siehst du die folgenden Details:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Version des Betriebssystems**. Die Version des Betriebssystems auf dem Benutzergerät. Weitere Informationen finden Sie unter Self-Service-Suche nach Apps und Desktops.
- **Zusätzliche Informationen zum Betriebssystem**—Alle zusätzlichen Informationen des Betriebssystems wie Buildnummern, Service Packs und Patches. Weitere Informationen finden Sie unter Self-Service-Suche nach Apps und Desktops.
- **Version der Arbeitsbereich-App**. Die Build-Version der Citrix Workspace-App oder Citrix Receiver.



In der Tabelle **DATA** können Sie die folgenden Vorgänge ausführen:

- Klicken Sie auf **Spalten hinzufügen oder entfernen**, um die Tabellenspalten basierend darauf zu aktualisieren, wie Sie die Daten anzeigen möchten.
- Klicken Sie auf **Sortieren nach**, und wählen Sie die Datenelemente für eine mehrspaltige Sortierung aus. Weitere Informationen finden Sie unter Mehrspaltige Sortierung.
- Klicken Sie auf In **CSV-Format exportieren**, um die in der Tabelle DATA angezeigten Daten in eine CSV-Datei herunterzuladen und für Ihre Analyse zu verwenden.

Suchleiste

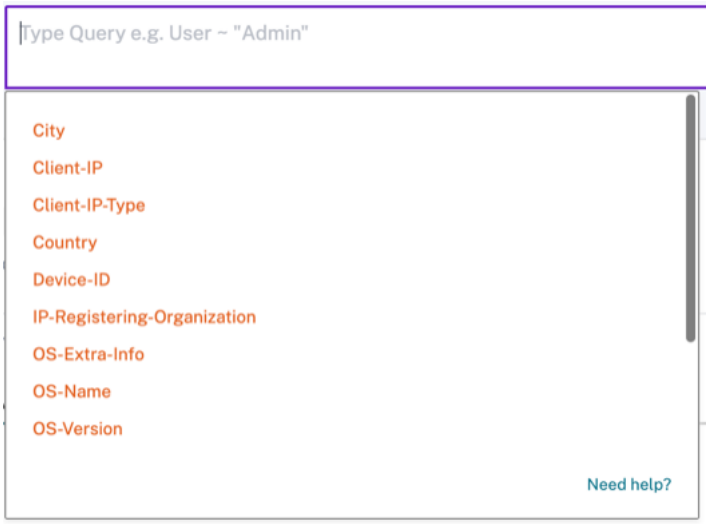
Sie können die Suchleiste auch verwenden, um Ihre Abfrage mithilfe der mit einem Anmeldeereignis verknüpften Dimensionen zu definieren.

Beispiel:

```
User = “test user” AND Client-IP = “10.xx.xx.xx AND Client-IP-Type = public”
```

```
User = “demo_user@citrix.com” AND OS-Major-Version = “macOS 10.13” AND OS-Minor-Version = 6
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Facetten

Sie können die folgenden Facetten für die Anmeldeereignisse verwenden:

- **Standorte**—Filtern Sie die Anmeldeereignisse nach Ländern und ihren Städten.
- **Betriebssystem**—Filtern Sie die Anmeldeereignisse nach Betriebssystem und deren Versionen.
- **Subnetz**—Filtert die Zugriffsereignisse nach den Subnetzen.
- **Client-IP-Typ**—Filtern Sie die Zugriffsereignisse nach öffentlichen und privaten IP-Typen.
- **IP-Registrierungsorganisation**—Filtern Sie die Zugriffsereignisse nach dem vom Benutzer verwendeten ISP.
- **Privater VPN-Dienst**—Filtert die Zugriffsereignisse nach den Namen der privaten VPN-Netzwerke.
- **Proxytyp**—Filtert die Zugriffsereignisse nach den Proxytyp-Klassifizierungen wie HTTP, Web, Tor und SOCKS.

> **Hinweis**
>
> Möglicherweise wird das Label “Nicht verfügbar”auch angezeigt, wenn Daten entweder nicht verfügbar oder nicht identifiziert sind.

Zeitleiste und Profil des Benutzerrisikos

December 12, 2023

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

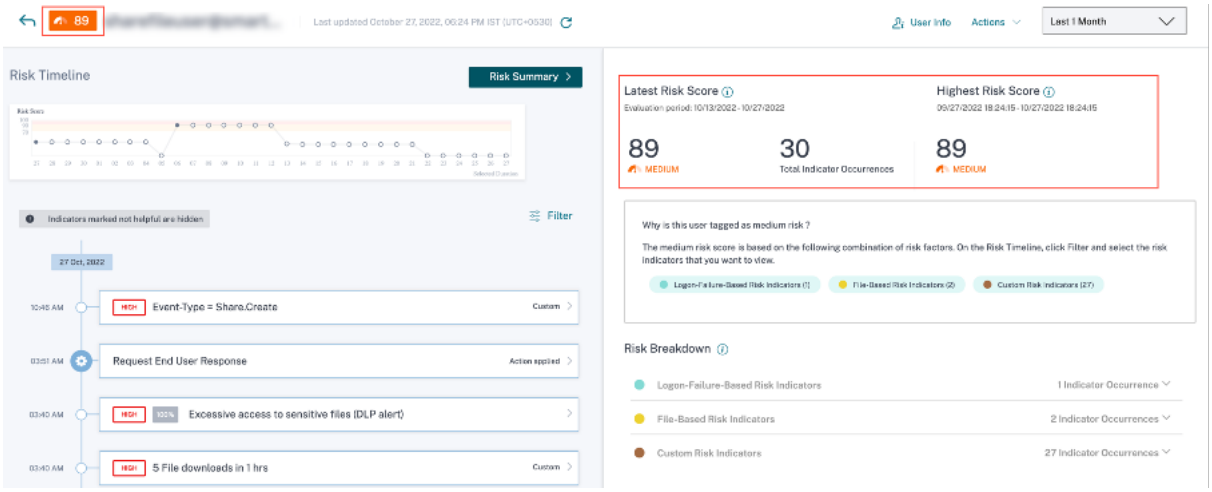
> **Hinweis**
>
> **Achtung**: Citrix Content Collaboration und ShareFile haben das Ende ihrer Lebensdauer erreicht und stehen Benutzern nicht mehr zur Verfügung.

Die Zeitleiste für das Benutzerrisiko im Profil eines Benutzers ermöglicht es Ihnen als Citrix Analytics-Administrator, tiefere Einblicke in das riskante Verhalten eines Benutzers zu erhalten. Standardmäßig wird der Zeitplan für das Benutzerrisiko für den letzten Monat angezeigt. Sie können auch die entsprechenden Aktionen sehen, die für einen ausgewählten Zeitraum auf ihrem Konto durchgeführt wurden. In der Zeitleiste des Benutzerrisikos können Sie tiefer in das Profil eines Benutzers eintauchen, um Folgendes zu verstehen:

- Verwendung der Anwendung
- Verwendung von Daten
- Nutzung der Geräte
- Nutzung von Standorten

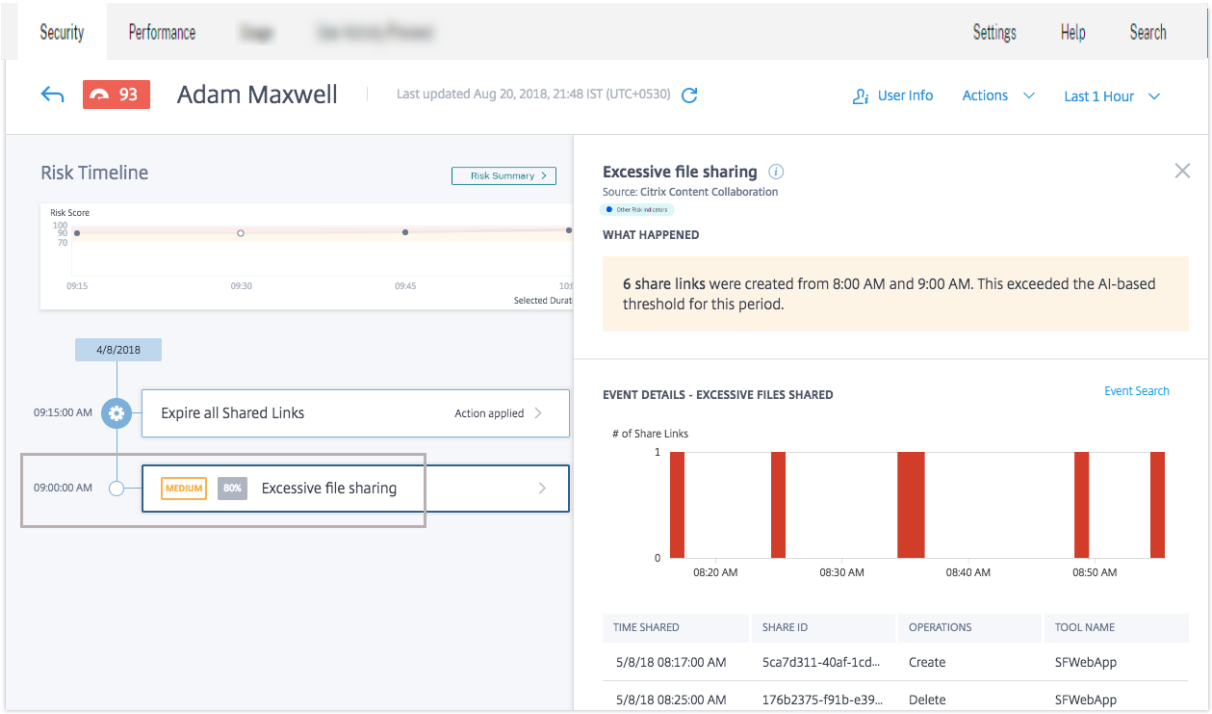
Außerdem können Sie die Risikobewertung und die Risikoindikatortrends für den Benutzer anzeigen und feststellen, ob der Benutzer ein Benutzer mit hohem Risiko ist oder nicht.

Sie können die aktuelle Risikobewertung des Benutzers in der oberen linken Ecke der Timeline-Seite für das Benutzerrisiko einsehen. In den Berichten der **Risikozusammenfassung** werden sowohl die letzten als auch die historischen Höchstwerte angezeigt.



Wenn Sie zum Risikozeitplan eines Benutzers gehen, können Sie entweder einen Risikoindikator oder eine Aktion auswählen, die auf sein Konto angewendet wurde. Wenn Sie eine der oben genannten Optionen wählen, zeigt der rechte Bereich den Risikoindikatorabschnitt oder den Aktionsabschnitt an.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



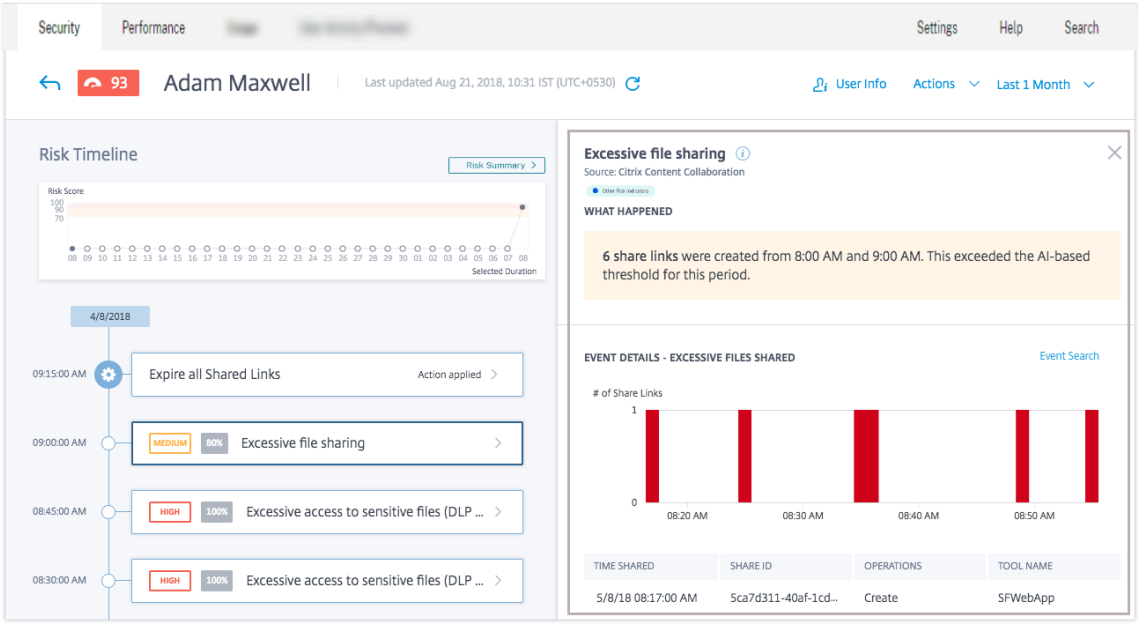
Risiko-Timeline

In der Risikozeitleiste werden die folgenden Informationen angezeigt:

- **Risikoindikatoren**. Risikoindikatoren sind Benutzeraktivitäten, die verdächtig sind oder eine Sicherheitsbedrohung für Ihr Unternehmen darstellen können. Die Indikatoren werden ausgelöst, wenn das Verhalten des Benutzers von seinem normalen Verhalten abweicht. Die Risikoindikatoren können für folgende Datenquellen gelten:
  - Citrix Content Collaboration
  - Citrix Gateway
  - Citrix Endpoint Management
  - Citrix Virtual Apps and Desktops oder Citrix DaaS (früher Citrix Virtual Apps and Desktops Service)
  - Citrix Secure Private Access

  Wenn Sie einen Risikoindikator aus der Zeitleiste des Benutzers auswählen, wird im rechten Bereich der Risikoindikatorinformationen angezeigt. Sie können den Grund für den Risikoindikator zusammen mit Details des Ereignisses anzeigen. Sie sind grob in die folgenden Abschnitte unterteilt:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



- **Was ist passiert**. Eine Zusammenfassung des Risikoindikators können Sie hier einsehen. Zum Beispiel, wenn Sie den Risikoindikator für **übermäßige Dateifreigabe** ausgewählt haben. Im Abschnitt Was passiert ist, können Sie die Anzahl der Freigabelinks anzeigen, die an Empfänger gesendet wurden, und wann das Freigabeereignis stattgefunden hat.
- **Ereignisdetails**. Sie können einzelne Ereigniseinträge in grafischem und tabellarischem Format zusammen mit Details des Ereignisses anzeigen. Klicken Sie auf **Ereignissuche**, um auf die Self-Service-Suchseite zuzugreifen und die Ereignisse anzuzeigen, die dem Risikoindikator des Benutzers entsprechen Weitere Informationen finden Sie unter **Self-Service-Suche**.
- **Zusätzliche kontextbezogene Informationen**. In diesem Abschnitt können Sie gegebenenfalls während des Auftretens eines Ereignisses geteilte Daten anzeigen.

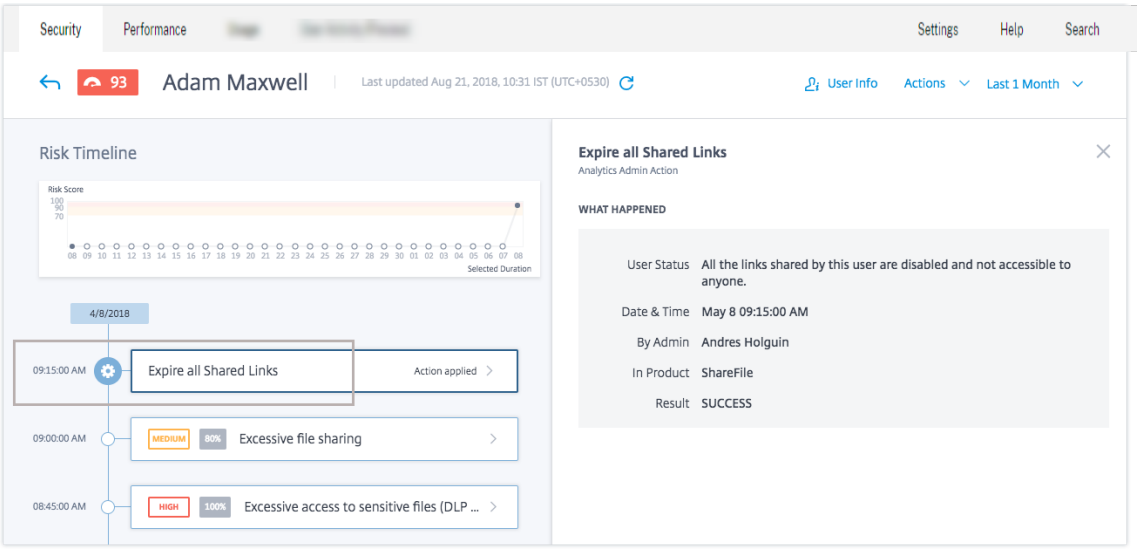
Sie können Risikoindikatoren manuell als hilfreich oder nicht hilfreich markieren. Weitere Informationen finden Sie unter Feedback zu Indikatoren für Benutzerrisiken.

Erfahren Sie mehr: Risikoindikatoren

- **Aktionen**. Aktionen helfen Ihnen, auf verdächtige Ereignisse zu reagieren und das Auftreten zukünftiger anomaler Ereignisse zu verhindern. Aktionen, die auf das Profil eines Benutzers angewendet wurden, werden auf der Risikozeitleiste angezeigt. Diese Aktionen werden entweder automatisch über konfigurierte Richtlinien auf das Konto eines Benutzers angewendet oder Sie können eine bestimmte Aktion manuell anwenden.

  Erfahren Sie mehr: Richtlinien und Aktionen.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



- **Privilegierte Benutzerereignisse**. Privilegierte Benutzerereignisse werden jedes Mal ausgelöst, wenn sich der Admin- oder Executive-Berechtigungsstatus eines Benutzers ändert. Wenn ein Risikoindikator für einen Benutzer ausgelöst wird, können Sie ihn mit dem angegebenen Ereignis zur Änderung des Berechtigungsstatus in Beziehung setzen. Bei Bedarf können Sie die entsprechende Aktion auf das Benutzerprofil anwenden. Die in der Zeitleiste des Benutzerrisikos angezeigten Admin- oder Exekutivberechtigungsereignisse lauten wie folgt

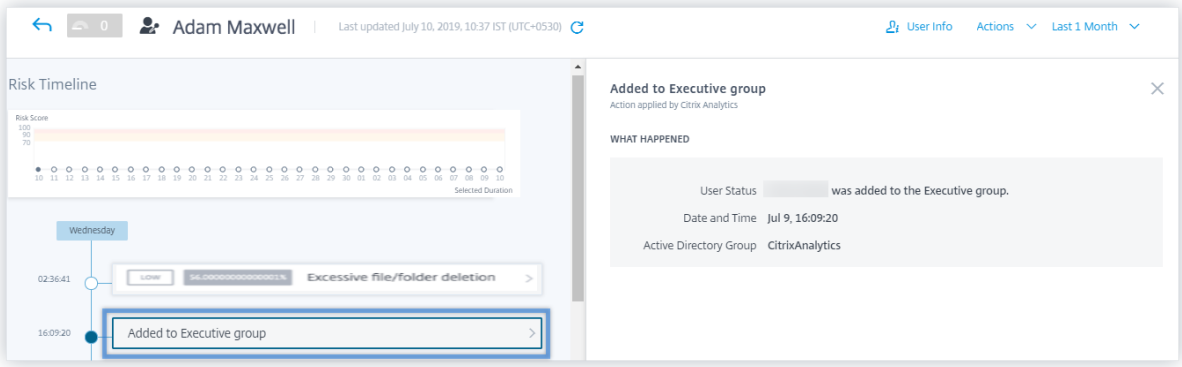
  - Zur Executive-Gruppe hinzugefügt
  - Aus Executive-Gruppe entfernt
  - Privileg auf Admin erhöht
  - Admin-Berechtigung wurde entfernt

  Betrachten Sie den Benutzer Adam Maxwell, der zur privilegierten Executive-Gruppe **CitrixAnalytics**hinzugefügt wurde. Das Ereignis **"Zur Führungsgruppe** hinzugefügt"wird zur Risikozeitleiste des Benutzers hinzugefügt. Jetzt beginnt Adam, übermäßig viele Dateien und Ordner zu löschen, und löst den Algorithmus für maschinelles Lernen aus, der ungewöhnliches Verhalten erkennt. Der Risikoindikator für **übermäßiges Löschen von Dateien oder Ordnern** wird der Risikozeitleiste des Benutzers hinzugefügt. Sie können das Ereignis und den Risikoindikator auf der Risikozeitleiste vergleichen. Nach dem Vergleich können Sie feststellen, ob der Risikoindikator als Folge des Ereignisses ausgelöst wurde. In diesem Fall können Sie entsprechende Aktionen auf Adams Profil anwenden. Weitere Informationen zu privilegierten Benutzern finden Sie unter Privilegierte Benutzer.

Wenn Sie ein Ereignis aus der Timeline des Benutzers auswählen, wird der Abschnitt mit den Ereignisinformationen im rechten Bereich angezeigt.

Für eine Führungskraft werden im rechten Bereich Informationen wie **Benutzerstatus**, **Datum und Uhrzeit sowieActive Directory-Gruppe**angezeigt.

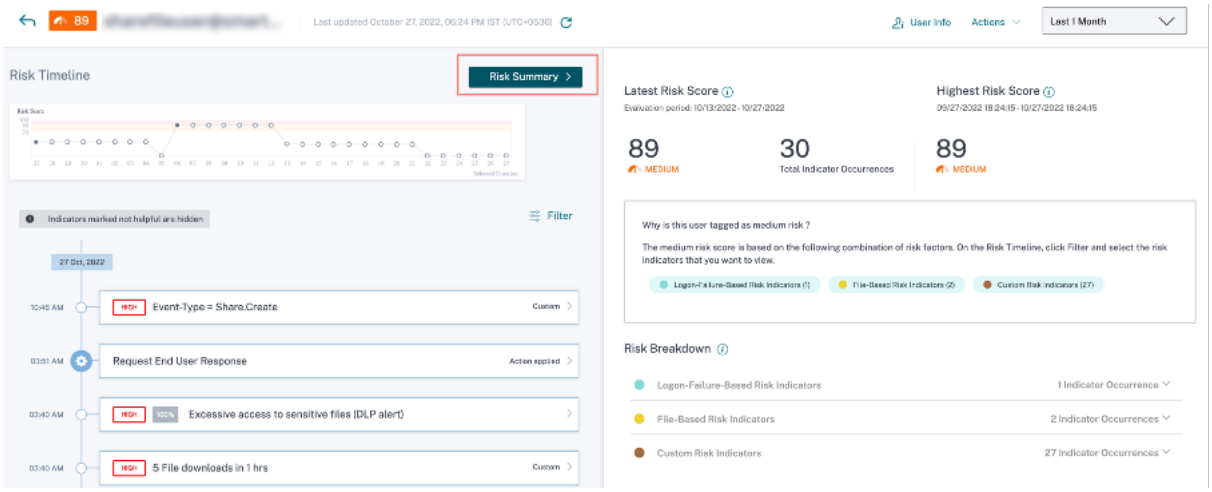
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Für ein Admin-Berechtigungsereignis werden im rechten Bereich Informationen wie **Benutzerstatus**, **Datum und Uhrzeit**sowie **In-Produkt**angezeigt.

Zusammenfassung des Risikos

Zeigen Sie die mit dem Benutzer verbundenen Risikofaktoren an, die zu seiner Risikobewertung beigetragen haben. Sie können die Details zur Risikobewertung sehen, die im ausgewählten Zeitraum als Maximum angesehen wurden, zusammen mit dem neuesten Ergebnis und der entsprechenden Anzahl der Risikoindikatoren. Wenn Sie entweder von der Haupt-Landingpage oder der Seite Risky Users zur Benutzer-Timeline navigieren, wird die Zeitauswahl von der Quellseite beibehalten. Weitere Informationen zu den Risikofaktoren finden Sie unter Citrix Benutzerrisikoindikatoren.



Klicken Sie auf **Risikoübersicht**, um die folgenden Informationen anzuzeigen:

- **Aktuelle Risikobewertung**: Die neueste Risikobewertung gibt das aktuelle Risiko des Benutzers auf der Grundlage des jüngsten Verhaltens an. Die Risikobewertung bestimmt das Risiko, das ein Benutzer für ein Unternehmen über einen Zeitraum von zwei Wochen darstellt. Der Risiko-Score-Wert ist dynamisch und variiert basierend auf der Analyse des Benutzerverhaltens. Basierend auf der Bewertung kann ein Benutzer in eine der folgenden Kategorien fallen:

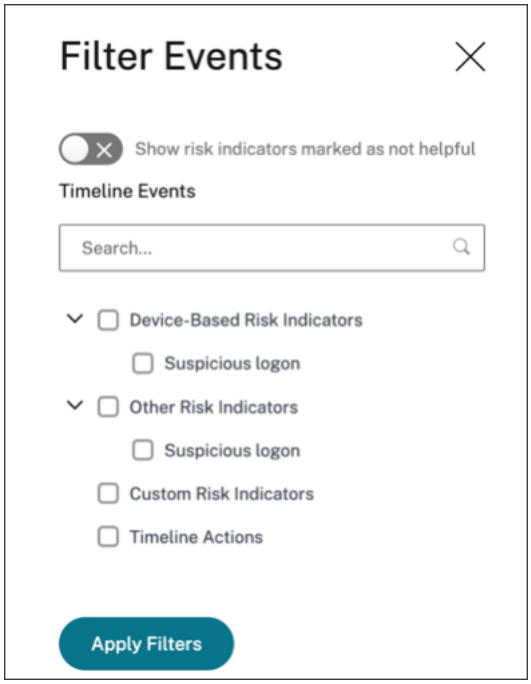
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Benutzer mit hohem Risiko, Benutzer mit mittlerem Risiko, Benutzer mit niedrigem Risiko und Benutzer mit einem Risikowert von Null. Weitere Informationen zu den Benutzerkategorien finden Sie unter Benutzer-Dashboard.

  - **Gesamtzahl der Indikatorvorkommen**: Gibt die Gesamtzahl der vom Benutzer in den letzten zwei Wochen ausgelösten Risikoindikatoren an. Diese ausgelösten Risikoindikatoren bestimmen die Risikobewertung des Benutzers.

- **Höchster Risikowert**: Der höchste Risikowert gibt den Höchstwert der Risikobewertungen an, die für diesen Benutzer innerhalb der ausgewählten Zeitdauer berechnet wurden. Sie ist repräsentativ für das Gesamtrisiko für den Benutzer und entspricht möglicherweise nicht immer der aktuellen Risikobewertung.
- **Risikofaktoren**: Gibt eine oder mehrere Kombinationen der Risikofaktoren an, die mit den Benutzeraktivitäten verbunden sind, die zur Risikobewertung beigetragen haben.
- **Risikoaufschlüsselung**: Gibt die Anzahl der Risikoindikatoren an, die der Benutzer für jeden Risikofaktor ausgelöst hat. Erweitern Sie die Zeile, um die Details anzuzeigen.

Klicken Sie in der Benutzerzeitleiste auf **Filtern** und wählen Sie die Risikofaktoren, die angewendeten Aktionen oder den Status des privilegierten Benutzers aus, der dem Benutzer zugeordnet ist, und zeigen Sie die entsprechenden Ereignisse an.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Benutzerprofil

Auf der **Benutzerprofilseite** werden die folgenden Benutzerinformationen angezeigt, die aus dem Active Directory des Benutzers stammen:

- Berufsbezeichnung
- Adresse
- E-Mail
- Telefon
- Standort
- Organisation

Citrix Benutzerrisikoindikatoren

April 12, 2024

> **Hinweis**
>
> **Achtung**: Citrix Content Collaboration und ShareFile haben das Ende ihrer Lebensdauer erreicht und stehen Benutzern nicht mehr zur Verfügung.

Benutzerrisikoindikatoren sind Benutzeraktivitäten, die verdächtig aussehen oder eine Sicherheitsbedrohung für Ihr Unternehmen darstellen können. Diese Risikoindikatoren erstrecken sich über alle Citrix Produkte, die in Ihrer Bereitstellung verwendet werden. Die Risikoindikatoren werden ausgelöst, wenn das Verhalten des Benutzers vom Normalwert abweicht. Jeder Risikoindikator kann einen oder mehrere Risikofaktoren aufweisen. Diese Risikofaktoren helfen Ihnen, die Art der Anomalien in den Benutzerereignissen zu bestimmen. Die Risikoindikatoren und die damit verbundenen Risikofaktoren bestimmen den Risiko-Score eines Nutzers.

Im Folgenden sind die mit den Risikoindikatoren verbundenen Risikofaktoren aufgeführt:

- **Gerätebasierte Risikoindikatoren**: Wird ausgelöst, wenn sich ein Benutzer von einem Gerät aus anmeldet, das aufgrund des Geräteverlaufs des Benutzers als ungewöhnlich angesehen wird.
- **Standortbasierte Risikoindikatoren**: Wird ausgelöst, wenn sich ein Benutzer von einer IP-Adresse aus anmeldet, die mit einem Standort verknüpft ist, der aufgrund des Standortverlaufs des Benutzers als ungewöhnlich angesehen wird.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **IP-basierte Risikoindikatoren**: Wird ausgelöst, wenn ein Benutzer versucht, von einer als verdächtig identifizierten IP-Adresse auf Ressourcen zuzugreifen, unabhängig davon, ob die IP-Adresse für den Benutzer ungewöhnlich ist.
- **Auf Anmeldefehlern basierende Risikoindikatoren**: Wird ausgelöst, wenn ein Benutzer ein Muster übermäßiger oder ungewöhnlicher Anmeldefehler aufweist.
- **Datenbasierte Risikoindikatoren**: Wird ausgelöst, wenn ein Benutzer versucht, Daten aus einer Workspace-Sitzung zu exfiltrieren. Zu den beobachteten Benutzerverhalten gehören Ereignisse zum Kopieren oder Einfügen, Download-Muster usw.
- **Dateibasierte Risikoindikatoren**: Wird ausgelöst, wenn das Verhalten eines Benutzers in Bezug auf den Dateizugriff auf Content Collaboration aufgrund seines historischen Zugriffsmusters als ungewöhnlich angesehen wird. Zu den beobachteten Benutzerverhalten gehören Download-Muster, Zugriff auf vertrauliche Inhalte, Aktivitäten, die auf Ransomware hinweisen, und so weiter.
- **Benutzerdefinierte Risikoindikatoren**: Wird ausgelöst, wenn eine vorkonfigurierte Bedingung oder eine benutzerdefinierte Bedingung erfüllt ist. Weitere Informationen finden Sie in den folgenden Artikeln:
  - Benutzerdefinierte Risikoindikatoren
  - Vorkonfigurierte benutzerdefinierte Risikoindikatoren und Richtlinien
- Andere Risikoindikatoren- Die Risikoindikatoren, die zu keinem der vordefinierten Risikofaktoren gehören, z. B. gerätebasiert, standortbasiert und fehlerbasiert bei der Anmeldung.

Die Risikoindikatoren werden auf der Grundlage der ähnlichen Risiken ebenfalls in Risikokategorien eingeteilt. Weitere Informationen finden Sie unter Risikokategorien.

Die folgende Tabelle zeigt die Korrelation zwischen den Risikoindikatoren, Risikofaktoren und den Risikokategorien.

Produkte	Indikator für das Benutzerrisiko	Risikofaktor	Kategorie Risiko
Citrix Endpoint Management	Gerät mit Apps auf der Sperrliste erkannt	Andere Risikoindikatoren	Kompromittierte Endpunkte
	Jailbreak oder gerootetes Gerät erkannt	Andere Risikoindikatoren	Kompromittierte Endpunkte
	Nicht verwaltetes Gerät erkannt	Andere Risikoindikatoren	Kompromittierte Endpunkte

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Produkte	Indikator für das Benutzerrisiko	Risikofaktor	Kategorie Risiko
Citrix Gateway	Fehler beim Scannen der Endpunktanalyse (EPA)	Andere Risikoindikatoren	Kompromittierte Benutzer
	Übermäßige Authentifizierungsfehler	Auf Anmeldeausfällen basierende Risikoindikatoren	Kompromittierte Benutzer
	Unmögliche Reisen	Standortbasierte Risikoindikatoren	Kompromittierte Benutzer
	Anmeldung von verdächtiger IP	IP-basierte Risikoindikatoren	Kompromittierte Benutzer
	Verdächtige Anmeldung	Gerätebasierte Risikoindikatoren, IP-basierte Risikoindikatoren, standortbasierte Risikoindikatoren und andere Risikoindikatoren	Kompromittierte Benutzer
	Ungewöhnlicher Authentifizierungsfehler	Auf Anmeldeausfällen basierende Risikoindikatoren	Kompromittierte Benutzer
Citrix Secure Private Access	Versuch, auf eine URL auf der Sperrliste zuzugreifen	Andere Risikoindikatoren	Insider-Bedrohungen
	Übermäßiger Datendownload	Andere Risikoindikatoren	Insider-Bedrohungen
	Zugriff auf riskante Website	Andere Risikoindikatoren	Insider-Bedrohungen
	Ungewöhnliches Uploadvolumen	Andere Risikoindikatoren	Insider-Bedrohungen

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Produkte	Indikator für das Benutzerrisiko	Risikofaktor	Kategorie Risiko
Citrix DaaS (früher Citrix Virtual Apps and Desktops Service) und on-premises Citrix Virtual Apps and Desktops	Unmögliche Reisen	Standortbasierte Risikoindikatoren	Kompromittierte Benutzer
	Potenzielle Datenexfiltration	Datenbasierte Risikoindikatoren	Exfiltration von Daten
	Verdächtige Anmeldung	Gerätebasierte Risikoindikatoren, IP-basierte Risikoindikatoren, standortbasierte Risikoindikatoren und andere Risikoindikatoren	Kompromittierte Benutzer

Sie können Risikoindikatoren manuell als hilfreich oder nicht hilfreich markieren. Weitere Informationen finden Sie unter Feedback zu Indikatoren für Benutzerrisiken.

Citrix Endpoint Management-Risikoindikatoren

May 4, 2022

Gerät mit Apps auf der Sperrliste erkannt

Citrix Analytics erkennt Zugriffsbedrohungen basierend auf Aktivitäten in einem Gerät mit gesperrten Apps und löst den entsprechenden Risikoindikator aus.

Der Risikoindikator **Gerät mit Apps auf der Sperrliste** wird ausgelöst, wenn der Endpoint Management Dienst während der Softwareinventur eine App auf der Sperrliste erkennt. Die Warnung stellt sicher, dass nur autorisierte Apps auf Geräten ausgeführt werden, die sich im Netzwerk Ihrer Organisation befinden.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Der Risikofaktor, der mit dem Gerät verbunden ist, bei dem gesperrte App erkannt wurden, sind die anderen Risikoindikatoren. Weitere Informationen zu den Risikofaktoren finden Sie unter Citrix Benutzerrisikoindikatoren.

Wann wird das Gerät mit gefundenen Apps auf der Sperrliste ausgelöst?

Der Risikoindikator **Gerät mit Apps auf der Sperrliste erkannt** wird, wird gemeldet, wenn Apps auf dem Gerät eines Benutzers auf der Sperrliste erkannt werden. Wenn der Endpoint Management Dienst eine oder mehrere Apps auf der Sperrliste auf einem Gerät während der Softwareinventur erkennt, wird ein Ereignis an Citrix Analytics gesendet.

Citrix Analytics überwacht diese Ereignisse und aktualisiert den Risikowert des Benutzers. Außerdem fügt es ein **Gerät mit auf Apps auf der Sperrliste erkannt** Risikoindikatoreintrag zur Risikozeitleiste des Benutzers hinzu.

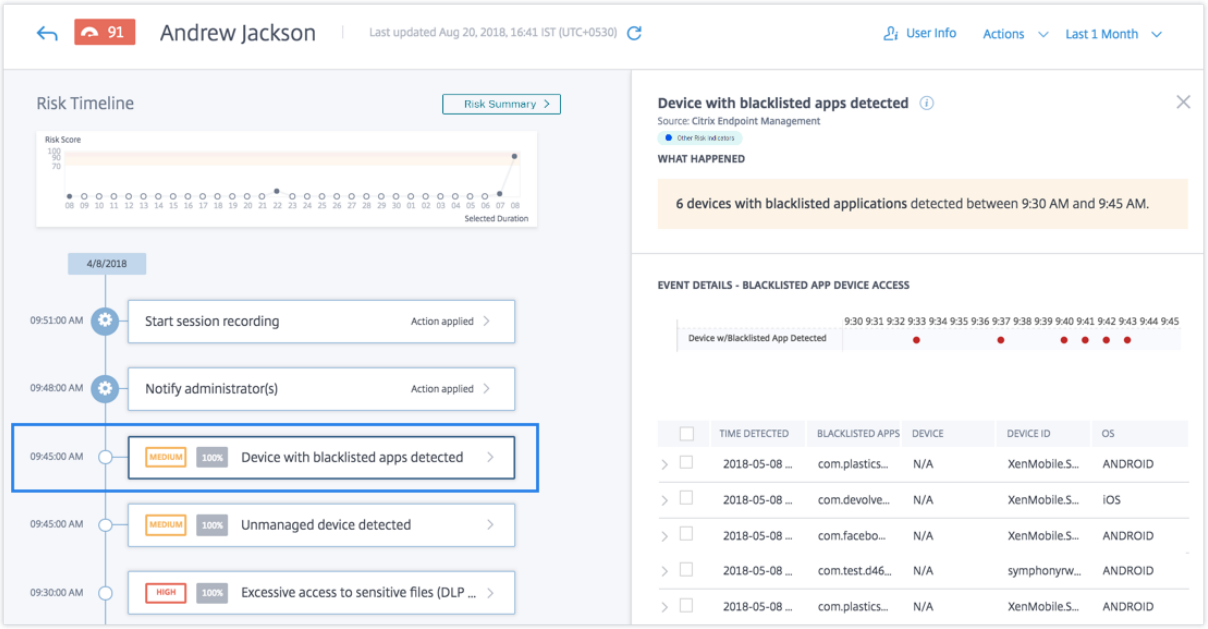
Wie analysiert man das Gerät mit dem Risikofaktor "Apps auf der Sperrliste erkannt"?

Betrachten Sie den Benutzer Andrew Jackson, der ein Gerät verwendet hat, auf dem kürzlich Apps auf der Sperrliste installiert wurden. Endpoint Management meldet diese Bedingung an Citrix Analytics, die Andrew Jackson eine aktualisierte Risikobewertung zuweist.

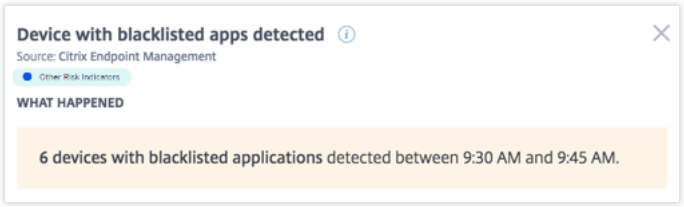
Aus der Risikozeitleiste von Andrew Jackson können Sie den gemeldeten Risikoindikator **Gerät mit auf Apps auf der Sperrliste erkannt** auswählen. Der Grund für das Ereignis wird zusammen mit Details wie der Liste der Apps auf der Sperrliste angezeigt, der Zeitpunkt, zu dem Endpoint Management die App auf der Sperrliste erkannt hat usw.

Um den Risikoindikator **Gerät mit auf Apps auf der Sperrliste erkannt** für einen Benutzer anzuzeigen, navigieren Sie zu **Sicherheit > Benutzer**, und wählen Sie den Benutzer aus.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

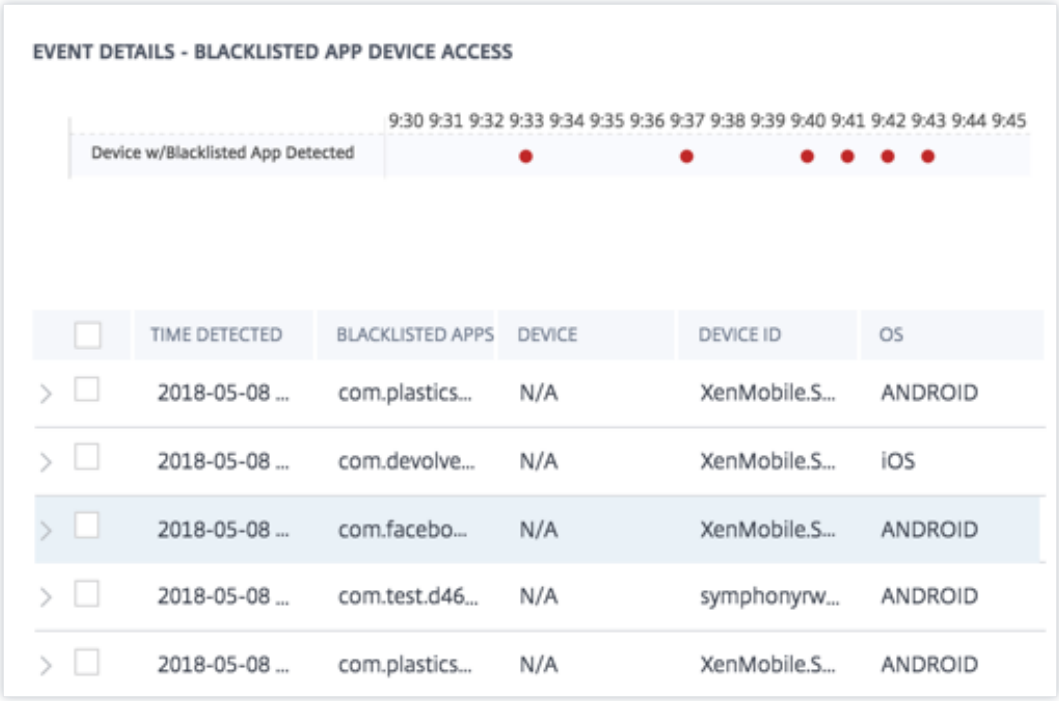


- Im Abschnitt **WAS PASSIERT IST**, können Sie die Zusammenfassung des Ereignisses anzeigen. Sie können die Anzahl der Geräte mit Anwendungen auf der Sperrliste anzeigen, die vom Endpoint Management-Dienst erkannt wurden, und den Zeitpunkt, zu dem die Ereignisse aufgetreten sind.



- Im Abschnitt **EREIGNISDETAILS** —**BLACKLISTED APP DEVICE ACCESS** werden die Ereignisse in grafischem und tabellarischem Format angezeigt. Die Ereignisse werden auch als einzelne Einträge im Diagramm angezeigt, und die Tabelle enthält folgende Schlüsselinformationen:
  - **Erfasste Zeit**- Wenn das Vorhandensein von Apps auf der Sperrliste von Endpoint Management gemeldet wurde.
  - **Apps auf der Sperrliste**- Die Apps auf der Sperrliste auf dem Gerät.
  - **Gerät**- Das verwendete Mobilgerät.
  - **Geräte-ID**- Informationen über die ID des Geräts, das zur Anmeldung bei der Sitzung verwendet wird.
  - **Betriebssystem**- Das Betriebssystem des Mobilgeräts.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



> **Hinweis**
>
> Zusätzlich zum Anzeigen der Details in einem Tabellenformat können Sie auf den Pfeil gegen die Instanz einer Warnung klicken, um weitere Details anzuzeigen.

Welche Aktionen können Sie auf den Benutzer anwenden?

Sie können die folgenden Aktionen für das Benutzerkonto ausführen:

- **Zur Merkliste hinzufügen**. Wenn Sie einen Benutzer auf zukünftige potenzielle Bedrohungen überwachen möchten, können Sie ihn einer Watchlist hinzufügen.
- **Benachrichtigen Sie Administrator (s)**. Bei ungewöhnlichen oder verdächtigen Aktivitäten im Benutzerkonto wird eine E-Mail-Benachrichtigung an alle oder ausgewählte Administratoren gesendet.

Weitere Informationen zu Aktionen und deren manueller Konfiguration finden Sie unter Richtlinien und Aktionen.

Um die Aktionen manuell auf den Benutzer anzuwenden, navigieren Sie zum Profil des Benutzers und wählen Sie den entsprechenden Risikoindikator aus. Wählen Sie im Menü **Aktionen** eine Aktion aus und klicken Sie auf **Übernehmen**.

> **Hinweis**
>
> Unabhängig von der Datenquelle, die einen Risikoindikator auslöst, können Aktionen in Bezug

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> auf andere Datenquellen angewendet werden.

Jailbreak oder gerootetes Gerät erkannt

Citrix Analytics erkennt Zugriffsbedrohungen basierend auf Jailbreak- oder Root-Geräteaktivitäten und löst den entsprechenden Risikoindikator aus.

Die Risikoanzeige für **Geräte mit Jailbreak oder Root** wird ausgelöst, wenn ein Benutzer ein Gerät mit Jailbreak oder Root verwendet, um eine Verbindung zum Netzwerk herzustellen. Secure Hub erkennt das Gerät und meldet den Vorfall an den Endpoint Management Dienst. Die Warnung stellt sicher, dass sich nur autorisierte Benutzer und Geräte im Netzwerk Ihres Unternehmens befinden.

Der mit dem Risikoindikator für Jailbroken oder Rooted Device verbundene Risikofaktor sind die anderen Risikoindikatoren. Weitere Informationen zu den Risikofaktoren finden Sie unter Citrix Benutzerrisikoindikatoren.

Wann wird der Risikoindikator für Jailbroken oder Rooting Device ausgelöst?

Es ist wichtig, dass Sicherheitsbeauftragte sicherstellen können, dass Benutzer über netzwerkkompatible Geräte eine Verbindung herstellen. Der Risikoindikator mit **Jailbreak oder Root-Gerät erkennt** Sie an Benutzer mit iOS-Geräten mit Jailbreak oder Android-Geräten, die gerootet sind.

Der Risikoindikator für **Geräte mit Jailbreak oder Root** wird ausgelöst, wenn ein registriertes Gerät Jailbreak oder Root erhält. Secure Hub erkennt das Ereignis auf dem Gerät und meldet es an den Endpoint Management-Dienst.

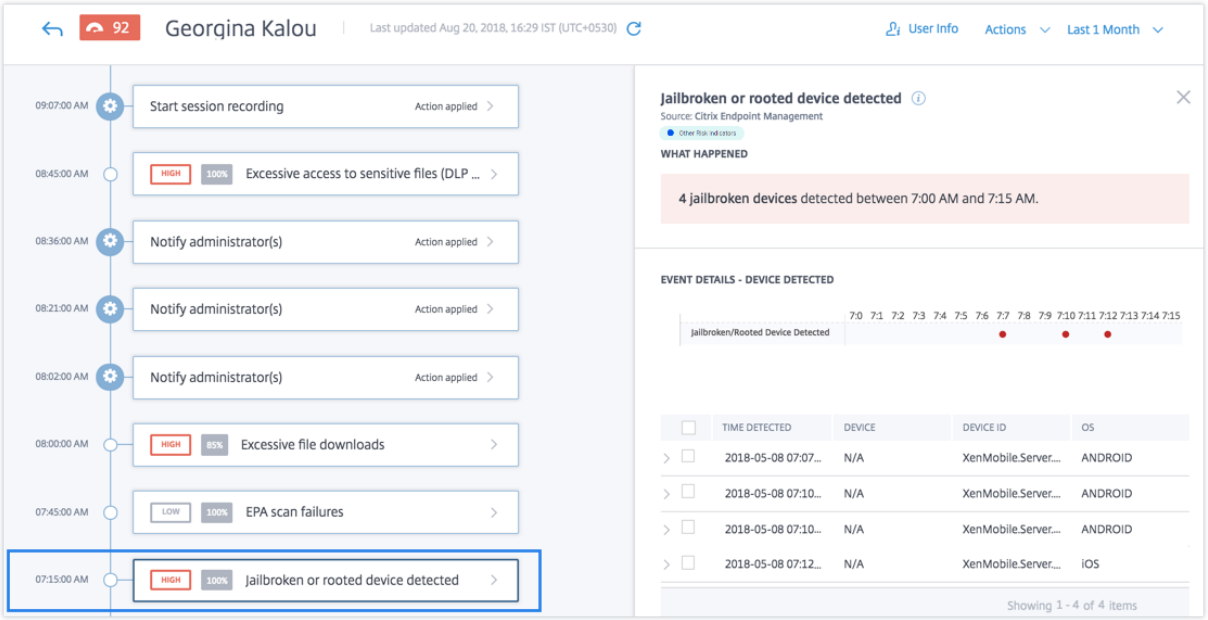
Wie analysiert man den erkannten Risikoindikator mit Jailbreak oder Root-Gerät?

Betrachten Sie die Benutzerin Georgina Kalou, deren registrierte iOS-Gerät kürzlich einen Jailbreak hatte. Dieses verdächtige Verhalten wird von Citrix Analytics erkannt und Georgina Kalou wird eine Risikobewertung zugewiesen.

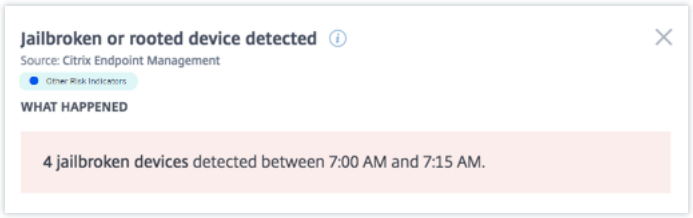
Aus der Risikozeitleiste von Georgina Kalou können Sie den gemeldeten Risikoindikator für **Jailbroken oder verwurzelte Geräte** auswählen. Der Grund für das Ereignis wird zusammen mit den Details wie der Zeitpunkt der Auslösung des Risikoindikators, Beschreibung des Ereignisses usw. angezeigt.

Um den Risikoindikator mit **Jailbreak oder gerootetes Gerät** für einen Benutzer anzuzeigen, navigieren Sie zu **Sicherheit > Benutzer**und wählen Sie den Benutzer aus.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

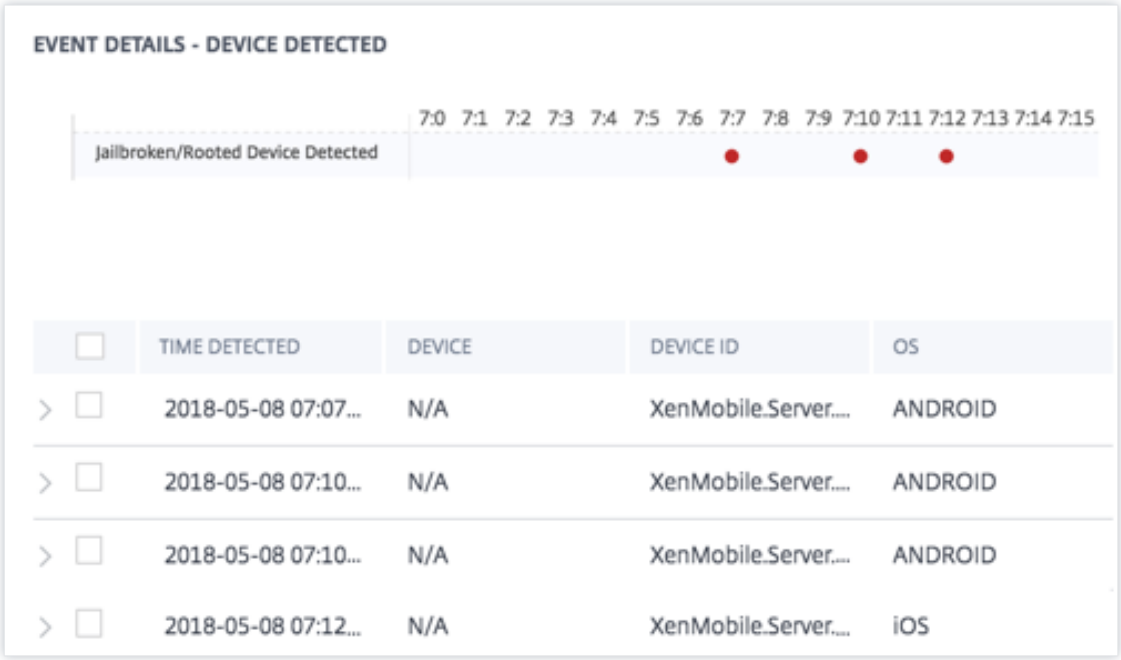


- Im Abschnitt **WAS PASSIERT IST**, können Sie die Zusammenfassung des Ereignisses anzeigen. Sie können die Anzahl der erkannten Geräte mit Jailbreak oder Root sowie den Zeitpunkt des Auftretens der Ereignisse anzeigen.



- Im Abschnitt **EREIGNISDETAILS** —**DEVICE DETECTED** werden die Ereignisse in grafischem und tabellarischem Format angezeigt. Die Ereignisse werden auch als einzelne Einträge im Diagramm angezeigt, und die Tabelle enthält folgende Schlüsselinformationen:
  - **Zeit erkannt**. Die Zeit, zu der das Gerät mit Jailbreak oder Root erkannt wird.
  - **Gerät**. Das verwendete Mobilgerät.
  - **Geräte-ID**. Informationen über die ID des Geräts, das zur Anmeldung an der Sitzung verwendet wird.
  - **Betriebssystem**. Das Betriebssystem des Mobilgeräts.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



> **Hinweis Klicken Sie**
>
> zusätzlich zum Anzeigen der Details im Tabellenformat auf den Pfeil gegen die Instanz einer Warnung, um weitere Details anzuzeigen.

Welche Aktionen können Sie auf den Benutzer anwenden?

Sie können die folgenden Aktionen für das Benutzerkonto ausführen:

- **Zur Merkliste hinzufügen**. Wenn Sie einen Benutzer auf zukünftige potenzielle Bedrohungen überwachen möchten, können Sie ihn einer Watchlist hinzufügen.
- **Benachrichtigen Sie Administrator (s)**. Bei ungewöhnlichen oder verdächtigen Aktivitäten im Benutzerkonto wird eine E-Mail-Benachrichtigung an alle oder ausgewählte Administratoren gesendet.

Weitere Informationen zu Aktionen und deren manueller Konfiguration finden Sie unter Richtlinien und Aktionen.

Um die Aktionen manuell auf den Benutzer anzuwenden, navigieren Sie zum Profil des Benutzers und wählen Sie den entsprechenden Risikoindikator aus. Wählen Sie im Menü **Aktionen** eine Aktion aus und klicken Sie auf **Übernehmen**.

> **Hinweis**

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> Unabhängig von der Datenquelle, die einen Risikoindikator auslöst, können Aktionen in Bezug auf andere Datenquellen angewendet werden.

Nicht verwaltetes Gerät erkannt

Citrix Analytics erkennt Zugriffsbedrohungen basierend auf nicht verwalteten Geräteaktivitäten und löst den entsprechenden Risikoindikator aus.

Der Risikoindikator für **nicht verwaltetes Gerät** wird ausgelöst, wenn ein Gerät:

- Aufgrund einer automatisierten Aktion aus der Ferne gelöscht.
- Manuell vom Administrator gelöscht.
- Vom Benutzer nicht registriert.

Der mit dem Risikoindikator für nicht verwaltete Geräte verbundene Risikofaktor sind die anderen Risikoindikatoren. Weitere Informationen zu den Risikofaktoren finden Sie unter Citrix Benutzerrisikoindikatoren.

Wann wird der Risikoindikator für das nicht verwaltete Gerät ausgelöst?

Der Risikoindikator für **nicht verwaltete Geräte** wird gemeldet, wenn das Gerät eines Benutzers nicht verwaltet wurde. Ein Gerät ändert sich in einen nicht verwalteten Zustand aufgrund von:

- Eine vom Benutzer ausgeführte Aktion.
- Eine Aktion, die vom Endpoint Management-Administrator oder vom Server ausgeführt wurde.

In Ihrer Organisation können Sie mithilfe des Endpoint Management-Dienstes die Geräte und Apps verwalten, die auf das Netzwerk zugreifen. Weitere Informationen finden Sie unter Verwaltungsmodi.

Wenn das Gerät eines Benutzers in einen nicht verwalteten Status wechselt, erkennt der Endpoint Management-Dienst dieses Ereignis und meldet es an Citrix Analytics. Der Risikowert des Benutzers wird aktualisiert. Der Risikoindikator für **nicht verwaltete Geräte** wurde zur Risikozeitleiste des Benutzers hinzugefügt.

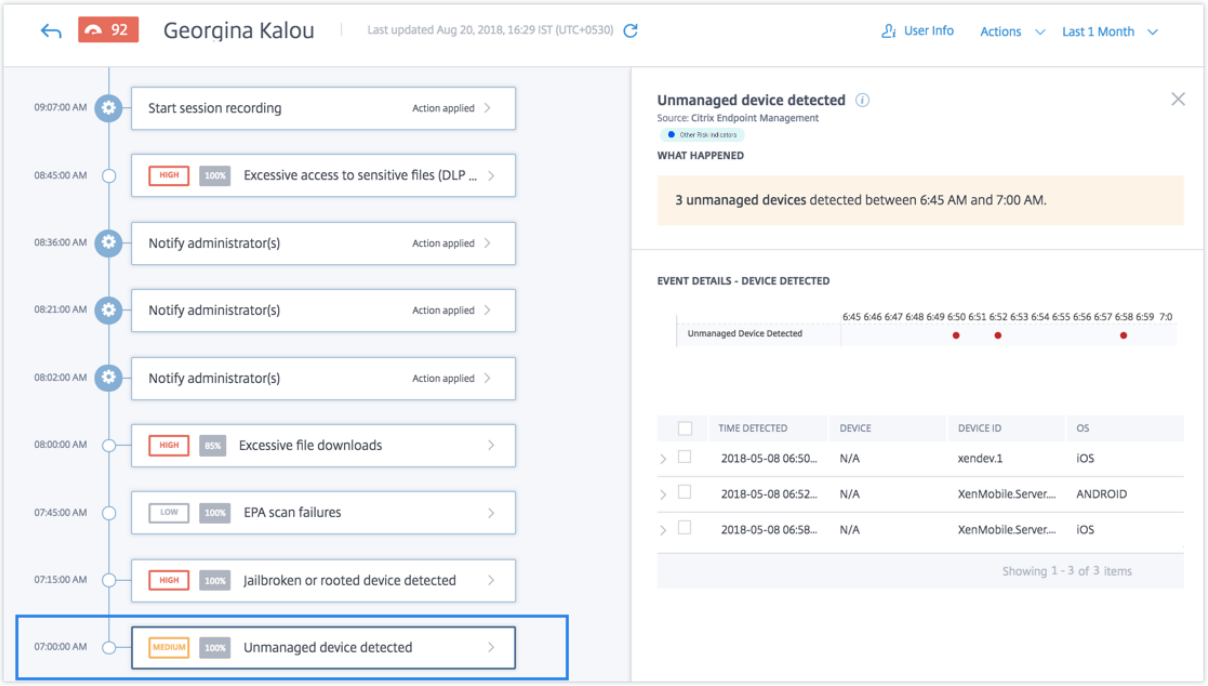
Wie analysiert man nicht verwaltete Geräte erkannte Risikoindikator?

Betrachten Sie die Benutzerin Georgina Kalou, deren Gerät durch eine automatisierte Aktion auf dem Server remote gelöscht wird. Endpoint Management meldet dieses Ereignis an Citrix Analytics, das Georgina Kalou eine aktualisierte Risikobewertung zuweist.

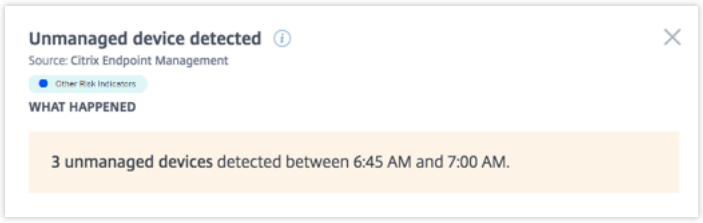
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Aus der Risikozeitleiste von Georgina Kalou können Sie den gemeldeten Risikoindikator für nicht verwaltete Geräte auswählen. Der Grund für das Ereignis wird zusammen mit Details wie der Zeitpunkt der Auslösung des Risikoindikators, Beschreibung des Ereignisses usw. angezeigt.

Um den Risikoindikator für **nicht verwaltetes Gerät** für einen Benutzer anzuzeigen, navigieren Sie zu **Sicherheit > Benutzer**und wählen Sie den Benutzer aus.



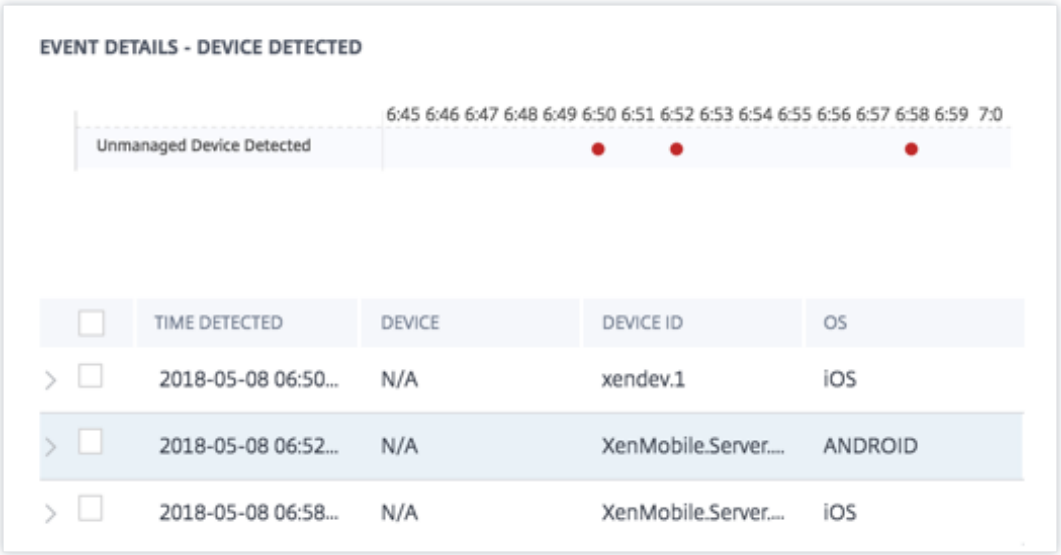
- Im Abschnitt **WAS PASSIERT IST**, können Sie eine Zusammenfassung des Ereignisses anzeigen. Sie können die Anzahl der erkannten nicht verwalteten Geräte und den Zeitpunkt des Auftretens der Ereignisse anzeigen.



- Im Abschnitt **EREIGNISDETAILS —DEVICE DETECTED** werden die Ereignisse in grafischem und tabellarischem Format angezeigt. Die Ereignisse werden auch als einzelne Einträge im Diagramm angezeigt, und die Tabelle enthält folgende Schlüsselinformationen:
  - **Zeit erkannt**. Die Uhrzeit, zu der das Ereignis erkannt wurde.
  - **Gerät**. Das verwendete Mobilgerät.
  - **Geräte-ID**. Die Geräte-ID des Mobilgeräts.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

– **Betriebssystem**. Das Betriebssystem des Mobilgeräts.



Welche Aktionen können Sie auf den Benutzer anwenden?

Sie können die folgenden Aktionen für das Benutzerkonto ausführen:

- **Zur Merkliste hinzufügen**. Wenn Sie einen Benutzer auf zukünftige potenzielle Bedrohungen überwachen möchten, können Sie ihn einer Watchlist hinzufügen.
- **Benachrichtigen Sie Administrator (s)**. Bei ungewöhnlichen oder verdächtigen Aktivitäten im Benutzerkonto wird eine E-Mail-Benachrichtigung an alle oder ausgewählte Administratoren gesendet.

Weitere Informationen zu Aktionen und deren manueller Konfiguration finden Sie unter Richtlinien und Aktionen.

Um die Aktionen manuell auf den Benutzer anzuwenden, navigieren Sie zum Profil des Benutzers und wählen Sie den entsprechenden Risikoindikator aus. Wählen Sie im Menü **Aktionen** eine Aktion aus und klicken Sie auf **Übernehmen**.

> **Hinweis**
>
> Unabhängig von der Datenquelle, die einen Risikoindikator auslöst, können Aktionen in Bezug auf andere Datenquellen angewendet werden.

Citrix Gateway-Risikoindikatoren

July 12, 2022

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Fehler beim Scannen von Endpunktanalyse (EPA)

Citrix Analytics erkennt Benutzerzugriffsbedrohungen basierend auf EPA-Scanfehlern und löst den entsprechenden Risikoindikator aus.

Der Risikofaktor, der mit dem Risikoindikator für den Endpunktanalyse-Scan verbunden ist, sind die anderen Weitere Informationen zu den Risikofaktoren finden Sie unter Citrix Benutzerrisikoindikatoren.

Wann wird der Risikoindikator für EPA-Scanausfälle ausgelöst?

Der Risikoindikator für EPA-Scanausfälle wird gemeldet, wenn ein Benutzer versucht, mit einem Gerät auf das Netzwerk zuzugreifen, das die End Point Analysis (EPA) Scanrichtlinien von Citrix Gateway zur Vorauthentifizierung oder nach der Authentifizierung fehlgeschlagen hat.

Citrix Gateway erkennt diese Ereignisse und meldet sie an Citrix Analytics. Citrix Analytics überwacht all diese Ereignisse, um zu erkennen, ob der Benutzer zu viele EPA-Scanfehler hatte. Wenn Citrix Analytics übermäßige EPA-Scan-Fehler für einen Benutzer feststellt, aktualisiert es den Risikowert des Benutzers und fügt der Risikozeitleiste des Benutzers einen Eintrag für den Risikoindikator des Benutzers hinzu.

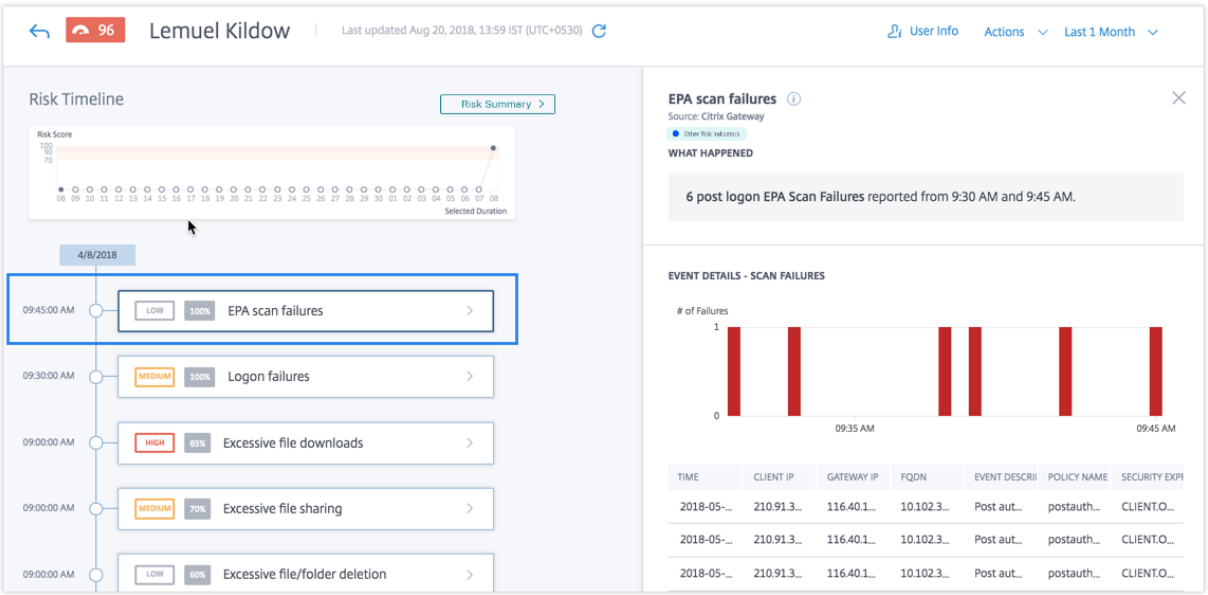
Wie analysiert man den EPA-Scan-Ausfallrisikoindikator?

Betrachten Sie den Benutzer Lemuel, der kürzlich mehrmals versucht hat, mit einem Gerät auf das Netzwerk zuzugreifen, das den EPA-Scan von Citrix Gateway nicht bestanden hat. Citrix Gateway meldet diesen Fehler Citrix Analytics, das Lemuel einen aktualisierten Risiko-Score zuweist. Der Risikoindikator für den EPA-Scanausfall wird dem Risikozeitplan von Lemuel Kildow hinzugefügt.

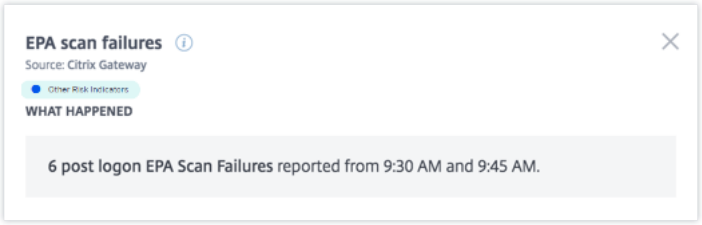
Um den Eintrag für den **EPA-Scanfehler** für einen Benutzer anzuzeigen, navigieren Sie zu **Sicherheit > Benutzer**und wählen Sie den Benutzer aus.

Aus der Risikozeitleiste von Lemuel Kildow können Sie den neuesten Risikoindikator für **EPA-Scanfehler** auswählen, der für den Benutzer gemeldet wurde. Wenn Sie einen Eintrag zum Risikoindikator für den EPA-Scanausfall aus der Zeitleiste auswählen, wird im rechten Fensterbereich ein entsprechendes Detailinformationsfenster angezeigt.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

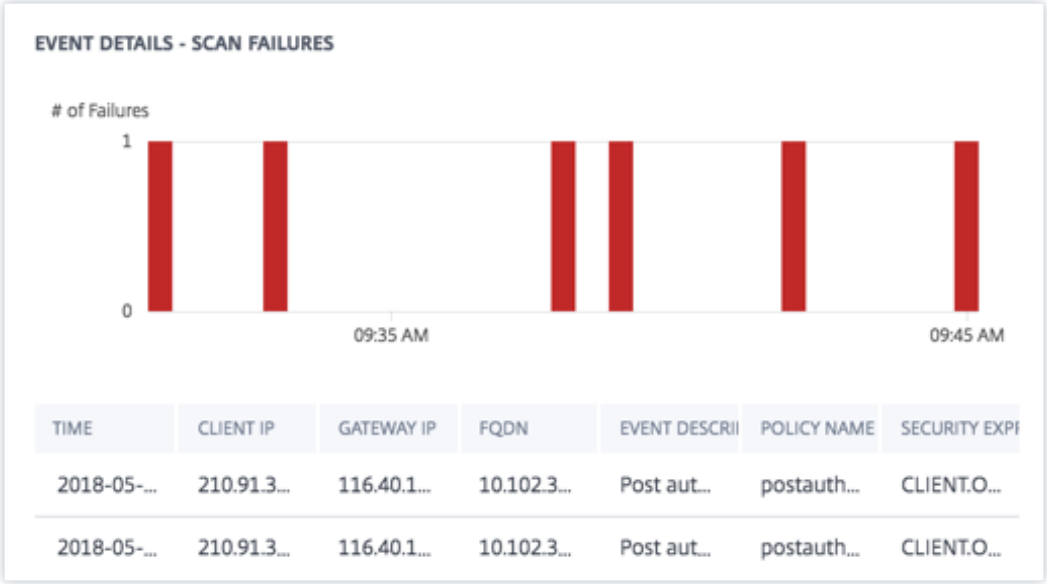


- Der Abschnitt **WHAT HAPPENED**, bietet eine kurze Zusammenfassung des Risikoindikators für EPA-Scans. Und beinhaltet die Anzahl der während des ausgewählten Zeitraums gemeldeten EPA-Scan-Fehler nach der Anmeldung.



- Der Abschnitt **EVENT DETAILS –SCAN FAILURES** enthält eine Timeline-Visualisierung der einzelnen EPA-Scanfehlerereignisse, die während des ausgewählten Zeitraums aufgetreten sind. Außerdem enthält es eine Tabelle, die die folgenden wichtigen Informationen zu jedem Ereignis enthält:
  - **Time**. Der Zeitpunkt, zu dem der EPA-Scanfehler aufgetreten ist.
  - **Client-IP**. Die IP-Adresse des Clients, der den Fehler des EPA-Scans verursacht.
  - **Gateway-IP**. Die IP-Adresse von Citrix Gateway, die den EPA-Scanfehler gemeldet hat.
  - **FQDN**. Der FQDN von Citrix Gateway.
  - **Beschreibung des Ereignisses**. Kurze Beschreibung des Grundes für den Fehler des EPA-Scans.
  - **Name der Richtlinie**. Der auf dem Citrix Gateway konfigurierte EPA-Scanrichtlinienname.
  - **Ausdruck der Sicherheit**. Der auf Citrix Gateway konfigurierte Sicherheitsausdruck.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Welche Aktionen können Sie auf den Benutzer anwenden?

Sie können die folgenden Aktionen für das Benutzerkonto ausführen:

- **Zur Merkliste hinzufügen**. Wenn Sie einen Benutzer auf zukünftige potenzielle Bedrohungen überwachen möchten, können Sie ihn einer Watchlist hinzufügen.
- **Benachrichtigen Sie Administrator(en)**. Bei ungewöhnlichen oder verdächtigen Aktivitäten im Benutzerkonto wird eine E-Mail-Benachrichtigung an alle oder ausgewählte Administratoren gesendet.
- **Benutzer abmelden**. Wenn ein Benutzer von seinem Konto abgemeldet ist, kann er nicht über Citrix Gateway auf eine Ressource zugreifen, bis der Citrix Gateway-Administrator die Aktion Benutzer abmelden löscht.
- **Benutzer sperren**: Wenn das Konto eines Benutzers aufgrund anomalem Verhalten gesperrt ist, kann er nicht über Citrix Gateway auf eine Ressource zugreifen, bis der Gateway-Administrator das Konto entsperrt hat.

Weitere Informationen zu Aktionen und deren manueller Konfiguration finden Sie unter Richtlinien und Aktionen.

Um die Aktionen manuell auf den Benutzer anzuwenden, navigieren Sie zum Profil des Benutzers und wählen Sie den entsprechenden Risikoindikator aus. Wählen Sie im Menü **Aktionen** eine Aktion aus und klicken Sie auf **Übernehmen**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Hinweis**
>
> Unabhängig von der Datenquelle, die einen Risikoindikator auslöst, können Aktionen in Bezug auf andere Datenquellen angewendet werden.

Übermäßige Authentifizierungsfehler

Citrix Analytics erkennt Benutzerzugriffsbedrohungen basierend auf übermäßigen Authentifizierungsfehlern und löst den entsprechenden Risikoindikator aus.

Der mit dem Risikoindikator für übermäßige Authentifizierungsfehler verbundene Risikofaktor sind die auf Anmeldefehlern basierenden Risikoindikatoren. Weitere Informationen zu den Risikofaktoren finden Sie unter Citrix Benutzerrisikoindikatoren.

Wann wird der Risikoindikator für übermäßige Authentifizierungsfehler ausgelöst?

Der Indikator für das Risiko eines Anmeldefehlers wird gemeldet, wenn der Benutzer innerhalb eines bestimmten Zeitraums auf mehrere Citrix Gateway-Authentifizierungsfehler stößt. Die Citrix Gateway-Authentifizierungsfehler können primäre, sekundäre oder tertiäre Authentifizierungsfehler sein, je nachdem, ob die Multifaktor-Authentifizierung für den Benutzer konfiguriert ist.

Citrix Gateway erkennt alle Fehler bei der Benutzerauthentifizierung und meldet diese Ereignisse an Citrix Analytics. Citrix Analytics überwacht alle diese Ereignisse, um festzustellen, ob der Benutzer zu viele Authentifizierungsfehler hatte. Wenn Citrix Analytics übermäßige Authentifizierungsfehler feststellt, aktualisiert es den Risikowert des Benutzers. Der Risikoindikator für übermäßige Authentifizierungsfehler wird zur Risikozeitleiste des Benutzers hinzugefügt.

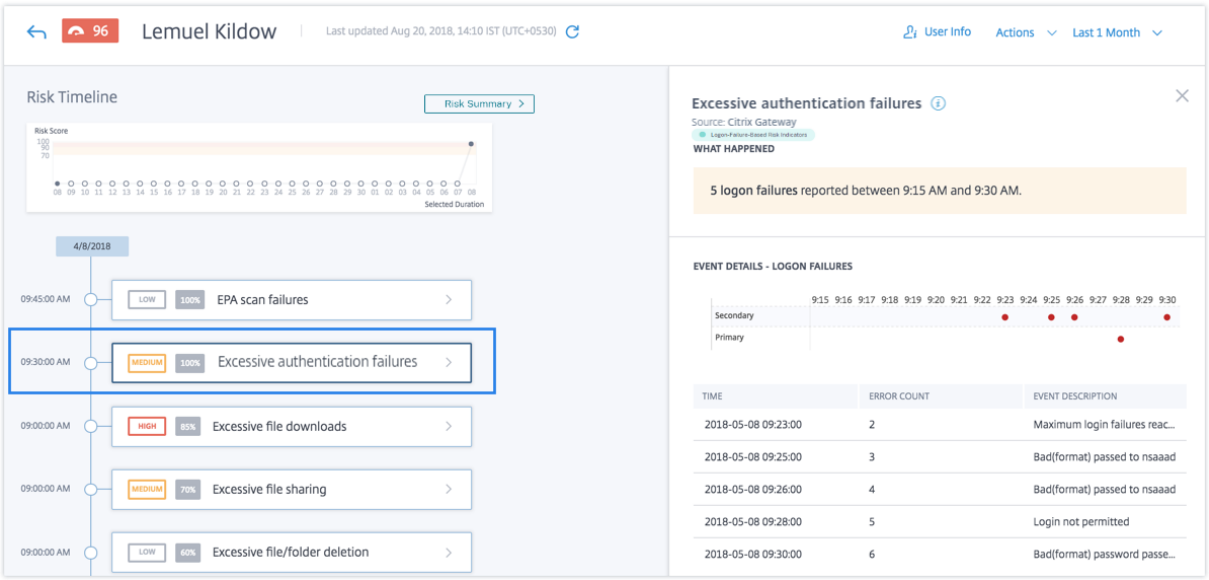
Wie analysiert man den Risikoindikator für übermäßige Authentifizierungsfehler?

Betrachten Sie den Benutzer Lemuel, der kürzlich mehrere Versuche zur Authentifizierung des Netzwerks nicht bestanden hat. Citrix Gateway meldet diese Fehler an Citrix Analytics, und Lemuel wird eine aktualisierte Risikobewertung zugewiesen. Der Risikoindikator für **übermäßige Authentifizierungsfehler** wird der Risikozeitleiste von Lemuel Kildow hinzugefügt.

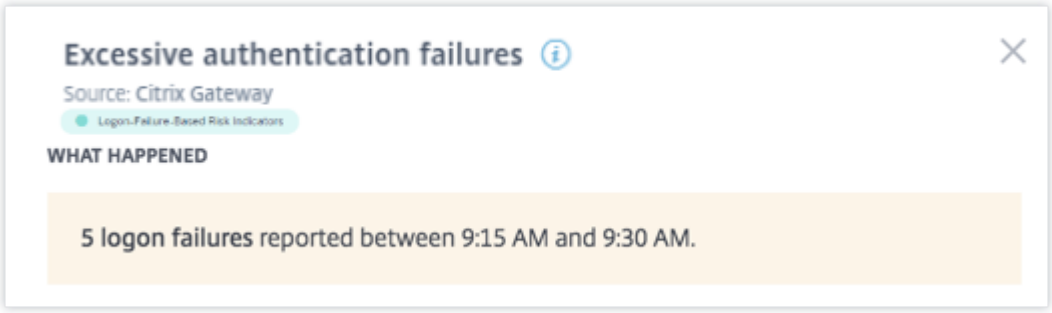
Um den Eintrag Risikoindikator für **übermäßige Authentifizierungsfehler** für einen Benutzer anzuzeigen, navigieren Sie zu **Sicherheit > Benutzer**, und wählen Sie den Benutzer aus.

Aus der Risikozeitleiste von Lemuel Kildow können Sie den neuesten Risikoindikator für **übermäßige Authentifizierungsfehler** auswählen, der für den Benutzer gemeldet wurde. Wenn Sie den Risikoindikator für **übermäßige Authentifizierungsfehler** aus der Risikozeitleiste auswählen, wird im rechten Fensterbereich ein entsprechendes Detailinformationsfenster angezeigt.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

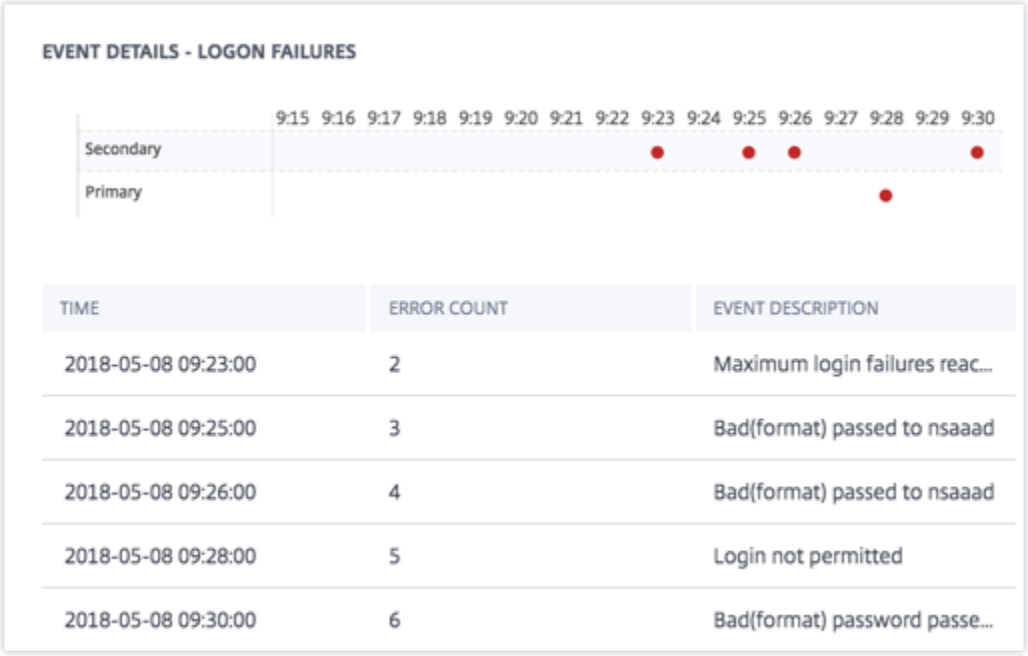


- Der Abschnitt **WHAT HAPPENED**, enthält eine kurze Zusammenfassung des Risikoindikators, einschließlich der Anzahl der Authentifizierungsfehler, die während des ausgewählten Zeitraums aufgetreten sind.



- Der Abschnitt **EVENT DETAILS** enthält eine Zeitleistenvisualisierung der einzelnen Ereignisse bei übermäßigen Authentifizierungsfehlern, die während des ausgewählten Zeitraums aufgetreten sind. Außerdem können Sie die folgenden wichtigen Informationen zu jedem Ereignisses anzeigen:
  - **Time**. Der Zeitpunkt, zu dem der Anmeldefehler aufgetreten ist.
  - **Anzahl der Fehler**. Die Anzahl der Authentifizierungsfehler, die für den Benutzer zum Zeitpunkt des Ereignisses und für die letzten 48 Stunden festgestellt wurden.
  - **Beschreibung des Ereignisses**. Kurze Beschreibung des Grundes für den Fehler bei der Anmeldung.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Welche Aktionen können Sie auf den Benutzer anwenden?

Sie können die folgenden Aktionen für das Benutzerkonto ausführen:

- **Zur Merkliste hinzufügen**. Wenn Sie einen Benutzer auf zukünftige potenzielle Bedrohungen überwachen möchten, können Sie ihn einer Watchlist hinzufügen.
- **Benachrichtigen Sie Administrator(en)**. Bei ungewöhnlichen oder verdächtigen Aktivitäten im Benutzerkonto wird eine E-Mail-Benachrichtigung an alle oder ausgewählte Administratoren gesendet.
- **Benutzer abmelden**. Wenn ein Benutzer von seinem Konto abgemeldet ist, kann er nicht über Citrix Gateway auf eine Ressource zugreifen, bis der Citrix Gateway-Administrator die Aktion Benutzer abmelden löscht.
- **Benutzer sperren**: Wenn das Konto eines Benutzers aufgrund anomalem Verhalten gesperrt ist, kann er nicht über Citrix Gateway auf eine Ressource zugreifen, bis der Gateway-Administrator das Konto entsperrt hat.

Weitere Informationen zu Aktionen und deren manueller Konfiguration finden Sie unter Richtlinien und Aktionen.

Um die Aktionen manuell auf den Benutzer anzuwenden, navigieren Sie zum Profil des Benutzers und wählen Sie den entsprechenden Risikoindikator aus. Wählen Sie im Menü **Aktionen** eine Aktion aus und klicken Sie auf **Übernehmen**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Hinweis**
>
> Unabhängig von der Datenquelle, die einen Risikoindikator auslöst, können Aktionen in Bezug auf andere Datenquellen angewendet werden.

Unmögliche Reisen

Citrix Analytics erkennt die Anmeldungen eines Benutzers als riskant, wenn die aufeinanderfolgenden Anmeldungen aus zwei verschiedenen Ländern innerhalb eines Zeitraums erfolgen, der unter der erwarteten Reisezeit zwischen den Ländern liegt.

Das Szenario der unmöglichen Reisezeit weist auf folgende Risiken hin:

- **Kompromittierte Anmeldeinformationen**: Ein Remote-Angreifer stiehlt die Anmeldeinformationen eines legitimen Benutzers.
- **Gemeinsame Anmeldeinformationen**: Verschiedene Benutzer verwenden dieselben Benutzeranmeldeinformationen.

Wann wird der Indikator Unmögliches Reiserisiko ausgelöst?

Der Indikator für **unmögliches Reiserisiko** wertet die Zeit und die geschätzte Entfernung zwischen jedem Paar aufeinanderfolgender Benutzeranmeldungen aus und löst aus, wenn die Entfernung größer ist, als eine einzelne Person in dieser Zeit möglicherweise zurücklegen kann.

> **Hinweis:**
>
> Dieser Risikoindikator enthält auch eine Logik zur Reduzierung von Fehlalarmen für die folgenden Szenarien, die nicht die tatsächlichen Standorte der Benutzer widerspiegeln:
>
> - Wenn sich Benutzer über Citrix Gateway über Proxyverbindungen anmelden.
> - Wenn sich Benutzer über Citrix Gateway von gehosteten Clients aus anmelden.

So analysieren Sie den Indikator für unmögliches Risiko

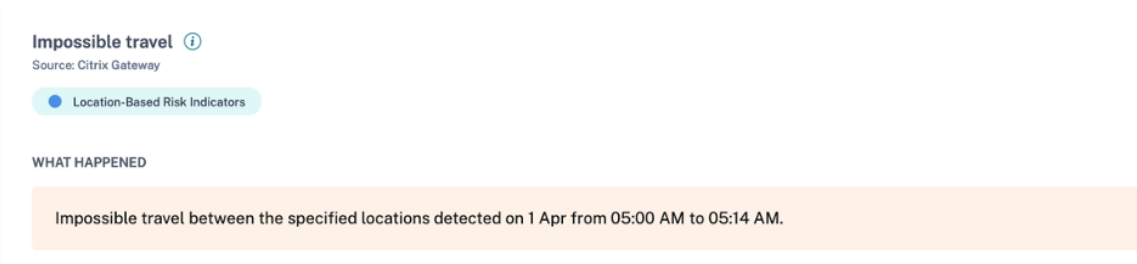
Stellen Sie sich den Benutzer Adam Maxwell vor, der sich innerhalb einer Minute von zwei Standorten aus anmeldet - Bengaluru, Indien und Oslo, Norwegen. Citrix Analytics erkennt dieses Anmeldeereignis als unmögliches Reiseszenario und löst den Indikator **Unmögliche Reise** aus. Der Risikoindikator wird dem Risikozeitplan von Adam Maxwell hinzugefügt und ihm wird ein Risiko-Score zugewiesen.

Um die Risikozeitleiste von Adam Maxwell anzuzeigen, wählen Sie **Sicherheit > Benutzer**aus. Wählen Sie im Bereich **Riskante Benutzer** den Benutzer Adam Maxwell aus.

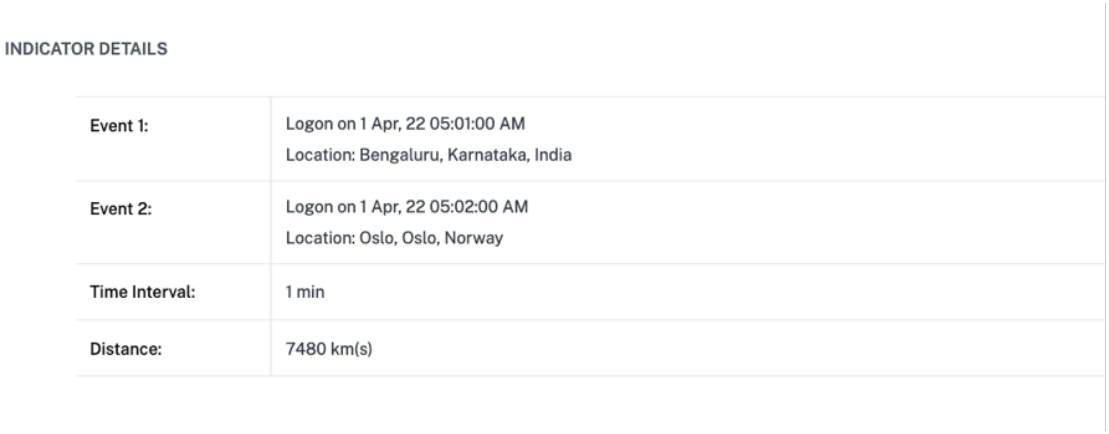
Wählen Sie in Adam Maxwells Risiko-Timeline den Indikator **Unmögliches Reiserisiko** aus. Sie können die folgenden Informationen anzeigen:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Der Abschnitt **WHAT** HAPPENED bietet eine kurze Zusammenfassung des unmöglichen Reiseereignisses.



- Der Abschnitt **INDICATOR DETAILS** enthält die Standorte, von denen aus sich der Benutzer angemeldet hat, die Zeitdauer zwischen den aufeinanderfolgenden Anmeldungen und die Entfernung zwischen den beiden Standorten.

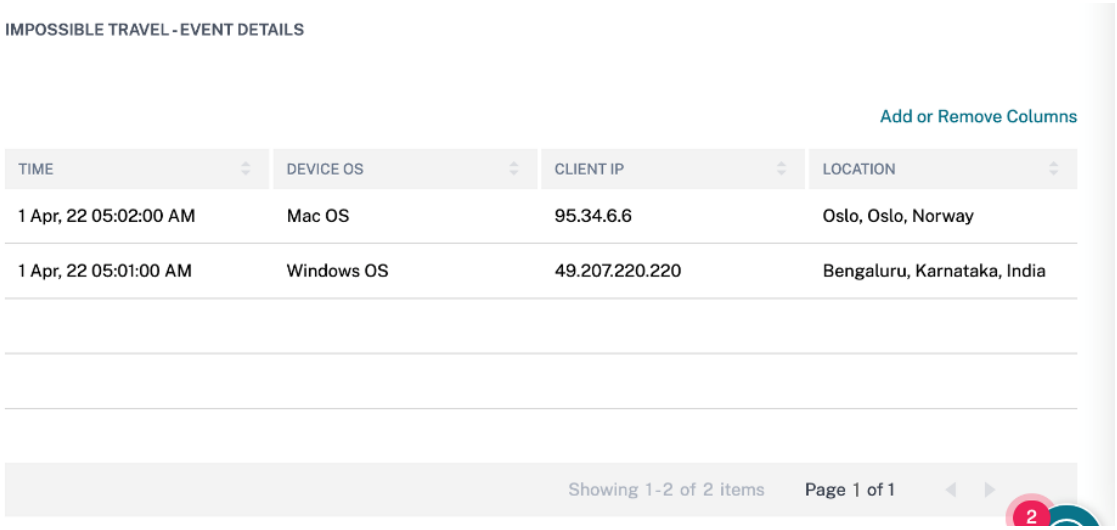


- Im Abschnitt **LOGON LOCATION- LAST 30 DAYS** wird eine geografische Kartenansicht der unmöglichen Reiseorte und der bekannten Standorte des Benutzers angezeigt. Die Standortdaten werden für die letzten 30 Tage angezeigt. Sie können mit der Maus über die Zeiger auf der Karte fahren, um die Gesamtzahl der Anmeldungen von jedem Standort aus anzuzeigen.

- Der Abschnitt **IMPOSSIBLE TRAVEL —EVENT DETAILS** enthält die folgenden Informationen über das unmögliche Reiseereignis:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Zeit**: Gibt das Datum und die Uhrzeit der Anmeldungen an.
- **Gerätebetriebssystem**: Zeigt das Betriebssystem des Benutzergeräts an.
- **Client-IP**: Zeigt die IP-Adresse des Benutzergeräts an.
- **Standort**: Gibt den Ort an, von dem aus sich der Benutzer angemeldet hat.



Welche Aktionen können Sie auf den Benutzer anwenden?

Sie können die folgenden Aktionen für das Konto des Benutzers ausführen:

- **Zur Merkliste hinzufügen**. Wenn Sie einen Benutzer auf zukünftige potenzielle Bedrohungen überwachen möchten, können Sie ihn einer Watchlist hinzufügen.
- **Benachrichtigen Sie Administrator(en)**. Bei ungewöhnlichen oder verdächtigen Aktivitäten im Konto des Benutzers wird eine E-Mail-Benachrichtigung an alle oder ausgewählte Administratoren gesendet.
- **Benutzer abmelden**. Wenn ein Benutzer von seinem Konto abgemeldet ist, kann er nicht über Citrix Gateway auf eine Ressource zugreifen, bis der Citrix Gateway-Administrator die Aktion Benutzer abmelden löscht.
- **Benutzer sperren**: Wenn das Konto eines Benutzers aufgrund eines anomalen Verhaltens gesperrt ist, kann er nicht über Citrix Gateway auf eine Ressource zugreifen, bis der Gateway-Administrator das Konto entsperrt.

Weitere Informationen zu Aktionen und deren manueller Konfiguration finden Sie unter Richtlinien und Aktionen.

Um die Aktionen manuell auf den Benutzer anzuwenden, navigieren Sie zum Benutzerprofil und wählen Sie den entsprechenden Risikoindikator aus. Wählen Sie im Menü **Aktionen** eine Aktion aus und klicken Sie auf **Übernehmen**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Hinweis**
>
> Unabhängig von der Datenquelle, die einen Risikoindikator auslöst, können Aktionen in Bezug auf andere Datenquellen angewendet werden.

Anmeldung von verdächtiger IP

Citrix Analytics erkennt Bedrohungen für den Benutzerzugriff basierend auf der Anmeldeaktivität einer verdächtigen IP und löst diesen Risikoindikator aus.

Der mit dem Indikator Anmeldung von verdächtigen IP-Risiken verbundene Risikofaktor sind die IP-basierten Risikoindikatoren. Weitere Informationen zu den Risikofaktoren finden Sie unter Citrix Benutzerrisikoindikatoren.

Wann wird der Indikator "Anmeldung von verdächtigen IP-Risiken"ausgelöst?

Der Risikoindikator "**Anmeldung von verdächtigen IP** "wird ausgelöst, wenn ein Benutzer versucht, von einer IP-Adresse aus, die Citrix Analytics als verdächtig identifiziert, auf das Netzwerk zuzugreifen. Die IP-Adresse wird aufgrund einer der folgenden Bedingungen als verdächtig angesehen:

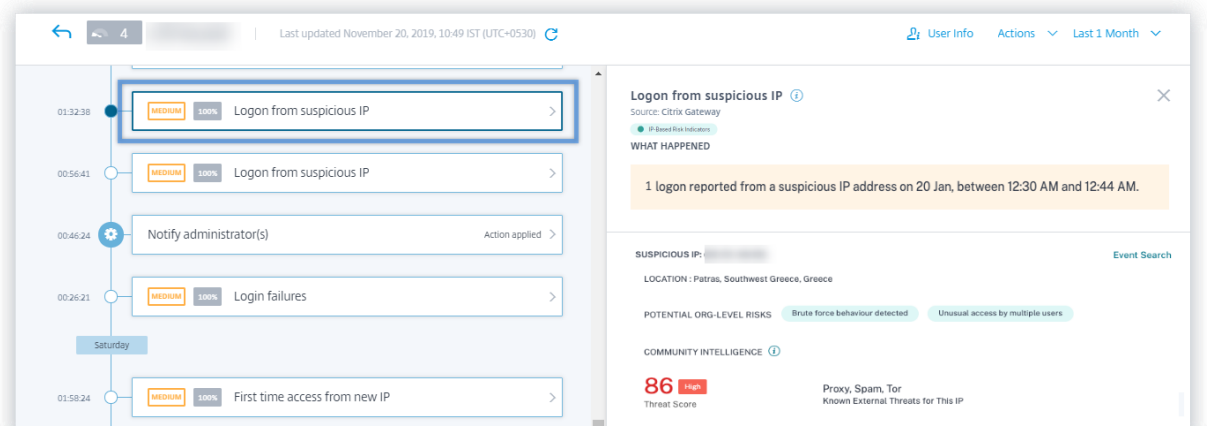
- Ist im externen IP-Bedrohungsintelligence-Feed aufgeführt
- Verfügt über mehrere Benutzeranmeldedatensätze von einem ungewöhnlichen Ort
- Übermäßige fehlgeschlagene Anmeldeversuche, die auf einen Brute-Force-Angriff hinweisen könnten

Citrix Analytics überwacht die Anmeldeereignisse, die von Citrix Gateway empfangen wurden, und erkennt, ob sich ein Benutzer von einer verdächtigen IP angemeldet hat. Wenn Citrix Analytics einen Anmeldeversuch von einer verdächtigen IP erkennt, aktualisiert es den Risikowert des Benutzers und fügt der Risikozeitleiste des Benutzers einen Eintrag für die **Anmeldung von verdächtigen IP-Risikoindikatoren** hinzu.

Wie analysiere ich die Anmeldung von verdächtigen IP-Risikoindikator?

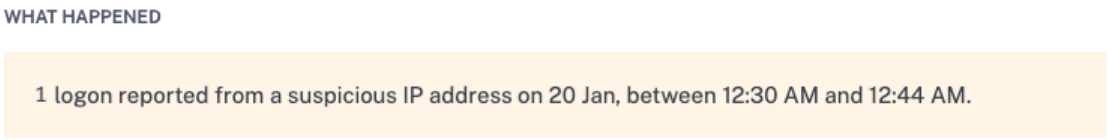
Betrachten Sie den Benutzer Lemuel, der versucht hat, von einer IP-Adresse, die Citrix Analytics als verdächtig identifiziert, auf das Netzwerk zuzugreifen. Citrix Gateway meldet das Anmeldeereignis an Citrix Analytics, das Lemuel einen aktualisierten Risikowert zuweist. Der Risikoindikator "**Anmeldung von verdächtigen IP** "wird zur Risikozeitleiste von Lemuel Kildow hinzugefügt.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

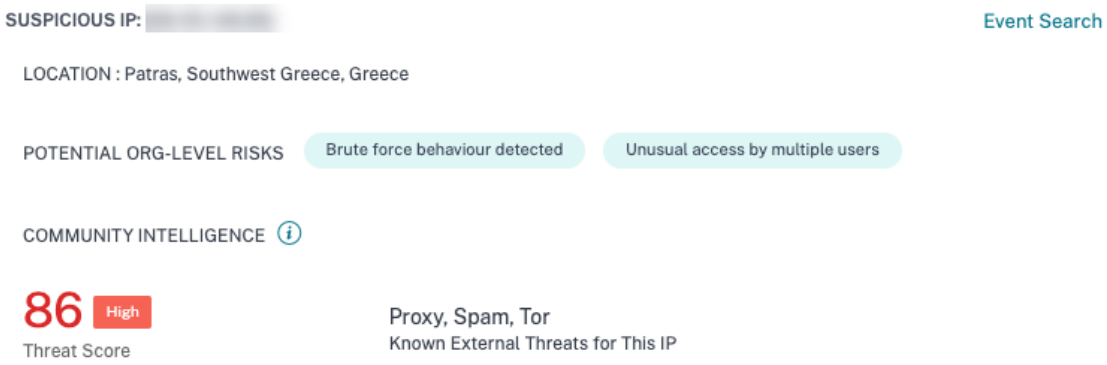


Um den für einen Benutzer gemeldeten Indikator "Anmeldung von verdächtigen IP-Risiken" anzuzeigen, navigieren Sie zu **Sicherheit** > **Benutzer**, und wählen Sie den Benutzer aus. Aus der Risikozeitleiste von Lemuel Kildow können Sie die neueste **Anmeldung aus dem für den Benutzer gemeldeten verdächtigen IP-Risikoindikator** auswählen. Wenn Sie den Eintrag "**Anmeldung von verdächtigem IP-Risiko** "aus der Zeitleiste auswählen, wird im rechten Bereich ein entsprechender Detailinformationsbereich angezeigt.

- Der Abschnitt **WHAT HAPPENED**, bietet eine kurze Zusammenfassung des Risikoindikators "Anmeldung von verdächtigen IP-Adressen". Und beinhaltet die Anzahl der Anmeldungen von einer verdächtigen IP-Adresse, die während des ausgewählten Zeitraums gemeldet wurden.



- Der Abschnitt **Verdächtige IP** enthält die folgenden Informationen:

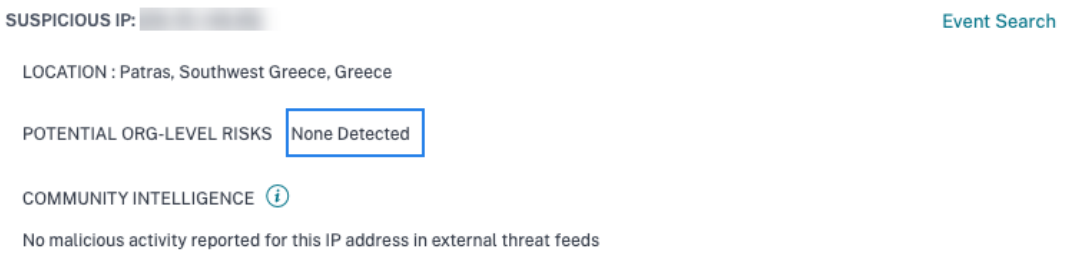


  - **Verdächtige IP**. Die IP-Adresse, die mit einer verdächtigen Anmeldeaktivität verknüpft ist.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

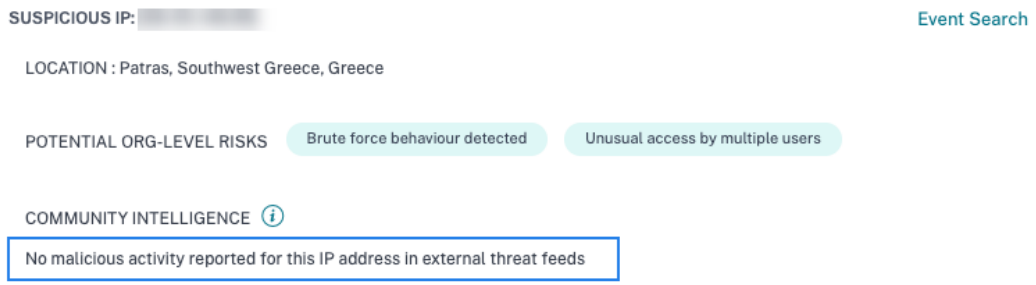
- **Standort**. Die Stadt, die Region und das Land des Nutzers. Diese Standorte werden basierend auf der Verfügbarkeit von Daten angezeigt.
- **Potenzielles Risiko auf Organisationsebene** Zeigt alle Muster verdächtiger IP-Aktivitäten an, die Citrix Analytics kürzlich in Ihrer Organisation entdeckt hat. Zu den riskanten Mustern gehören übermäßige Anmeldefehler, die mit potenziellen Brute-Force-Versuchen und ungewöhnlichem Zugriff mehrerer Benutzer übereinstimmen.

  Wenn für eine IP-Adresse in Ihrer Organisation kein riskantes Muster festgestellt wird, wird die folgende Meldung angezeigt.



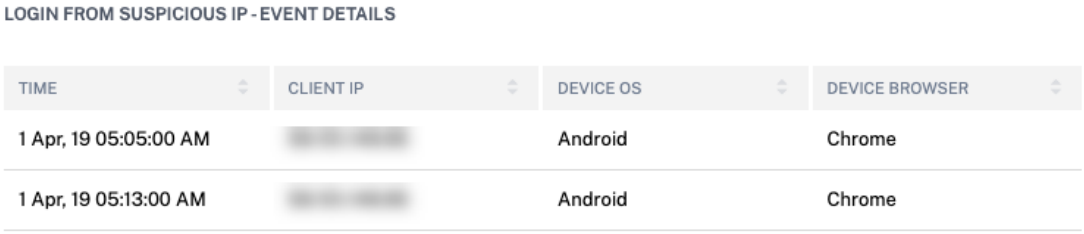
- **Community-Intelligenz**. Stellt den Bedrohungswert und die Bedrohungskategorien einer IP-Adresse bereit, die im externen IP Threat Intelligence-Feed als hohes Risiko identifiziert werden. Citrix Analytics weist der IP-Adresse mit hohem Risiko eine Risikobewertung zu. Der Risikowert beginnt bei 80.

  Wenn für eine IP-Adresse keine Bedrohungsinformationen im externen IP Threat Intelligence Feed verfügbar sind, wird die folgende Meldung angezeigt.



- Der Abschnitt **EVENT-DETAILS** enthält die folgenden Informationen über die verdächtige Anmeldeaktivität:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.


LOGIN FROM SUSPICIOUS IP - EVENT DETAILS

TIME	CLIENT IP	DEVICE OS	DEVICE BROWSER
1 Apr, 19 05:05:00 AM	[redacted]	Android	Chrome
1 Apr, 19 05:13:00 AM	[redacted]	Android	Chrome

- **Time**. Der Zeitpunkt der verdächtigen Anmeldeaktivität.
- **Client-IP**. Die IP-Adresse des Geräts des Benutzers, das für die verdächtige Anmeldeaktivität verwendet wurde.
- **Geräte-OS**. Das Betriebssystem des Browsers.
- **Geräte-Browser**. Der Webbrowser, der für die verdächtige Anmeldeaktivität verwendet wird.

Welche Aktionen können Sie auf den Benutzer anwenden?

Sie können die folgenden Aktionen für das Benutzerkonto ausführen:

- **Zur Merkliste hinzufügen**. Wenn Sie einen Benutzer auf zukünftige potenzielle Bedrohungen überwachen möchten, können Sie ihn einer Watchlist hinzufügen.
- **Benachrichtigen Sie Administrator(en)**. Bei ungewöhnlichen oder verdächtigen Aktivitäten im Benutzerkonto wird eine E-Mail-Benachrichtigung an alle oder ausgewählte Administratoren gesendet.
- **Benutzer abmelden**. Wenn ein Benutzer von seinem Konto abgemeldet ist, kann er nicht über Citrix Gateway auf eine Ressource zugreifen, bis der Citrix Gateway-Administrator die Aktion Benutzer abmelden löscht.
- **Benutzer sperren**: Wenn das Konto eines Benutzers aufgrund anomalem Verhalten gesperrt ist, kann er nicht über Citrix Gateway auf eine Ressource zugreifen, bis der Gateway-Administrator das Konto entsperrt hat.

Weitere Informationen zu Aktionen und deren manueller Konfiguration finden Sie unter Richtlinien und Aktionen.

Um die Aktionen manuell auf den Benutzer anzuwenden, navigieren Sie zum Profil des Benutzers und wählen Sie den entsprechenden Risikoindikator aus. Wählen Sie im Menü **Aktionen** eine Aktion aus und klicken Sie auf **Übernehmen**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Hinweis**
>
> Unabhängig von der Datenquelle, die einen Risikoindikator auslöst, können Aktionen in Bezug auf andere Datenquellen angewendet werden.

Verdächtige Anmeldung

> **Hinweise**
>
> - Dieser Risikoindikator ersetzt den Risikoindikator für den Zugriff von einem ungewöhnlichen Standort aus.
> - Alle Richtlinien, die auf dem Risikoindikator Zugriff von einem ungewöhnlichen Ort aus basieren, werden automatisch mit dem Risikoindikator für verdächtige Anmeldung verknüpft.

Citrix Analytics erkennt die Anmeldungen des Benutzers, die ungewöhnlich oder riskant erscheinen, basierend auf mehreren Kontextfaktoren, die gemeinsam durch das Gerät, den Standort und das Netzwerk definiert werden, die vom Benutzer verwendet werden.

Wann wird der Risikoindikator für verdächtige Anmeldung ausgelöst?

Der Risikoindikator wird durch die Kombination der folgenden Faktoren ausgelöst, wobei jeder Faktor aufgrund einer oder mehrerer Bedingungen als potenziell verdächtig angesehen wird.

Faktor	Bedingungen
Ungewöhnliches Gerät	Der Benutzer meldet sich von einem Gerät mit einer Signatur an, die sich von den in den letzten 30 Tagen verwendeten Geräten unterscheidet. Die Gerätesignatur basiert auf dem Betriebssystem des Geräts und dem verwendeten Browser.
Ungewöhnlicher Ort	Melden Sie sich von einer Stadt oder einem Land aus an, in dem sich der Benutzer in den letzten 30 Tagen nicht angemeldet hat. Die Stadt oder das Land ist geografisch weit von den letzten (letzten 30 Tagen) Anmeldeorten entfernt.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Faktor	Bedingungen
	Null oder mindestens Benutzer haben sich in den letzten 30 Tagen von der Stadt oder dem Land aus angemeldet.
Ungewöhnliches Netzwerk	Melden Sie sich von einer IP-Adresse aus an, die der Benutzer in den letzten 30 Tagen nicht verwendet hat. Melden Sie sich von einem IP-Subnetz aus an, das der Benutzer in den letzten 30 Tagen nicht verwendet hat. Null oder mindestens Benutzer haben sich in den letzten 30 Tagen vom IP-Subnetz aus angemeldet.
IP-Bedrohung	Die IP-Adresse wird vom Community Threat Intelligence Feed Webroot als hohes Risiko identifiziert. Citrix Analytics hat kürzlich sehr verdächtige Anmeldeaktivitäten anhand der IP-Adresse anderer Benutzer erkannt.

So analysieren Sie den Risikoindikator für verdächtige Anmeldung

Man denke an den Benutzer Adam Maxwell, der sich zum ersten Mal aus Andhra Pradesh, Indien, anmeldet. Er verwendet ein Gerät mit bekannter Signatur, um auf die Ressourcen der Organisation zuzugreifen. Er stellt jedoch eine Verbindung über ein Netzwerk her, das er in den letzten 30 Tagen nicht genutzt hat.

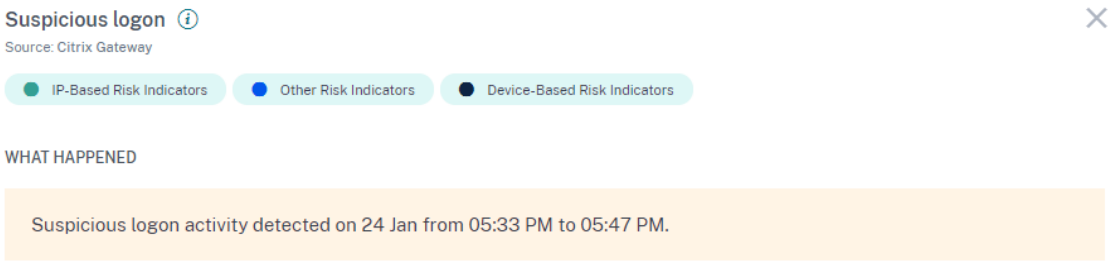
Citrix Analytics erkennt dieses Anmeldeereignis als verdächtig, da die Faktoren Standort und Netzwerk von seinem üblichen Verhalten abweichen und den Risikoindikator für verdächtige Anmeldung auslösen. Der Risikoindikator wird zu Adam Maxwells Risikozeitplan hinzugefügt und ihm wird ein Risiko-Score zugewiesen.

Um Adam Maxwells Risikozeit anzuzeigen, wählen Sie **Sicherheit > Benutzer**. Wählen Sie im Bereich **Riskante Benutzer** den Benutzer Adam Maxwell aus.

Wählen Sie in der Risikozeitleiste von Adam Maxwell den Risikoindikator für **verdächtige Anmeldung** aus. Sie sehen die folgenden Informationen an:

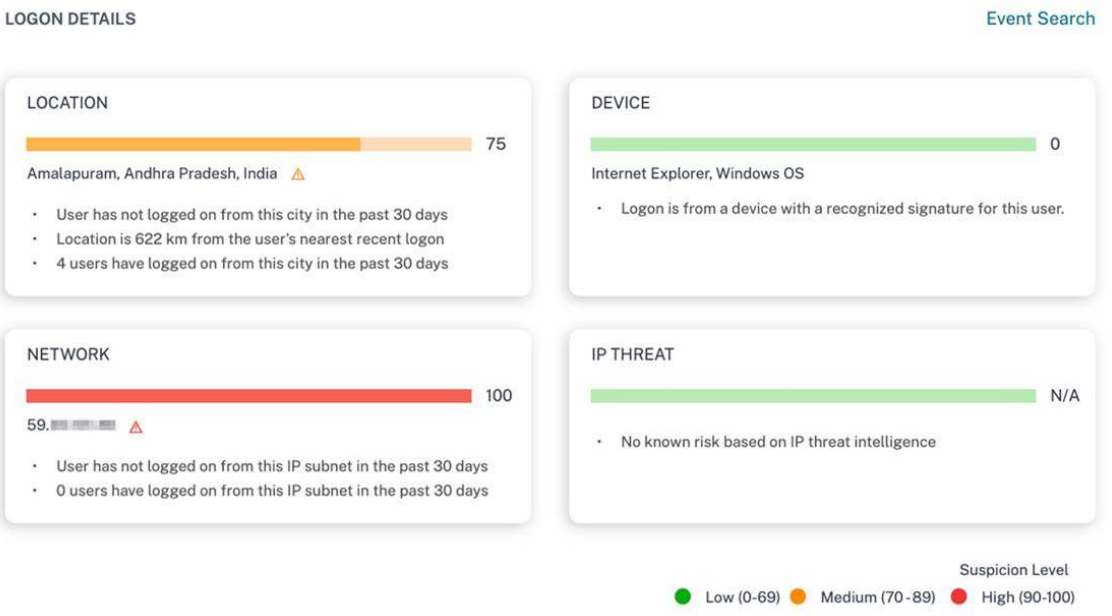
- Der Abschnitt **WHAT** HAPPENED bietet eine kurze Zusammenfassung der verdächtigen Aktivitäten, einschließlich der Risikofaktoren und des Zeitpunkts des Ereignisses.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



- Der Abschnitt **LOGON DETAILS** enthält eine detaillierte Zusammenfassung der verdächtigen Aktivitäten, die den einzelnen Risikofaktoren entsprechen. Jedem Risikofaktor wird ein Score zugewiesen, der das Verdachtsniveau angibt. Jeder einzelne Risikofaktor weist nicht auf ein hohes Risiko eines Benutzers hin. Das Gesamtrisiko basiert auf der Korrelation der verschiedenen Risikofaktoren.

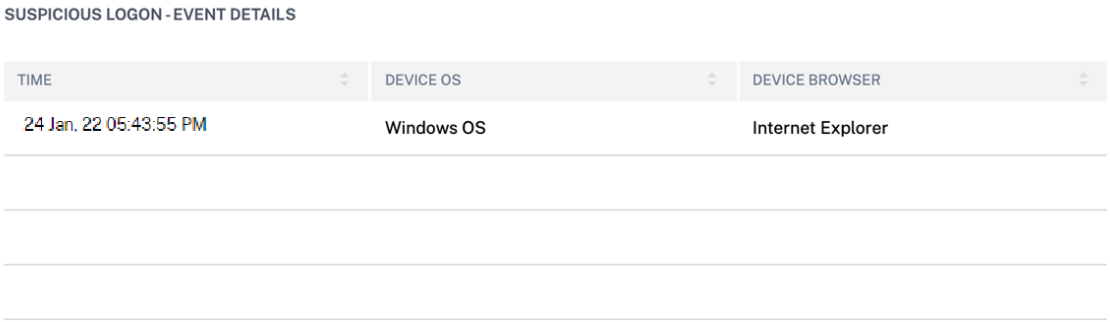
Stufe des Verdachts	Indikation
0–69	Der Faktor scheint normal zu sein und wird nicht als verdächtig angesehen.
70–89	Der Faktor erscheint etwas ungewöhnlich und wird bei anderen Faktoren als mäßig verdächtig angesehen.
90–100	Der Faktor ist völlig neu oder ungewöhnlich und wird bei anderen Faktoren als äußerst verdächtig angesehen.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Der **LOGON LOCATION- LAST 30 DAYS** zeigt eine geografische Kartenansicht der letzten bekannten Standorte und des aktuellen Standorts des Benutzers an. Die Standortdaten werden für die letzten 30 Tage angezeigt. Sie können mit der Maus über die Zeiger auf der Karte fahren, um die Gesamtzahl der Anmeldungen von jedem Standort aus anzuzeigen.

- Der Abschnitt **SUSPICIOUS LOGON- EVENT DETAILS** enthält die folgenden Informationen über das verdächtige Anmeldeereignis:
  - **Uhrzeit**: Zeigt Datum und Uhrzeit der verdächtigen Anmeldung an.
  - **Gerätebetriebssystem**: Zeigt das Betriebssystem des Benutzergeräts an.
  - **Gerätebrowser**: Zeigt den Webbrowser an, mit dem Sie sich bei Citrix Gateway anmelden.



Welche Aktionen können Sie auf den Benutzer anwenden?

Sie können die folgenden Aktionen für das Benutzerkonto ausführen:

- **Zur Merkliste hinzufügen**. Wenn Sie einen Benutzer auf zukünftige potenzielle Bedrohungen überwachen möchten, können Sie ihn einer Watchlist hinzufügen.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Benachrichtigen Sie Administrator(en)**. Bei ungewöhnlichen oder verdächtigen Aktivitäten im Benutzerkonto wird eine E-Mail-Benachrichtigung an alle oder ausgewählte Administratoren gesendet.
- **Benutzer abmelden**. Wenn ein Benutzer von seinem Konto abgemeldet ist, kann er nicht über Citrix Gateway auf eine Ressource zugreifen, bis der Citrix Gateway-Administrator die Aktion Benutzer abmelden löscht.
- **Benutzer sperren**: Wenn das Konto eines Benutzers aufgrund anomalem Verhalten gesperrt ist, kann er nicht über Citrix Gateway auf eine Ressource zugreifen, bis der Gateway-Administrator das Konto entsperrt hat.

Weitere Informationen zu Aktionen und deren manueller Konfiguration finden Sie unter Richtlinien und Aktionen.

Um die Aktionen manuell auf den Benutzer anzuwenden, navigieren Sie zum Profil des Benutzers und wählen Sie den entsprechenden Risikoindikator aus. Wählen Sie im Menü **Aktionen** eine Aktion aus und klicken Sie auf **Übernehmen**.

> **Hinweis**
>
> Unabhängig von der Datenquelle, die einen Risikoindikator auslöst, können Aktionen in Bezug auf andere Datenquellen angewendet werden.

Ungewöhnliches Authentifizierungs

Citrix Analytics erkennt zugriffsbasierte Bedrohungen, wenn ein Benutzer Anmeldefehler aufgrund einer ungewöhnlichen IP-Adresse hat, und löst den entsprechenden Risikoindikator aus.

Der mit dem Indikator für ungewöhnliche Authentifizierungsrisiken verbundene Risikofaktor sind die auf Anmeldefehlern basierenden Risikoindikatoren. Weitere Informationen zu den Risikofaktoren finden Sie unter Citrix Benutzerrisikoindikatoren.

Wann wird die Anzeige für ungewöhnliche Authentifizierungsfehler ausgelöst?

Sie können benachrichtigt werden, wenn ein Benutzer in Ihrer Organisation Anmeldefehler aufgrund einer ungewöhnlichen IP-Adresse hat, die seinem üblichen Verhalten widerspricht.

Citrix Gateway erkennt diese Ereignisse und meldet sie an Citrix Analytics. Citrix Analytics erhält die Ereignisse und erhöht den Risikowert des Benutzers. Der Risikoindikator für **ungewöhnliche Authentifizierungsfehler** wird zur Risikozeitleiste des Benutzers hinzugefügt.

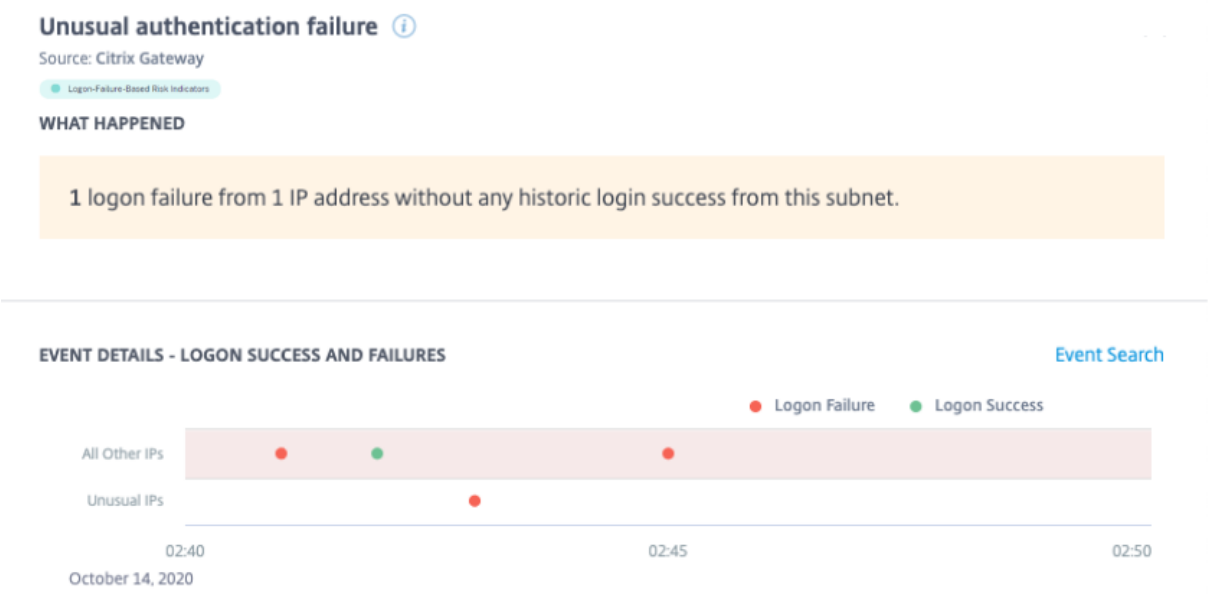
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Wie analysiert man den ungewöhnlichen Indikator für Authentifizierungsfehler?

Betrachten Sie die Benutzerin Georgina Kalou, die sich routinemäßig von ihren üblichen Heim- und Büronetzwerken aus bei Citrix Gateway anmeldet. Ein Remote-Angreifer versucht, Georginas Konto zu authentifizieren, indem er verschiedene Kennwörter errät, was zu Authentifizierungsfehlern in einem unbekannten Netzwerk führt.

In diesem Szenario meldet Citrix Gateway diese Ereignisse an Citrix Analytics, das Georgina Kalou eine aktualisierte Risikobewertung zuweist. Der Risikoindikator für ungewöhnliche Authentifizierung wird dem Risikozeitplan von Georgina Kalou hinzugefügt.

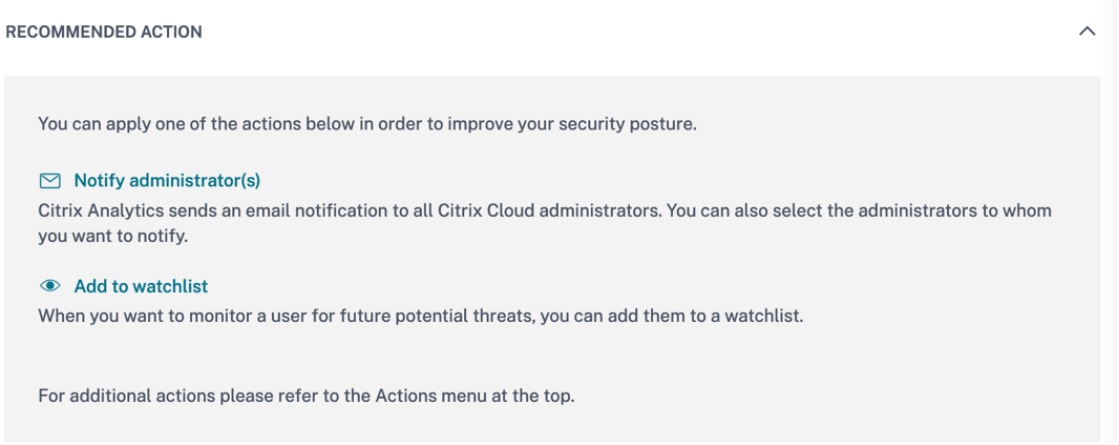
Aus der Risikozeitleiste von Georgina Kalou können Sie den gemeldeten Risikoindikator für ungewöhnliche Authentifizierungsfehler auswählen. Der Grund für das Ereignis wird zusammen mit Details wie der Zeitpunkt des Ereignisses und dem Ort angezeigt.



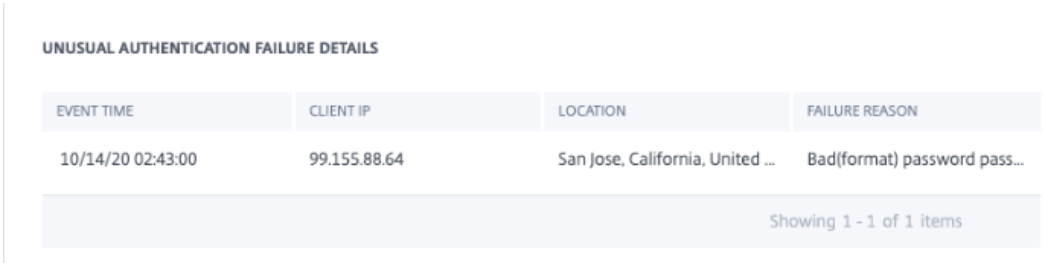
- Im Abschnitt **WHAT HAPPENED** können Sie die kurze Zusammenfassung anzeigen, die die Gesamtzahl der Authentifizierungsfehler und den Zeitpunkt des Ereignisses enthält.
- Im Abschnitt **RECOMMENDED ACTION** finden Sie die vorgeschlagenen Maßnahmen, die auf den Risikoindikator angewendet werden können. Citrix Analytics for Security empfiehlt die Aktionen je nach Schweregrad des vom Benutzer ausgehenden Risikos. Die Empfehlung kann eine oder eine Kombination der folgenden Aktionen sein:
  - Administrator (en) benachrichtigen
  - Zur Watchlist hinzufügen
  - Erstellen einer Richtlinie

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Sie können eine Aktion basierend auf der Empfehlung auswählen. Oder Sie können eine Aktion, die Sie je nach Ihrer Wahl anwenden möchten, aus dem Menü **Aktionen** auswählen. Weitere Informationen finden Sie unter Manuelles Anwenden einer Aktion.



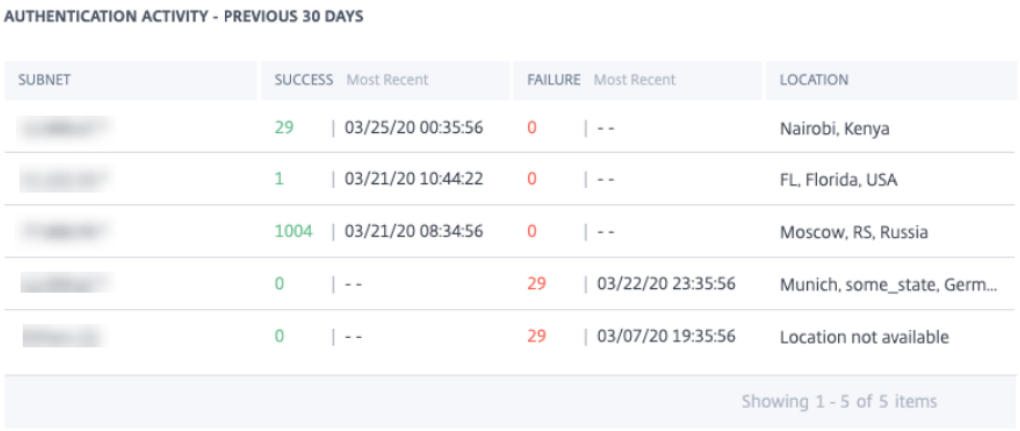
- Im Abschnitt **EVENT DETAILS** –**LOGON SUCCESS and FAILURES** können Sie ein Diagramm anzeigen, das die ungewöhnlichen Authentifizierungsfehler anzeigt, zusammen mit allen anderen Anmeldeaktivitäten, die während derselben Dauer erkannt wurden.
- Im Abschnitt **UNUSUAL AUTHENTICATION DETAILS** enthält die Tabelle die folgenden Informationen zu den ungewöhnlichen Authentifizierungsfehlern:
  - **Anmeldezeit** —Datum und Uhrzeit des Ereignisses
  - **Client-IP** —IP-Adresse des Benutzergeräts
  - **Ort** —Der Ort, von dem aus das Ereignis stattgefunden hat
  - **Grund für den Ausfall** —Der Grund für das Scheitern der



- Im Abschnitt **USER AUTHENTICATION ACTIVITY** –**PREVIOUS 30 DAYS** enthält die Tabelle die folgenden Informationen über die letzten 30 Tage der Authentifizierungsaktivität für den Benutzer:
  - Subnetz —Die IP-Adresse aus dem Benutzernetzwerk.
  - Erfolg —Die Gesamtzahl der erfolgreichen Authentifizierungsereignisse und der Zeitpunkt des letzten Erfolgsereignisses für den Benutzer.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Fehler —Die Gesamtzahl der fehlgeschlagenen Authentifizierungsereignisse und der Zeitpunkt des letzten fehlgeschlagenen Ereignisses für den Benutzer.
- Ort —Der Ort, von dem aus das Authentifizierungsereignis stattgefunden hat.



Welche Aktionen können Sie auf den Benutzer anwenden?

Sie können die folgenden Aktionen für das Benutzerkonto ausführen:

- **Zur Merkliste hinzufügen**. Wenn Sie einen Benutzer auf zukünftige potenzielle Bedrohungen überwachen möchten, können Sie ihn einer Watchlist hinzufügen.
- **Benachrichtigen Sie Administrator(en)**. Bei ungewöhnlichen oder verdächtigen Aktivitäten im Benutzerkonto wird eine E-Mail-Benachrichtigung an alle oder ausgewählte Administratoren gesendet.
- **Benutzer abmelden**. Wenn ein Benutzer von seinem Konto abgemeldet ist, kann er nicht über Citrix Gateway auf eine Ressource zugreifen, bis der Citrix Gateway-Administrator die Aktion Benutzer abmelden löscht.
- **Benutzer sperren**: Wenn das Konto eines Benutzers aufgrund anomalem Verhalten gesperrt ist, kann er nicht über Citrix Gateway auf eine Ressource zugreifen, bis der Gateway-Administrator das Konto entsperrt hat.

Weitere Informationen zu Aktionen und deren manueller Konfiguration finden Sie unter Richtlinien und Aktionen.

Um die Aktionen manuell auf den Benutzer anzuwenden, navigieren Sie zum Profil des Benutzers und wählen Sie den entsprechenden Risikoindikator aus. Wählen Sie im Menü **Aktionen** eine Aktion aus und klicken Sie auf **Übernehmen**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Hinweis**
>
> Unabhängig von der Datenquelle, die einen Risikoindikator auslöst, können Aktionen in Bezug auf andere Datenquellen angewendet werden.

Citrix Secure Private Access-Risikoindikatoren

April 12, 2024

Zugriff auf riskante Website

> **Hinweis**
>
> Die folgenden Funktionen von Citrix Analytics for Security sind beeinträchtigt, da die kategorienbasierte Webfilterung durch Secure Private Access nicht mehr unterstützt wird:
>
> 1. Datenfelder wie Kategorie-Gruppe, Kategorie und Reputation von URLs sind im Citrix Analytics for Security Dashboard nicht mehr verfügbar.
> 2. Der Indikator für riskante Website-Zugriffe, der auf denselben Daten basiert, ist ebenfalls veraltet und wird für Kunden nicht ausgelöst.
> 3. Alle vorhandenen benutzerdefinierten Risikoindikatoren, die die Datenfelder (Kategorie-Gruppe, Kategorie und Reputation von URLs) und die zugehörigen Richtlinien verwenden, werden nicht mehr ausgelöst.

Einzelheiten zur Einstellung von Secure Private Access finden Sie unter Veraltete Funktionen.

Versuch, auf eine URL auf der Sperrliste zuzugreifen

Citrix Analytics erkennt Datenzugriffsbedrohungen basierend auf den URLs auf der Sperrliste, auf die der Benutzer zugreift, und löst den entsprechenden Risikoindikator aus.

Der Risikoindikator **Versuch, auf eine URL auf der Sperrliste zuzugreifen**, wird in Citrix Analytics gemeldet, wenn ein Benutzer versucht, auf eine URL zuzugreifen, die in Secure Private Access auf der Sperrliste ist.

Der Risikofaktor im Zusammenhang mit dem Risikoindikator **Versuch, auf eine URL auf der Sperrliste zuzugreifen**, sind die anderen Risikoindikatoren. Weitere Informationen zu den Risikofaktoren finden Sie unter Citrix Benutzerrisikoindikatoren.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Wann wird der Risikoindikator “Versuch, auf eine URL auf der Sperrliste zuzugreifen” ausgelöst?

Secure Private Access hat eine URL-Kategorisierungsfunktion, die richtlinienbasierte Steuerung bietet, um den Zugriff auf URLs auf der Sperrliste einzuschränken. Wenn ein Benutzer versucht, auf eine URL auf der Sperrliste zuzugreifen, meldet Secure Private Access dieses Ereignis an Citrix Analytics. Citrix Analytics aktualisiert den Risikowert des Benutzers und fügt der Risikozeitleiste des Benutzers den Eintrag **Versuch, auf eine URL auf der Sperrliste zuzugreifen**, den Eintrag für den URL-Risikoindikator des Benutzers hinzu.

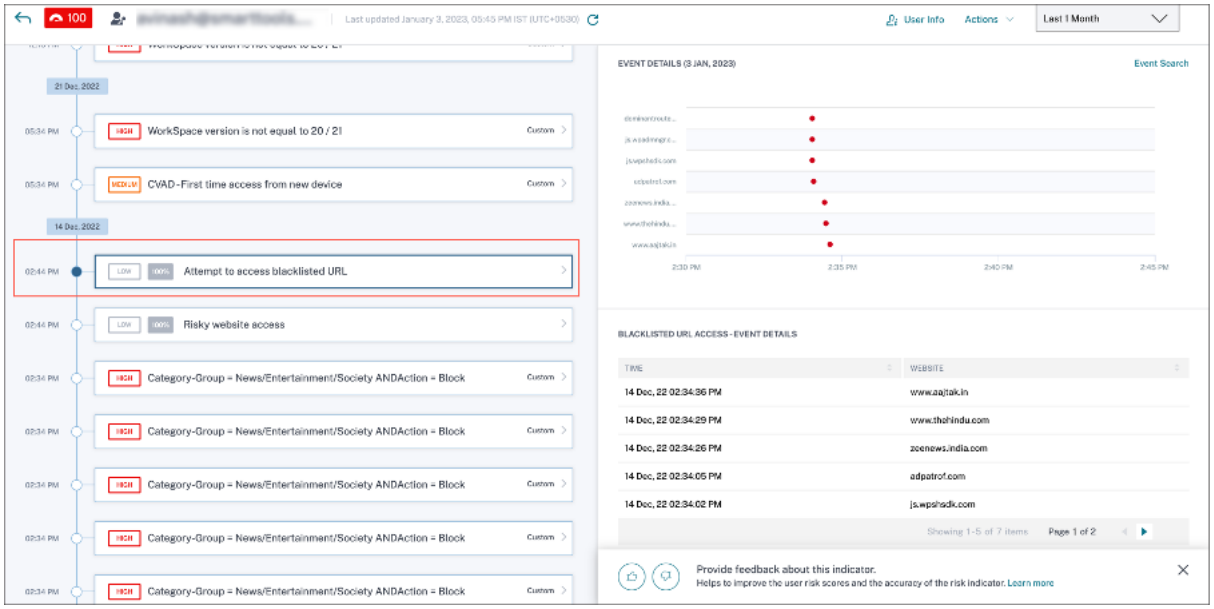
Wie analysiert man den Risikoindikator “Versuch, auf eine URL auf der Sperrliste zuzugreifen”?

Stellen Sie sich eine Benutzerin Georgina Kalou vor, die auf eine URL zugegriffen hat, die in Secure Private Access auf der Sperrliste ist. Secure Private Access meldet dieses Ereignis an Citrix Analytics, das Georgina Kalou eine aktualisierte Risikobewertung zuweist. Der Risikoindikator **Versuch, auf eine URL auf der Sperrliste zuzugreifen**, wird der Risikozeitleiste von Georgina Kalou hinzugefügt.

Aus der Risikozeitleiste von Georgina Kalou können Sie den gemeldeten **Versuch, auf eine URL auf der Sperrliste zuzugreifen**. Der Grund für das Ereignis wird zusammen mit den Details zu den Ereignissen angezeigt, z. B. Zeit des Ereignisses und Websitedetails.

Um den Eintrag **Versuch, auf eine URL auf der Sperrliste zuzugreifen**, für einen Benutzer anzuzeigen, navigieren Sie zu **Sicherheit > Benutzer** und wählen Sie den Benutzer aus.

Wenn Sie den Eintrag **Versuch, auf eine URL auf der Sperrliste zuzugreifen**-Risikoindikators aus der Timeline auswählen, wird im rechten Bereich ein entsprechendes detailliertes Informationsfeld angezeigt.

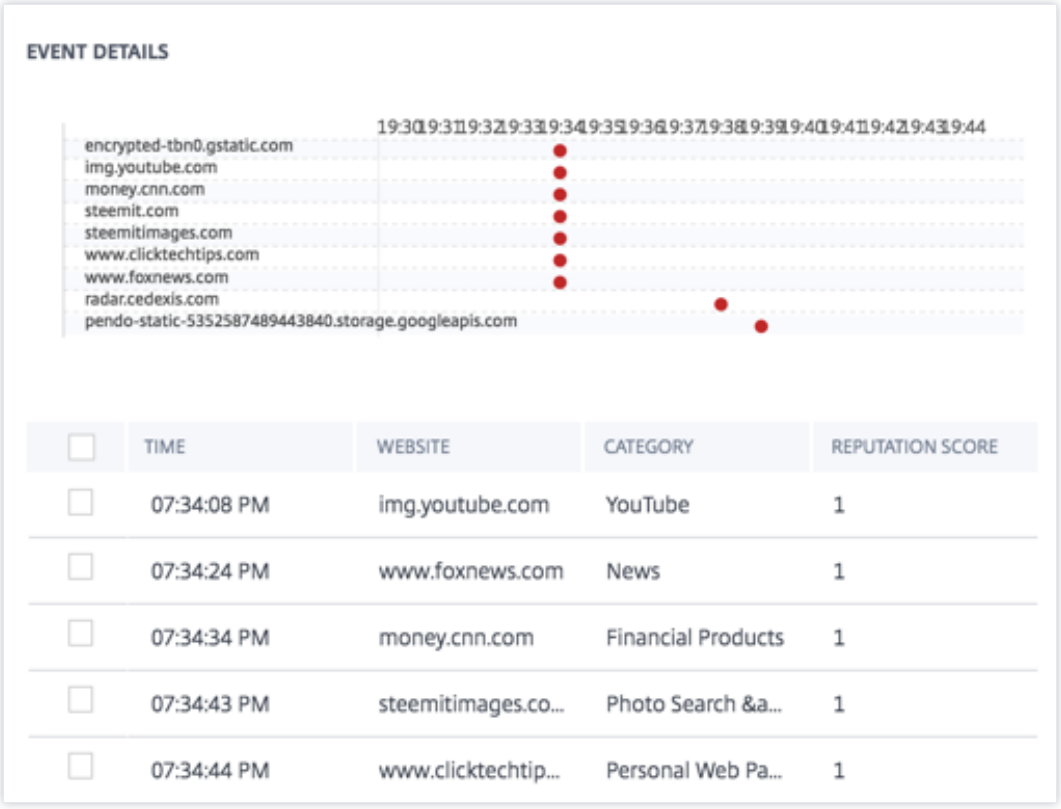


© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Der Abschnitt **WAS PASSIERT IST**, bietet eine kurze Zusammenfassung des Risikoindikators. Es enthält die Details der URL auf der Sperrliste, auf die der Benutzer während des ausgewählten Zeitraums zugegriffen hat.

- Der Abschnitt **EVENT-DETAILS** enthält eine Timeline-Visualisierung der einzelnen Ereignisse, die während des ausgewählten Zeitraums aufgetreten sind. Außerdem können Sie die folgenden wichtigen Informationen zu jedem Ereignisses anzeigen:
  - **Zeit**. Die Uhrzeit, zu der das Ereignis eintrat.
  - **Website**. Die riskante Website, auf die der Benutzer zugegriffen hat.
  - **Kategorie**. Die von Secure Private Access angegebene Kategorie für die URL auf der Sperrliste.
  - **Reputationsbewertung**. Die von Secure Private Access zurückgegebene Reputationsbewertung für die URL auf der Sperrliste. Weitere Informationen finden Sie unter URL Reputation Score.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Welche Aktionen können Sie auf den Benutzer anwenden?

Sie können die folgenden Aktionen für das Benutzerkonto ausführen:

- **Zur Merkliste hinzufügen**. Wenn Sie einen Benutzer auf zukünftige potenzielle Bedrohungen überwachen möchten, können Sie ihn einer Watchlist hinzufügen.
- **Benachrichtigen Sie Administrator(en)**. Bei ungewöhnlichen oder verdächtigen Aktivitäten im Benutzerkonto wird eine E-Mail-Benachrichtigung an alle oder ausgewählte Administratoren gesendet.

Weitere Informationen zu Aktionen und deren manueller Konfiguration finden Sie unter Richtlinien und Aktionen.

Um die Aktionen manuell auf den Benutzer anzuwenden, navigieren Sie zum Profil des Benutzers und wählen Sie den entsprechenden Risikoindikator aus. Wählen Sie im Menü **Aktionen** eine Aktion aus und klicken Sie auf **Übernehmen**.

> **Hinweis**
>
> Unabhängig von der Datenquelle, die einen Risikoindikator auslöst, können Aktionen in Bezug auf andere Datenquellen angewendet werden.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Ungewöhnliches Uploadvolumen

Citrix Analytics erkennt Datenzugriffsbedrohungen basierend auf ungewöhnlichen Upload-Volume-Aktivitäten und löst den entsprechenden Risikoindikator aus.

Der Indikator für **ungewöhnliches Upload-Volumenrisiko** wird gemeldet, wenn ein Benutzer überschüssiges Datenvolumen auf eine Anwendung oder Website hochlädt.

Der Risikofaktor, der mit dem Risikoindikator für ungewöhnliches Upload-Volumen verbunden ist, sind die Weitere Informationen zu den Risikofaktoren finden Sie unter Citrix Benutzerrisikoindikatoren.

Wann wird der Indikator für das ungewöhnliche Upload-Volumenrisiko ausgelöst?

Sie können Secure Private Access so konfigurieren, dass Benutzeraktivitäten wie bösartige, gefährliche oder unbekannte besuchte Websites und die verbrauchte Bandbreite sowie riskante Downloads und Uploads überwacht werden. Wenn ein Benutzer in Ihrer Organisation Daten auf eine Anwendung oder Website hochlädt, meldet Secure Private Access diese Ereignisse an Citrix Analytics.

Citrix Analytics überwacht all diese Ereignisse und wenn es feststellt, dass diese Benutzeraktivität dem üblichen Verhalten des Benutzers widerspricht, aktualisiert es den Risikowert des Benutzers. Der Indikator für das **ungewöhnliche Upload-Volumenrisiko** wird zur Risikozeitleiste des Benutzers hinzugefügt.

Wie analysiert man den ungewöhnlichen Upload-Volumenrisikoindikator?

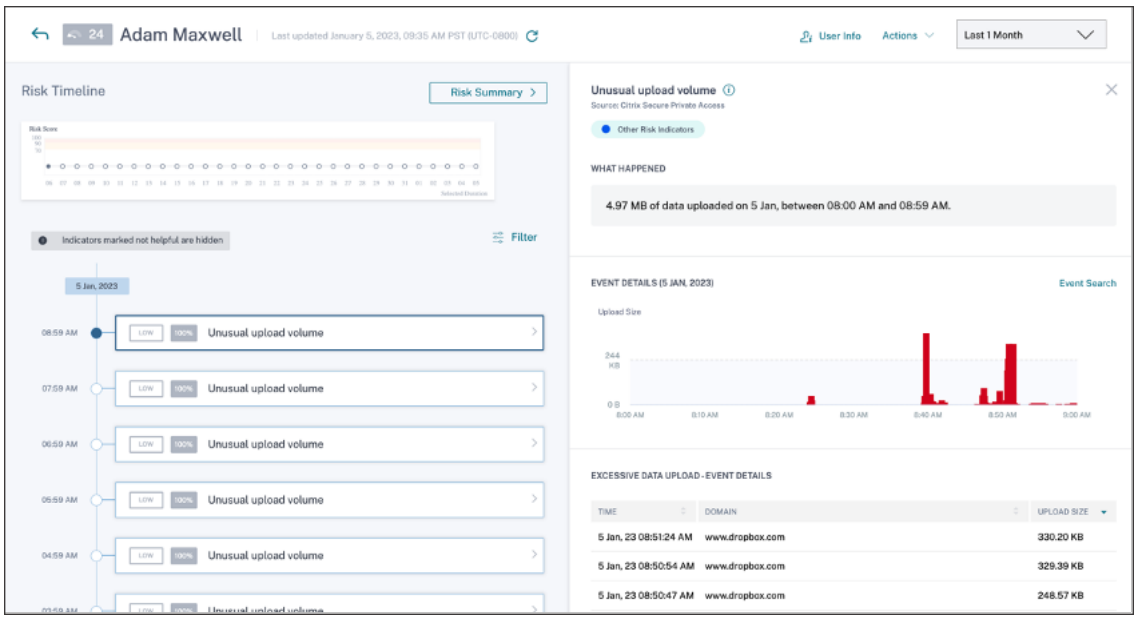
Betrachten Sie einen Benutzer Adam Maxwell, der überschüssiges Datenvolumen auf eine Anwendung oder Website hochgeladen hat. Secure Private Access meldet diese Ereignisse an Citrix Analytics, das Adam Maxwell eine aktualisierte Risikobewertung zuweist. Der Risikoindikator für das **ungewöhnliche Upload-Volumen** wird zur Risikozeitleiste von Adam Maxwell hinzugefügt.

Aus der Risikozeitleiste von Adam Maxwell können Sie den gemeldeten Risikoindikator für das **ungewöhnliche Upload-Volumen** auswählen. Der Grund für das Ereignis wird zusammen mit den Details zu den Ereignissen wie Uhrzeit des Ereignisses und der Domäne angezeigt.

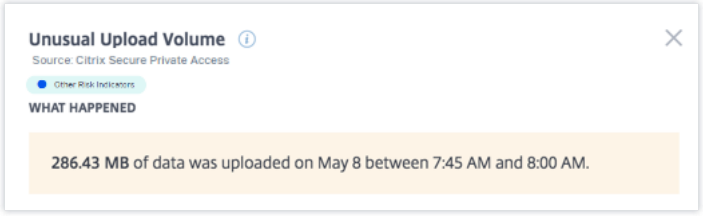
Um den Indikator für das **ungewöhnliche Upload-Volumenrisiko** anzuzeigen, navigieren Sie zu **Sicherheit > Benutzer**und wählen Sie den Benutzer aus.

Wenn Sie einen Eintrag für ein **ungewöhnliches Upload-Volumenrisikoindikator** aus der Zeitleiste auswählen, wird im rechten Bereich ein entsprechendes detailliertes Informationsfeld angezeigt.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

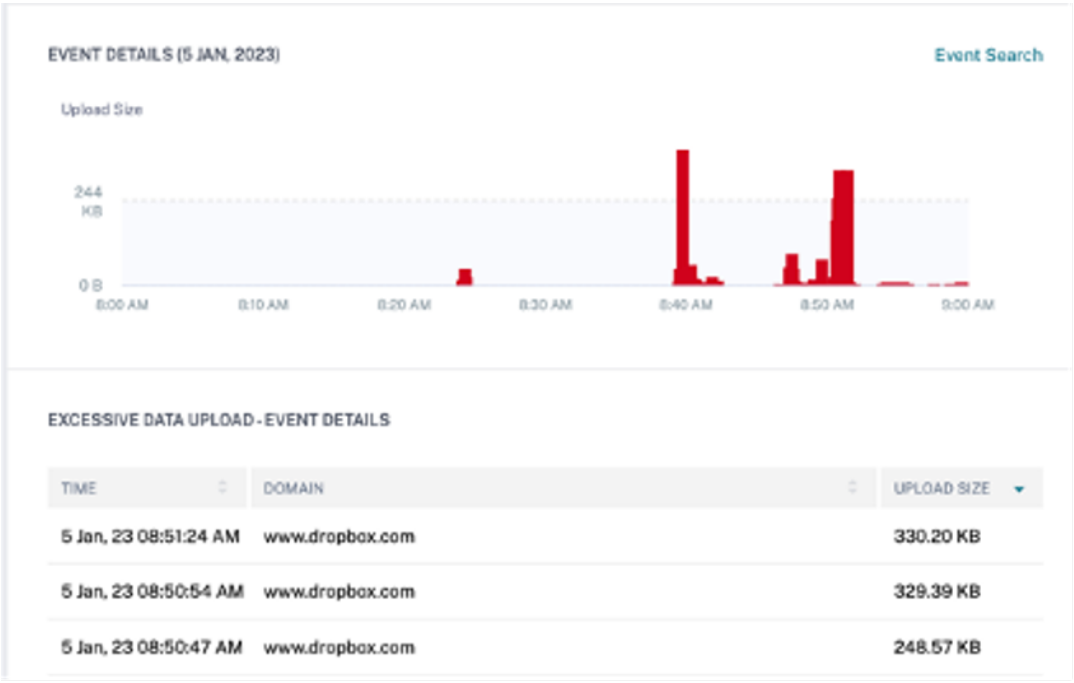


- Der Abschnitt **WAS PASSIERT IST**, bietet eine kurze Zusammenfassung des Risikoindikators, einschließlich des Volumens der während des ausgewählten Zeitraums hochgeladenen Daten.



- Der Abschnitt **EREIGNISDETAILS** enthält eine Timeline-Visualisierung der einzelnen Daten-Upload-Ereignisse, die während des ausgewählten Zeitraums aufgetreten sind. Außerdem können Sie die folgenden wichtigen Informationen zu jedem Ereignisses anzeigen:
  - **Zeit**. Die Zeit, zu der die übermäßigen Daten auf eine Anwendung oder eine Website hochgeladen wurden.
  - **Domäne**. Die Domäne, auf die der Benutzer die Daten hochgeladen hat.
  - **Upload-Größe**. Volumen der auf die Domain hochgeladenen Daten.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Welche Aktionen können Sie auf den Benutzer anwenden?

Sie können die folgenden Aktionen für das Benutzerkonto ausführen:

- **Zur Merkliste hinzufügen**. Wenn Sie einen Benutzer auf zukünftige potenzielle Bedrohungen überwachen möchten, können Sie ihn einer Watchlist hinzufügen.
- **Benachrichtigen Sie Administrator(en)**. Bei ungewöhnlichen oder verdächtigen Aktivitäten im Benutzerkonto wird eine E-Mail-Benachrichtigung an alle oder ausgewählte Administratoren gesendet.

Weitere Informationen zu Aktionen und deren manueller Konfiguration finden Sie unter Richtlinien und Aktionen.

Um die Aktionen manuell auf den Benutzer anzuwenden, navigieren Sie zum Profil des Benutzers und wählen Sie den entsprechenden Risikoindikator aus. Wählen Sie im Menü **Aktionen** eine Aktion aus und klicken Sie auf **Übernehmen**.

> **Hinweis**
>
> Unabhängig von der Datenquelle, die einen Risikoindikator auslöst, können Aktionen in Bezug auf andere Datenquellen angewendet werden.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Übermäßiger Datendownload

Citrix Analytics erkennt Datenzugriffsbedrohungen basierend auf den übermäßigen Daten, die von Benutzern in Ihrem Netzwerk heruntergeladen wurden, und löst den entsprechenden Risikoindikator aus.

Der Risikoindikator wird gemeldet, wenn ein Benutzer in Ihrer Organisation überschüssige Datenmengen von einer Anwendung oder Website herunterlädt.

Wann wird der Risikoindikator für übermäßiges Herunterladen von Daten ausgelöst?

Sie können Secure Private Access so konfigurieren, dass Benutzeraktivitäten wie bösartige, gefährliche oder unbekannte besuchte Websites und die verbrauchte Bandbreite sowie riskante Downloads und Uploads überwacht werden. Wenn ein Benutzer in Ihrer Organisation Daten von einer Anwendung oder Website herunterlädt, meldet Secure Private Access diese Ereignisse an Citrix Analytics.

Citrix Analytics überwacht alle diese Ereignisse und wenn es feststellt, dass die Benutzeraktivität dem üblichen Verhalten des Benutzers widerspricht, aktualisiert es den Risikowert des Benutzers. Der Risikoindikator für übermäßige Datendownloads wird zur Risikozeitleiste des Benutzers hinzugefügt.

Der mit dem Risikoindikator für übermäßige Datendownloads verbundene Risikofaktor sind die anderen Risikoindikatoren Weitere Informationen zu den Risikofaktoren finden Sie unter Citrix Benutzerrisikoindikatoren.

Wie analysiert man den Risikoindikator für übermäßige Datendownloads?

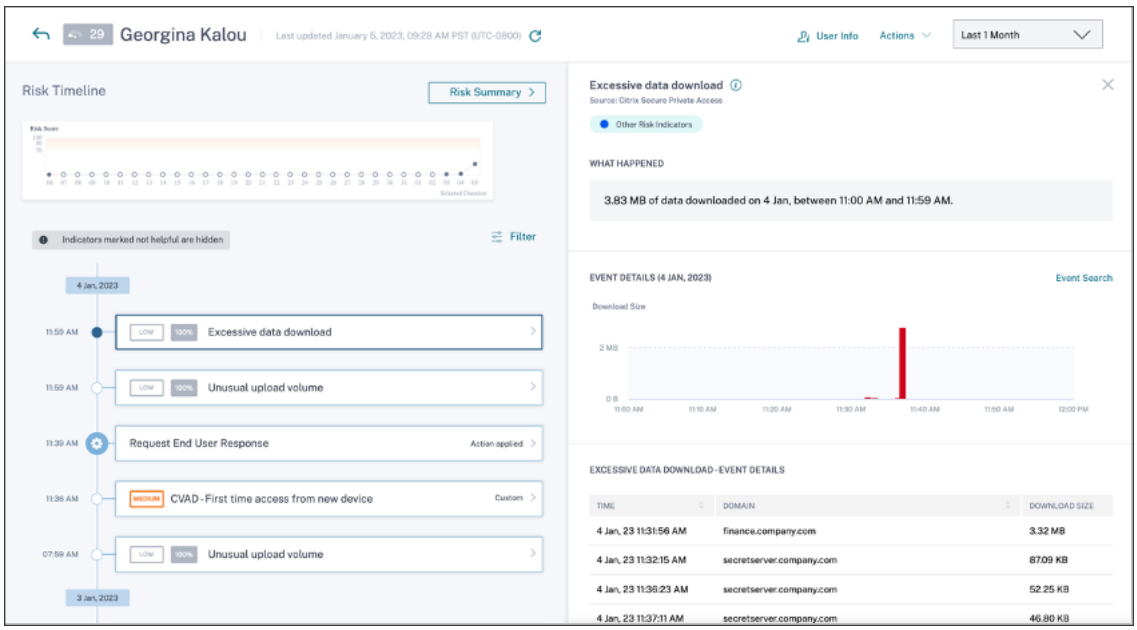
Betrachten Sie einen Benutzer Georgina Kalou, heruntergeladen überschüssiges Datenvolumen von einer Anwendung oder Website. Secure Private Access meldet diese Ereignisse an Citrix Analytics, das Georgina Kalou eine aktualisierte Risikobewertung zuweist und den Eintrag Risikoindikator für **übermäßigen Datendownload** zur Risikozeitleiste des Benutzers hinzufügt.

Aus der Risikozeitleiste von Georgina Kalou können Sie den gemeldeten Risikoindikator für **übermäßige Datendownloads** auswählen. Der Grund für das Ereignis wird zusammen mit den Details zu den Ereignissen wie Uhrzeit und Domaindetails angezeigt.

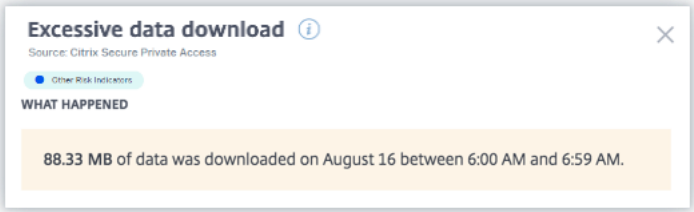
Um den Indikator für **übermäßige Datenübertragungsrisiken** anzuzeigen, navigieren Sie zu **Sicherheit > Benutzer**, und wählen Sie den Benutzer aus.

Wenn Sie den Risikoindikator für **übermäßige Daten** in der Zeitleiste auswählen, wird im rechten Bereich ein entsprechendes Detailinformationsfenster angezeigt.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

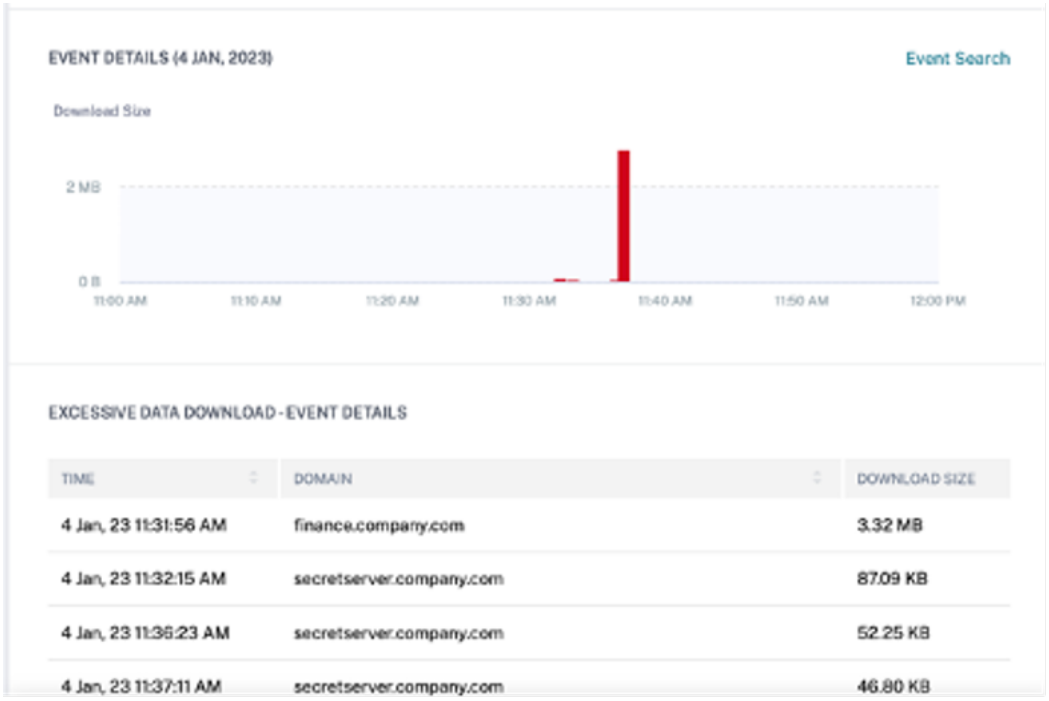


- Der Abschnitt **WAS PASSIERT IST**, bietet eine kurze Zusammenfassung des Risikoindikators, einschließlich des Volumens der während des ausgewählten Zeitraums heruntergeladenen Daten.



- Der Abschnitt **EVENT-DETAILS** enthält eine Timeline-Visualisierung der einzelnen Daten-Download-Ereignisse, die während des ausgewählten Zeitraums aufgetreten sind. Außerdem können Sie die folgenden wichtigen Informationen zu jedem Ereignisses anzeigen:
  - **Zeit**. Die Zeit, zu der die übermäßigen Daten auf eine Anwendung oder eine Website heruntergeladen wurden.
  - **Domäne**. Die Domäne, in die der Benutzer Daten heruntergeladen hat.
  - **Downloadgröße**. Volumen der auf die Domain heruntergeladenen Daten.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Welche Aktionen können Sie auf den Benutzer anwenden?

Sie können die folgenden Aktionen für das Benutzerkonto ausführen:

- **Zur Merkliste hinzufügen**. Wenn Sie einen Benutzer auf zukünftige potenzielle Bedrohungen überwachen möchten, können Sie ihn einer Watchlist hinzufügen.
- **Benachrichtigen Sie Administrator(en)**. Bei ungewöhnlichen oder verdächtigen Aktivitäten im Benutzerkonto wird eine E-Mail-Benachrichtigung an alle oder ausgewählte Administratoren gesendet.

Weitere Informationen zu Aktionen und deren manueller Konfiguration finden Sie unter Richtlinien und Aktionen.

Um die Aktionen manuell auf den Benutzer anzuwenden, navigieren Sie zum Profil des Benutzers und wählen Sie den entsprechenden Risikoindikator aus. Wählen Sie im Menü **Aktionen** eine Aktion aus und klicken Sie auf **Übernehmen**.

> **Hinweis**
>
> Unabhängig von der Datenquelle, die einen Risikoindikator auslöst, können Aktionen in Bezug auf andere Datenquellen angewendet werden.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Citrix Virtual Apps and Desktops und Citrix DaaS-Risikoindikatoren

July 12, 2022

Unmögliche Reisen

Citrix Analytics erkennt die Anmeldungen eines Benutzers als riskant, wenn die aufeinanderfolgenden Anmeldungen aus zwei verschiedenen Ländern innerhalb eines Zeitraums erfolgen, der unter der erwarteten Reisezeit zwischen den Ländern liegt.

Das Szenario der unmöglichen Reisezeit weist auf folgende Risiken hin:

- **Kompromittierte Anmeldeinformationen**: Ein Remote-Angreifer stiehlt die Anmeldeinformationen eines legitimen Benutzers.
- **Gemeinsame Anmeldeinformationen**: Verschiedene Benutzer verwenden dieselben Benutzeranmeldeinformationen.

Wann wird der Indikator Unmögliches Reiserisiko ausgelöst?

Der Indikator für **unmögliches Reiserisiko** wertet die Zeit und die geschätzte Entfernung zwischen jedem Paar aufeinanderfolgender Benutzeranmeldungen aus und löst aus, wenn die Entfernung größer ist, als eine einzelne Person in dieser Zeit möglicherweise zurücklegen kann.

> **Hinweis:**
>
> Dieser Risikoindikator enthält auch eine Logik zur Reduzierung von Fehlalarmen für die folgenden Szenarien, die nicht die tatsächlichen Standorte der Benutzer widerspiegeln:
>
> - Wenn sich Benutzer über Proxyverbindungen bei virtuellen Apps und Desktops anmelden.
> - Wenn sich Benutzer von gehosteten Clients bei virtuellen Apps und Desktops anmelden.

So analysieren Sie den Indikator für unmögliches Risiko

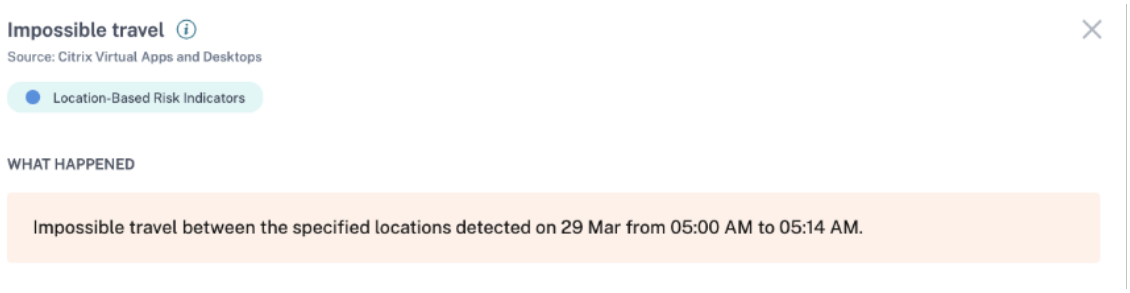
Man denke an den Benutzer Adam Maxwell, der sich innerhalb einer Minute von zwei Standorten aus anmeldet - Moskva, Russland und Hohhot, China. Citrix Analytics erkennt dieses Anmeldeereignis als unmögliches Reiseszenario und löst den Indikator **Unmögliche Reise** aus. Der Risikoindikator wird dem Risikozeitplan von Adam Maxwell hinzugefügt und ihm wird ein Risiko-Score zugewiesen.

Um die Risikozeitleiste von Adam Maxwell anzuzeigen, wählen Sie **Sicherheit > Benutzer**aus. Wählen Sie im Bereich **Riskante Benutzer** den Benutzer Adam Maxwell aus.

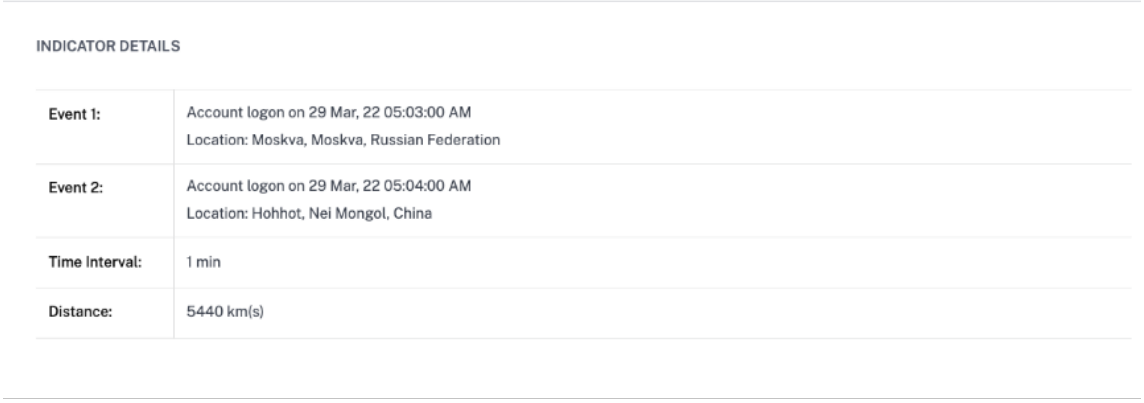
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Wählen Sie in Adam Maxwells Risiko-Timeline den Indikator **Unmögliches Reiserisiko** aus. Sie können die folgenden Informationen anzeigen:

- Der Abschnitt **WHAT** HAPPENED bietet eine kurze Zusammenfassung des unmöglichen Reiseereignisses.

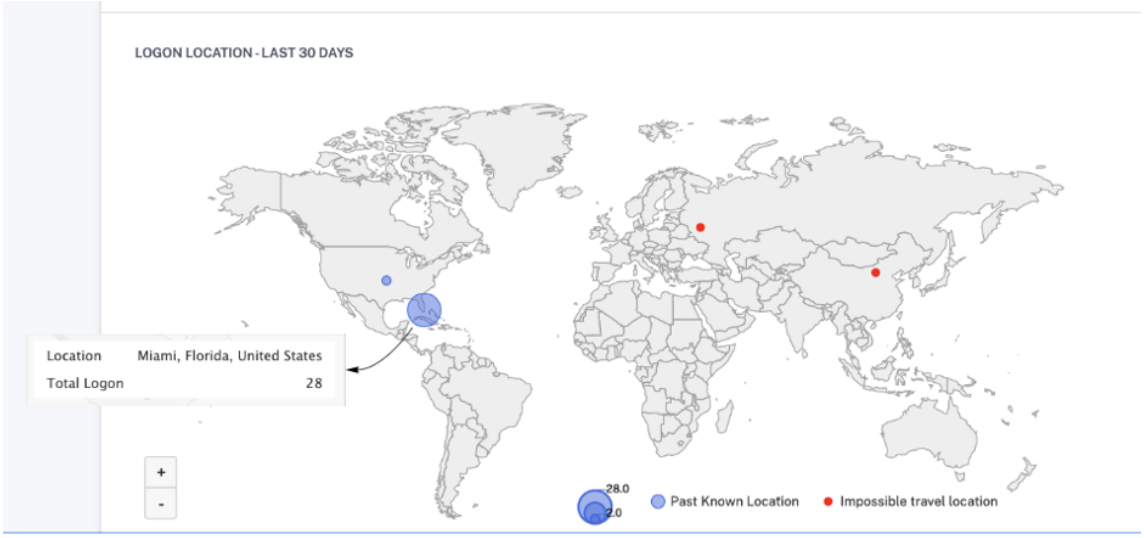


- Der Abschnitt **INDICATOR DETAILS** enthält die Standorte, von denen aus sich der Benutzer angemeldet hat, die Zeitdauer zwischen den aufeinanderfolgenden Anmeldungen und die Entfernung zwischen den beiden Standorten.



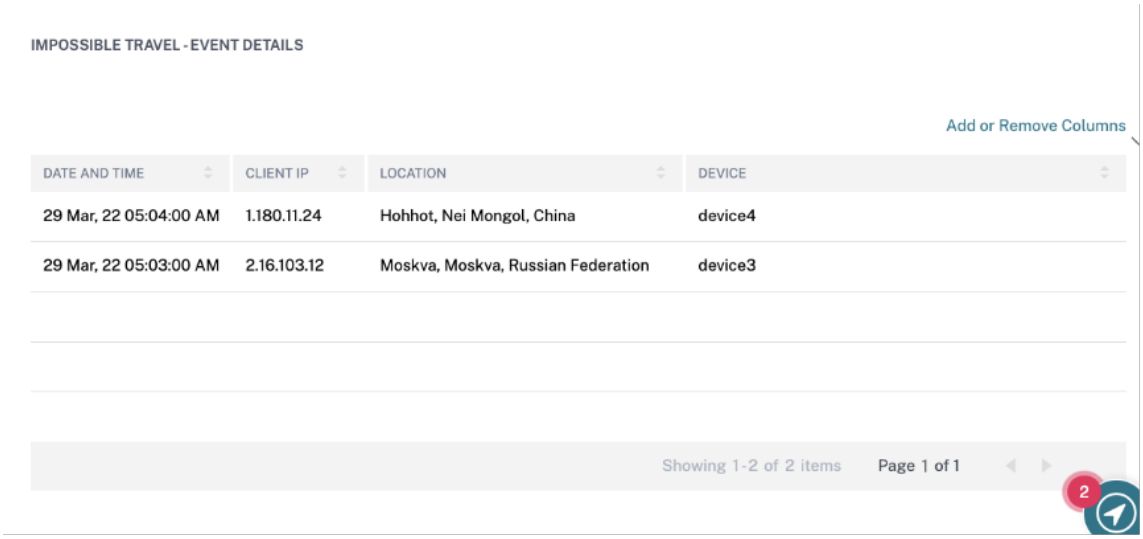
- Im Abschnitt **LOGON LOCATION- LAST 30 DAYS** wird eine geografische Kartenansicht der unmöglichen Reiseorte und der bekannten Standorte des Benutzers angezeigt. Die Standortdaten werden für die letzten 30 Tage angezeigt. Sie können mit der Maus über die Zeiger auf der Karte fahren, um die Gesamtzahl der Anmeldungen von jedem Standort aus anzuzeigen.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



- Der Abschnitt **IMPOSSIBLE TRAVEL** —**EVENT DETAILS** enthält die folgenden Informationen über das unmögliche Reiseereignis:
  - **Datum und Uhrzeit**: Gibt das Datum und die Uhrzeit der Anmeldungen an.
  - **Client-IP**: Zeigt die IP-Adresse des Benutzergeräts an.
  - **Standort**: Gibt den Ort an, von dem aus sich der Benutzer angemeldet hat.
  - **Gerät**: Zeigt den Gerätenamen des Benutzers an.
  - **Anmeldetyp**: Zeigt an, ob es sich bei der Benutzeraktivität um eine Sitzungsanmeldung oder eine Kontoanmeldung handelt. Das Kontoanmeldeereignis wird ausgelöst, wenn die Authentifizierung eines Benutzers bei seinem Konto erfolgreich ist. Während das Sitzungsanmeldeereignis ausgelöst wird, wenn ein Benutzer seine Anmeldeinformationen eingibt und sich bei seiner App- oder Desktopsitzung anmeldet.
  - **Betriebssystem**: Zeigt das Betriebssystem des Benutzergeräts an.
  - **Browser**: Zeigt den Webbrowser an, der für den Zugriff auf die Anwendung verwendet wird.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Welche Aktionen können Sie auf die Benutzer anwenden?

Sie können die folgenden Aktionen für das Konto des Benutzers ausführen:

- **Zur Merkliste hinzufügen**. Wenn Sie einen Benutzer auf zukünftige potenzielle Bedrohungen überwachen möchten, können Sie ihn einer Watchlist hinzufügen.
- **Benachrichtigen Sie Administrator(en)**. Bei ungewöhnlichen oder verdächtigen Aktivitäten im Konto des Benutzers wird eine E-Mail-Benachrichtigung an alle oder ausgewählte Administratoren gesendet.
- **Benutzer abmelden**. Wenn ein Benutzer von seinem Konto abgemeldet ist, kann er nicht über virtuelle Desktops auf die Ressource zugreifen.
- **Sitzungsaufzeichnung starten**. Wenn ein ungewöhnliches Ereignis für das Virtual Desktops-Konto des Benutzers auftritt, kann der Administrator mit der Aufzeichnung der Benutzeraktivitäten zukünftiger Anmeldesitzungen beginnen. Wenn der Benutzer jedoch Citrix Virtual Apps and Desktops 7.18 oder höher verwendet, kann der Administrator die Aufzeichnung der aktuellen Anmeldesitzung des Benutzers dynamisch starten und beenden.

Weitere Informationen zu Aktionen und deren manueller Konfiguration finden Sie unter Richtlinien und Aktionen.

Um die Aktionen manuell auf den Benutzer anzuwenden, navigieren Sie zum Benutzerprofil und wählen Sie den entsprechenden Risikoindikator aus. Wählen Sie im Menü **Aktion** eine Aktion aus und klicken Sie auf **Übernehmen**.

> **Hinweis**
>
> Unabhängig von der Datenquelle, die einen Risikoindikator auslöst, können Aktionen in Bezug auf andere Datenquellen angewendet werden.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Potenzielle Datenexfiltration

Citrix Analytics erkennt Datenbedrohungen basierend auf übermäßigen Versuchen, Daten zu exfiltrieren, und löst den entsprechenden Risikoindikator aus.

Der mit dem Risikoindikator für potenzielle Datenexfiltration verbundene Risikofaktor sind die datenbasierten Risikoindikatoren. Weitere Informationen zu den Risikofaktoren finden Sie unter Citrix Benutzerrisikoindikatoren.

Der Risikoindikator für **potenzielle Datenexfiltration** wird ausgelöst, wenn ein Citrix Receiver-Benutzer versucht, Dateien auf ein Laufwerk oder einen Drucker herunterzuladen oder zu übertragen. Diese Daten können ein Ereignis zum Herunterladen von Dateien sein, z. B. das Herunterladen einer Datei auf ein lokales Laufwerk, zugeordnete Laufwerke oder ein externes Speichergerät. Die Daten können auch mit der Zwischenablage oder mit der Aktion zum Kopieren und Einfügen exfiltriert werden.

> **Hinweis**
>
> Die Zwischenablage wird nur von den SaaS-Anwendungen unterstützt.

Wann wird der Risikoindikator für potenzielle Datenexfiltration ausgelöst?

Sie können benachrichtigt werden, wenn ein Benutzer in einem bestimmten Zeitraum eine übermäßige Anzahl von Dateien auf ein Laufwerk oder einen Drucker übertragen hat. Dieser Risikoindikator wird auch ausgelöst, wenn der Benutzer die Aktion zum Kopieren und Einfügen auf seinem lokalen Computer verwendet.

Wenn Citrix Receiver dieses Verhalten erkennt, empfängt Citrix Analytics dieses Ereignis und weist dem jeweiligen Benutzer eine Risikobewertung zu. Der Risikoindikator für **potenzielle Datenexfiltration** wird zur Risikozeitleiste des Benutzers hinzugefügt.

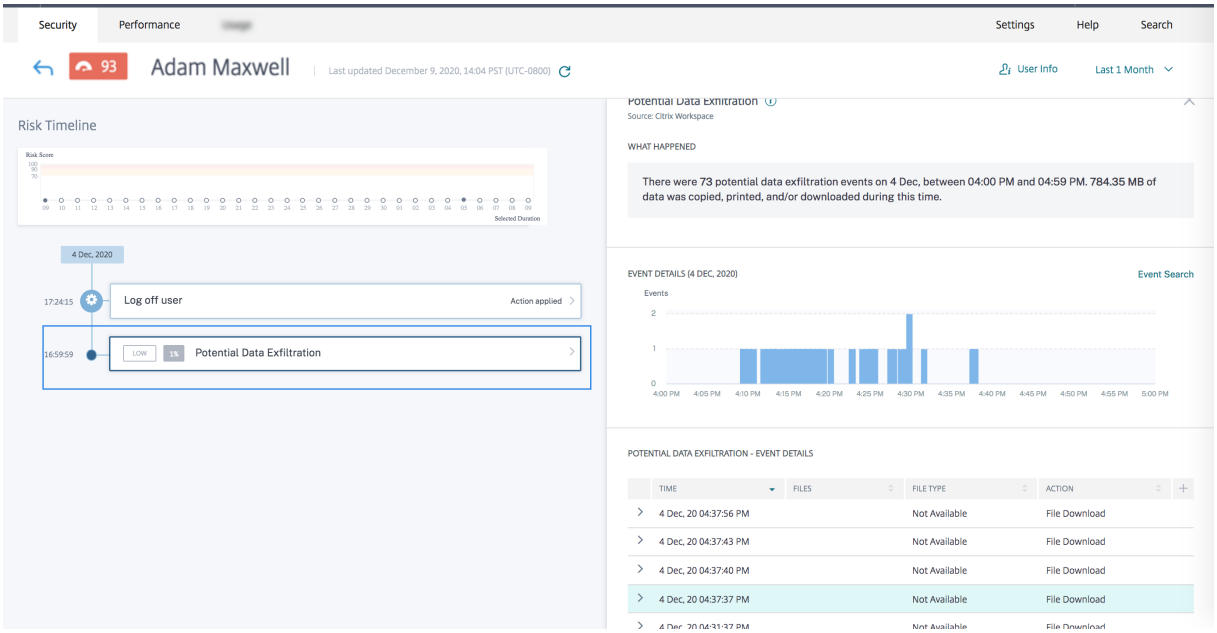
Wie analysiert man den Risikoindikator für potenzielle Datenexfiltration?

Betrachten Sie den Benutzer Adam Maxwell, der an einer Sitzung angemeldet ist und versucht, Dateien zu drucken, die das vordefinierte Limit überschreiten. Durch diese Aktion hatte Adam Maxwell sein normales Dateiübertragungsverhalten basierend auf maschinellem Lernen überschritten.

Aus der Zeitleiste von Adam Maxwell können Sie den Risikoindikator für **potenzielle Datenexfiltration** auswählen. Der Grund für das Ereignis wird zusammen mit den Details wie den übertragenen Dateien und dem Gerät, mit dem die Datei übertragen wurde, angezeigt.

Um den für einen Benutzer gemeldeten Risikoindikator für die **potenzielle Datenexfiltration** anzuzeigen, navigieren Sie zu **Sicherheit > Benutzer**und wählen Sie den Benutzer aus.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



- Im Abschnitt **WHAT HAPPENED**, können Sie die Zusammenfassung des potenziellen Datenexfiltrationsereignisses anzeigen. Sie können die Anzahl der Datenexfiltrationsereignisse während eines bestimmten Zeitraums anzeigen.

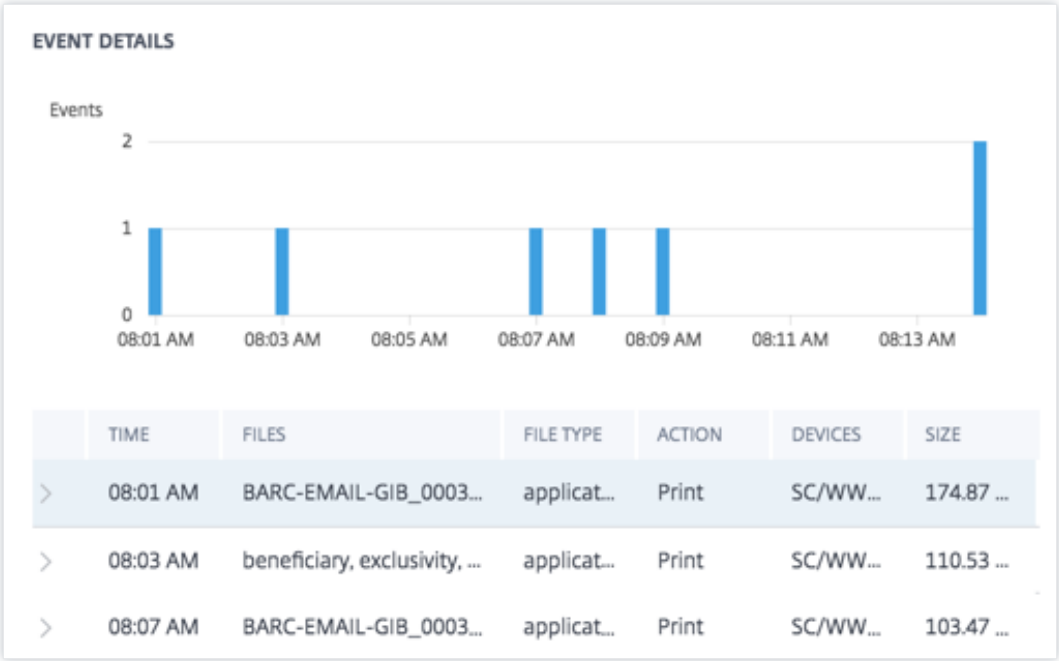
- Im Abschnitt **EVENT-DETAILS** werden die Versuche der Datenexfiltration in einem grafischen und tabellarischen Format angezeigt. Die Ereignisse werden als einzelne Einträge in der Grafik angezeigt, und die Tabelle enthält die folgenden wichtigen Informationen:
  - **Time**. Die Zeit, zu der das Datenexfiltrationsereignis eintrat
  - **Akten**. Die Datei, die entweder heruntergeladen, gedruckt oder kopiert wurde.
  - **Dateityp**. Der Dateityp, der entweder heruntergeladen, gedruckt oder kopiert wurde.

    > **Hinweis**
    >
    > Der gedruckte Dateiname ist nur über das Druckereignis für SaaS-Apps verfügbar.

  - **Aktion**. Die Art von Datenexfiltrationsereignis, die durchgeführt wurden - Drucken, Herunterladen oder Kopieren.
  - **Geräte**. Das verwendete Gerät.
  - **Größe**. Die Größe der Datei, die exfiltriert wird.

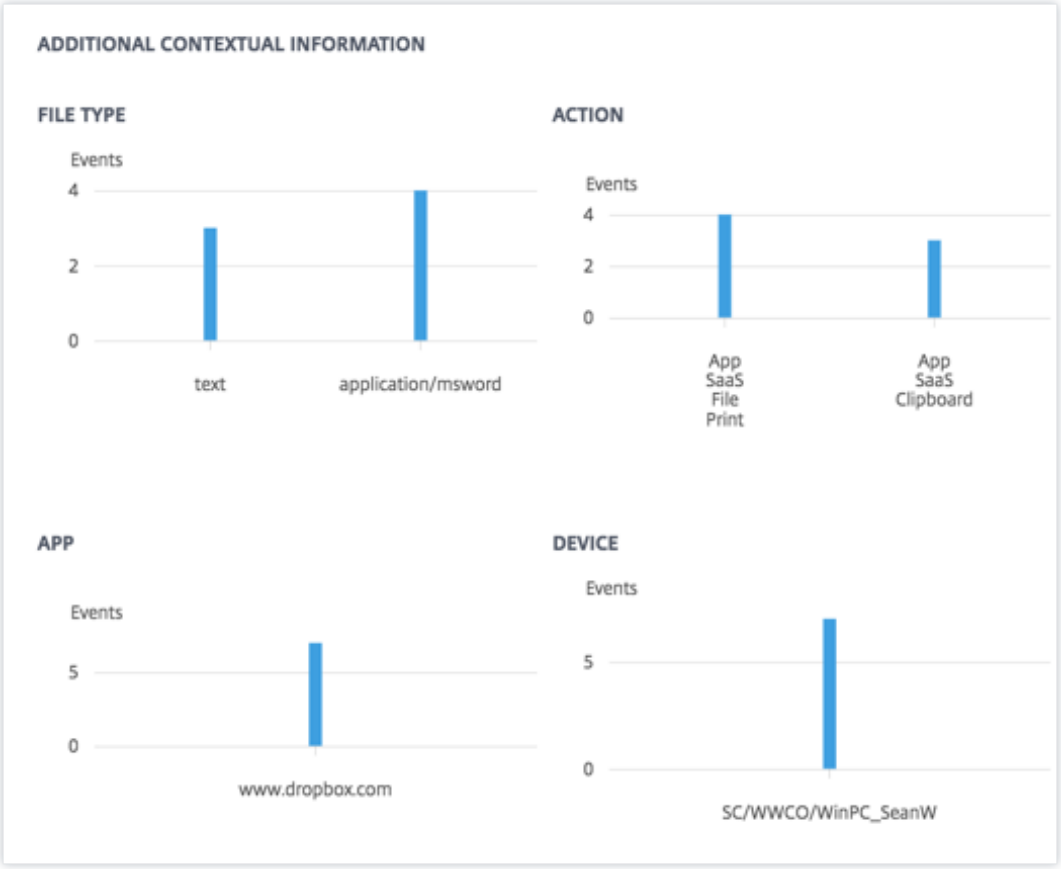
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Standort**. Die Stadt, aus der der Benutzer versucht, Daten zu exfiltrieren.



- Im Abschnitt **ADDITIONAL CONTEXTUAL INFORMATION** können Sie während des Auftretens des Ereignisses Folgendes anzeigen:
  - Die Anzahl der Dateien, die exfiltriert wurden.
  - Die durchgeführten Aktionen.
  - Die verwendeten Anwendungen.
  - Vom Benutzer verwendetes Gerät.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Welche Aktionen können Sie auf den Benutzer anwenden?

Sie können die folgenden Aktionen für das Benutzerkonto ausführen:

- **Zur Merkliste hinzufügen**. Wenn Sie einen Benutzer auf zukünftige potenzielle Bedrohungen überwachen möchten, können Sie ihn einer Watchlist hinzufügen.
- **Benachrichtigen Sie Administrator(en)**. Bei ungewöhnlichen oder verdächtigen Aktivitäten im Benutzerkonto wird eine E-Mail-Benachrichtigung an alle oder ausgewählte Administratoren gesendet.
- **Benutzer abmelden**. Wenn ein Benutzer von seinem Konto abgemeldet ist, kann er nicht über virtuelle Desktops auf die Ressource zugreifen.
- **Sitzungsaufzeichnung starten**. Wenn das Virtual Desktop-Konto des Benutzers ein ungewöhnliches Ereignis vorliegt, kann der Administrator mit der Aufzeichnung der Aktivitäten des Benutzers zukünftiger Anmeldesitzungen beginnen. Wenn der Benutzer jedoch Citrix Virtual Apps and Desktops 7.18 oder höher aktiviert ist, kann der Administrator die Aufzeichnung der aktuellen Anmeldesitzung des Benutzers dynamisch starten und beenden.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Weitere Informationen zu Aktionen und deren manueller Konfiguration finden Sie unter Richtlinien und Aktionen.

Um die Aktionen manuell auf den Benutzer anzuwenden, navigieren Sie zum Profil des Benutzers und wählen Sie den entsprechenden Risikoindikator aus. Wählen Sie im Menü **Aktion** eine Aktion aus und klicken Sie auf **Übernehmen**.

> **Hinweis**
>
> Unabhängig von der Datenquelle, die einen Risikoindikator auslöst, können Aktionen in Bezug auf andere Datenquellen angewendet werden.

Verdächtige Anmeldung

Citrix Analytics erkennt die Anmeldungen des Benutzers, die ungewöhnlich oder riskant erscheinen, basierend auf mehreren Kontextfaktoren, die gemeinsam durch das Gerät, den Standort und das Netzwerk definiert werden, die vom Benutzer verwendet werden.

Wann wird der Risikoindikator für verdächtige Anmeldung ausgelöst?

Der Risikoindikator wird durch die Kombination der folgenden Faktoren ausgelöst, wobei jeder Faktor aufgrund einer oder mehrerer Bedingungen als potenziell verdächtig angesehen wird.

Faktor	Bedingungen
Ungewöhnliches Gerät	Der Benutzer meldet sich von einem Gerät aus an, das in den letzten 30 Tagen nicht verwendet wurde. Der Benutzer meldet sich von einem HTML5-Client oder einem Chrome-Client aus an, wo die Gerätesignatur nicht mit dem Verlauf des Benutzers übereinstimmt.
Ungewöhnlicher Ort	Melden Sie sich von einer Stadt oder einem Land aus an, in dem sich der Benutzer in den letzten 30 Tagen nicht angemeldet hat. Die Stadt oder das Land ist geografisch weit von den letzten (letzten 30 Tagen) Anmeldeorten entfernt.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Faktor	Bedingungen
	Null oder mindestens Benutzer haben sich in den letzten 30 Tagen von der Stadt oder dem Land aus angemeldet.
Ungewöhnliches Netzwerk	Melden Sie sich von einer IP-Adresse aus an, die der Benutzer in den letzten 30 Tagen nicht verwendet hat. Melden Sie sich von einem IP-Subnetz aus an, das der Benutzer in den letzten 30 Tagen nicht verwendet hat. Null oder mindestens Benutzer haben sich in den letzten 30 Tagen vom IP-Subnetz aus angemeldet.
IP-Bedrohung	Die IP-Adresse wird vom Community Threat Intelligence Feed Webroot als hohes Risiko identifiziert. Citrix Analytics hat kürzlich sehr verdächtige Anmeldeaktivitäten anhand der IP-Adresse anderer Benutzer erkannt.

So analysieren Sie den Risikoindikator für verdächtige Anmeldung

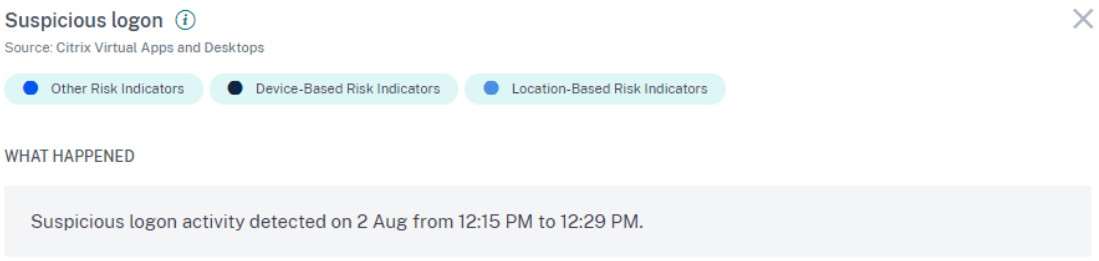
Betrachten Sie den Benutzer Adam Maxwell, der sich zum ersten Mal aus Mumbai, Indien, anmeldet. Er verwendet ein neues Gerät oder ein Gerät, das in den letzten 30 Tagen nicht verwendet wurde, um sich bei Citrix Virtual Apps and Desktops anzumelden und eine Verbindung zu einem neuen Netzwerk herzustellen. Citrix Analytics erkennt dieses Anmeldeereignis als verdächtig, da die Faktoren Standort, Gerät und Netzwerk von seinem üblichen Verhalten abweichen und den Indikator für **verdächtiges Anmelderisiko auslösen** . Der Risikoindikator wird zu Adam Maxwells Risikozeitplan hinzugefügt und ihm wird ein Risiko-Score zugewiesen.

Um Adam Maxwells Risikozeit anzuzeigen, wählen Sie **Sicherheit > Benutzer**. Wählen Sie im Bereich **Riskante Benutzer** den Benutzer Adam Maxwell aus.

Wählen Sie in der Risikozeitleiste von Adam Maxwell den Risikoindikator für verdächtige Anmeldung aus. Sie können die folgenden Informationen anzeigen:

- Der Abschnitt **WHAT** HAPPENED bietet eine kurze Zusammenfassung der verdächtigen Aktivitäten, einschließlich der Risikofaktoren und des Zeitpunkts des Ereignisses.

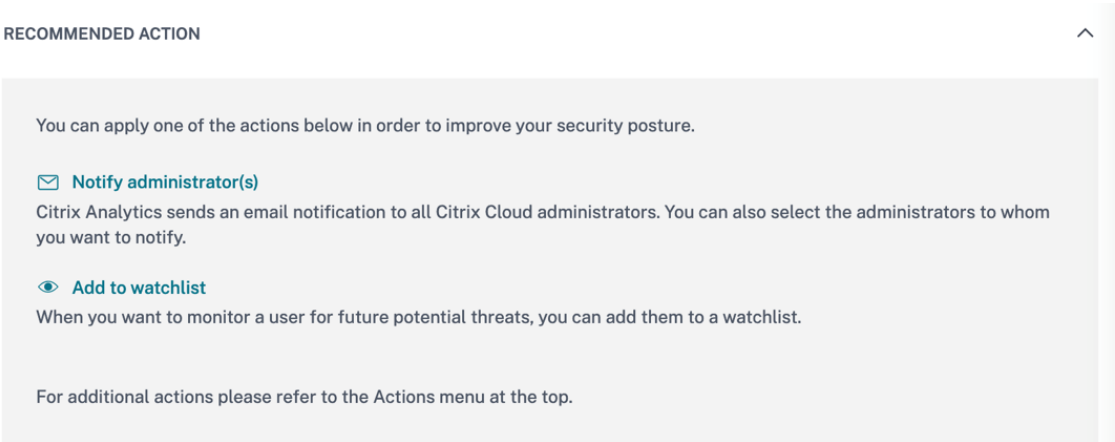
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



- Im Abschnitt **RECOMMENDED ACTION** finden Sie die vorgeschlagenen Maßnahmen, die auf den Risikoindikator angewendet werden können. Citrix Analytics for Security empfiehlt die Aktionen je nach Schweregrad des vom Benutzer ausgehenden Risikos. Die Empfehlung kann eine oder eine Kombination der folgenden Aktionen sein:

  - Administrator (en) benachrichtigen
  - Zur Watchlist hinzufügen
  - Erstellen einer Richtlinie

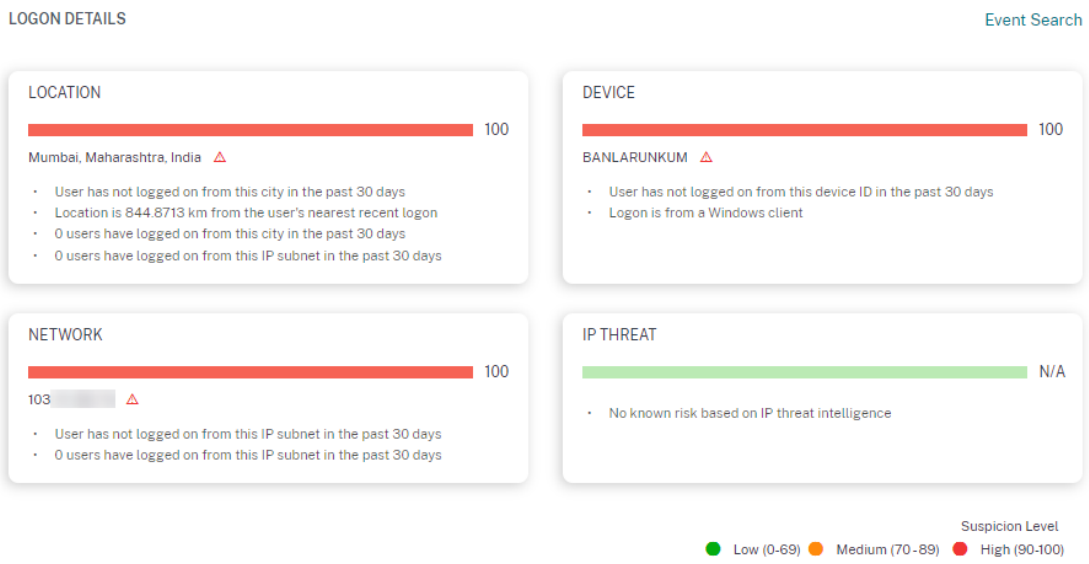
  Sie können eine Aktion basierend auf der Empfehlung auswählen. Oder Sie können eine Aktion, die Sie je nach Ihrer Wahl anwenden möchten, aus dem Menü **Aktionen** auswählen. Weitere Informationen finden Sie unter Manuelles Anwenden einer Aktion.



- Der Abschnitt **LOGON DETAILS** enthält eine detaillierte Zusammenfassung der verdächtigen Aktivitäten, die den einzelnen Risikofaktoren entsprechen. Jedem Risikofaktor wird ein Score zugewiesen, der das Verdachtsniveau angibt. Jeder einzelne Risikofaktor weist nicht auf ein hohes Risiko eines Benutzers hin. Das Gesamtrisiko basiert auf der Korrelation der verschiedenen Risikofaktoren.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Stufe des Verdachts	Indikation
0–69	Der Faktor scheint normal zu sein und wird nicht als verdächtig angesehen.
70–89	Der Faktor erscheint etwas ungewöhnlich und wird bei anderen Faktoren als mäßig verdächtig angesehen.
90–100	Der Faktor ist völlig neu oder ungewöhnlich und wird bei anderen Faktoren als äußerst verdächtig angesehen.

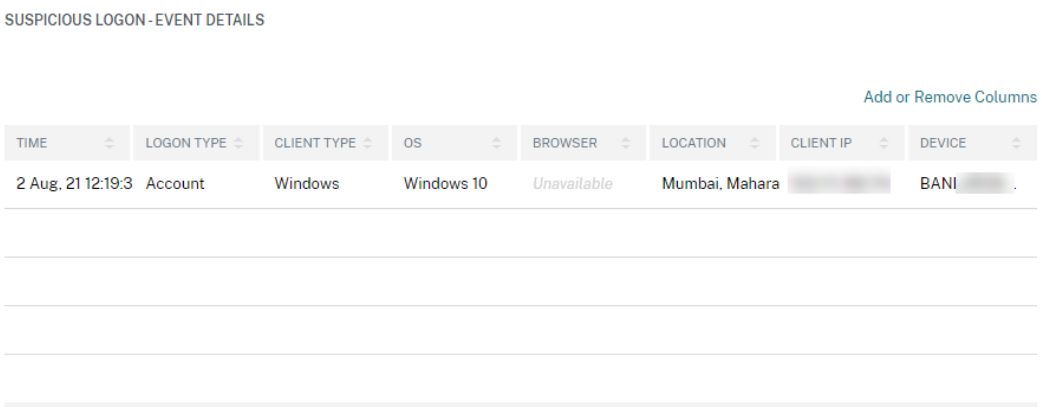


- Im Abschnitt **LOGON LOCATION- LAST 30 DAY** wird eine geografische Kartenansicht der letzten bekannten Standorte und des aktuellen Standorts des Benutzers angezeigt. Die Standortdaten werden für die letzten 30 Tage angezeigt. Sie können mit der Maus über die Zeiger auf der Karte fahren, um die Gesamtzahl der Anmeldungen von jedem Standort aus anzuzeigen.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Der Abschnitt **SUSPICIOUS LOGON- EVENT DETAILS** enthält die folgenden Informationen über das verdächtige Anmeldeereignis:
  - **Uhrzeit**: Zeigt Datum und Uhrzeit der verdächtigen Anmeldung an.
  - **Anmeldetyp**: Zeigt an, ob es sich bei der Benutzeraktivität um eine Sitzungsanmeldung oder eine Kontoanmeldung handelt. Das Kontoanmeldeereignis wird ausgelöst, wenn die Authentifizierung eines Benutzers für sein Konto erfolgreich ist. Während das Sitzungsanmeldeereignis ausgelöst wird, wenn ein Benutzer seine Anmeldeinformationen eingibt und sich bei seiner App- oder Desktopsitzung anmeldet.
  - **Clienttyp**: Gibt den Typ der Citrix Workspace-App an, die auf dem Benutzergerät installiert ist. Abhängig vom Betriebssystem des Benutzergeräts kann der Clienttyp Android, iOS, Windows, Linux, Mac usw. sein.
  - **Betriebssystem**: Zeigt das Betriebssystem des Benutzergeräts an.
  - **Browser**: Zeigt den Webbrowser an, der für den Zugriff auf die Anwendung verwendet wird.
  - **Standort**: Gibt den Ort an, von dem aus sich der Benutzer angemeldet hat.
  - **Client-IP**: Zeigt die IP-Adresse des Benutzergeräts an.
  - **Gerät**: Zeigt den Gerätenamen des Benutzers an.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Welche Aktionen können Sie auf die Benutzer anwenden?

Sie können die folgenden Aktionen für das Benutzerkonto ausführen:

- **Zur Merkliste hinzufügen**. Wenn Sie einen Benutzer auf zukünftige potenzielle Bedrohungen überwachen möchten, können Sie ihn einer Watchlist hinzufügen.
- **Benachrichtigen Sie Administrator(en)**. Bei ungewöhnlichen oder verdächtigen Aktivitäten im Benutzerkonto wird eine E-Mail-Benachrichtigung an alle oder ausgewählte Administratoren gesendet.
- **Benutzer abmelden**. Wenn ein Benutzer von seinem Konto abgemeldet ist, kann er nicht über virtuelle Desktops auf die Ressource zugreifen.
- **Sitzungsaufzeichnung starten**. Wenn das Virtual Desktop-Konto des Benutzers ein ungewöhnliches Ereignis vorliegt, kann der Administrator mit der Aufzeichnung der Aktivitäten des Benutzers zukünftiger Anmeldesitzungen beginnen. Wenn der Benutzer jedoch Citrix Virtual Apps and Desktops 7.18 oder höher aktiviert ist, kann der Administrator die Aufzeichnung der aktuellen Anmeldesitzung des Benutzers dynamisch starten und beenden.

Weitere Informationen zu Aktionen und deren manueller Konfiguration finden Sie unter Richtlinien und Aktionen.

Um die Aktionen manuell auf den Benutzer anzuwenden, navigieren Sie zum Profil des Benutzers und wählen Sie den entsprechenden Risikoindikator aus. Wählen Sie im Menü **Aktion** eine Aktion aus und klicken Sie auf **Übernehmen**.

> **Hinweis**
>
> Unabhängig von der Datenquelle, die einen Risikoindikator auslöst, können Aktionen in Bezug auf andere Datenquellen angewendet werden.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Feedback zu Indikatoren für Benutzerrisiken geben

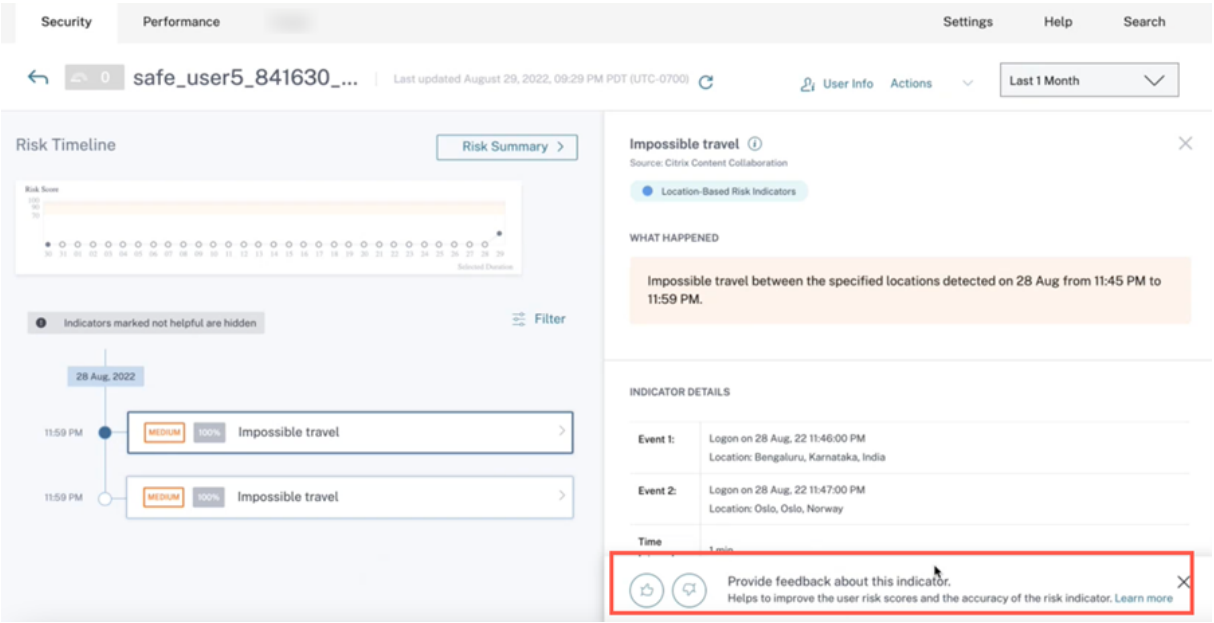
October 20, 2022

Risikoindikatoren wurden entwickelt, um potenziell verdächtige oder anomale Benutzeraktivitäten zu erkennen und zu melden und gleichzeitig die Risikobewertung des Benutzers automatisch zu erhöhen. In der Praxis entsprechen einige Vorkommen eines Risikoindikators zwar einer legitimen zugrunde liegenden Sicherheitsbedrohung, andere erweisen sich jedoch als harmlos.

Mit der Indikator-Feedback können Sie das Auftreten von Risikoindikatoren explizit kennzeichnen

- Ebenso hilfreich, wenn Sie glauben, dass ein echtes zugrunde liegendes Benutzerrisiko besteht
- Ist nicht hilfreich, wenn Sie festgestellt haben, dass keine Sicherheitsbedrohung vorliegt. In diesem Fall wird das Auftreten des Indikators standardmäßig in der Benutzerzeitleiste ausgeblendet, und die Risikobewertung des Benutzers wird automatisch angepasst, um das Auftreten dieses Indikators in nachfolgenden Berechnungen auszuschließen.

Darüber hinaus wird Ihr kollektives Feedback verwendet, um zukünftige Verbesserungen der Risikoindikatoralgorithmen voranzutreiben.

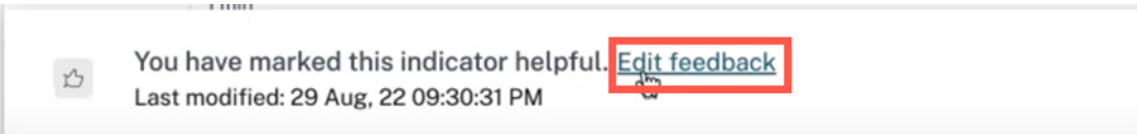


Ein Feedback-Banner (mit einem Daumen-Hoch- und Runter-Symbol) wird für jeden Standard-Risikoindikatoreintrag in der Benutzer-Timeline angezeigt.

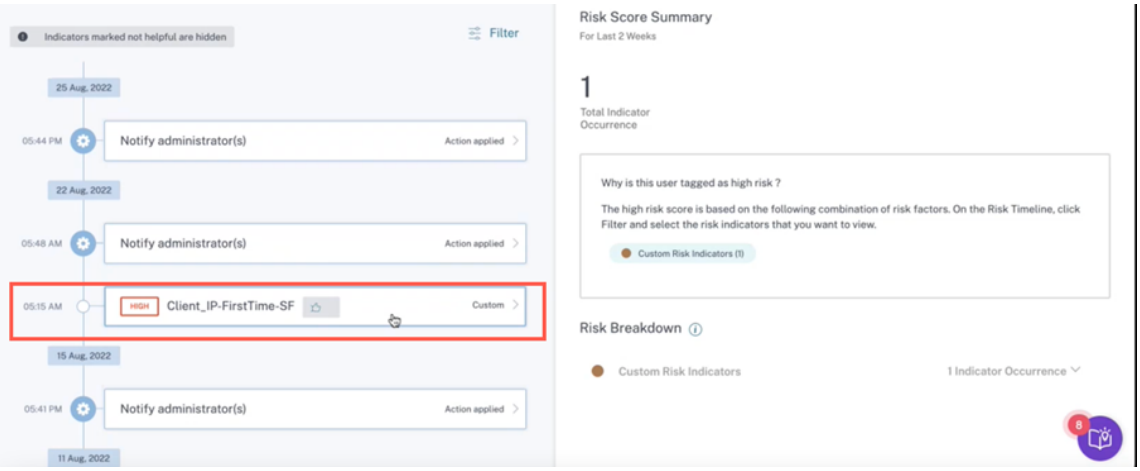
- **Daumen-hoch-Symbol** - Der Indikator ist hilfreich und hat riskante Aktivitäten korrekt identifiziert. Sie können auf das Symbol “Daumen hoch”klicken und zusätzliche Kommentare dazu abgeben, wie hilfreich der Indikator ist und welchen Nutzen er hat.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Sie können Ihr Feedback speichern und den Indikator als hilfreich markieren. Sie können Ihren Kommentar auch bearbeiten, indem Sie auf Feedback bearbeiten klicken. Das Feedback-Banner zeigt die Zeitleiste des zuletzt eingereichten Feedbacks an.



Wenn ein Risikoindikator als hilfreich markiert ist, wird dieses Feedback im entsprechenden Benutzer-Timeline-Eintrag angezeigt und an Citrix Analytics gemeldet. Die Bewertung des Benutzerrisikos wird nicht beeinträchtigt.

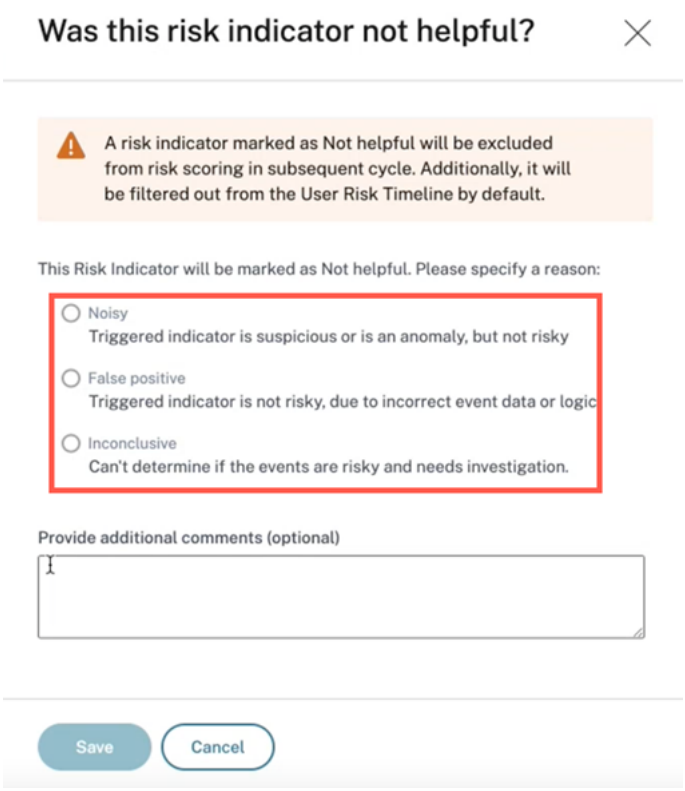


- Symbol **Daumen runter** - Anzeige ist nicht hilfreich oder wurde falsch ausgelöst. Sie können den Indikator als nicht hilfreich markieren und ihn als **Verrauscht**, **Falsch positiv** oder **Nicht eindeutig** einstufen. Dieses Auftreten des Risikoindikators wird von allen nachfolgenden Aktualisierungen der Risikobewertung des Benutzers ausgeschlossen. Sie können bei Bedarf auch zusätzliche Kommentare abgeben.

  - **Verrauscht** —Der ausgelöste Indikator ist verdächtig oder eine Anomalie, aber nicht riskant.
  - **Falsch positiv** —Der ausgelöste Indikator ist aufgrund falscher Ereignisdaten oder Logik nicht riskant.
  - **Nicht eindeutig** —Es kann nicht festgestellt werden, ob die Ereignisse riskant sind und untersucht werden müssen.

    > **Hinweis**
    >
    > Es dauert bis zu 15 Minuten, um den Risiko-Score neu zu kalibrieren.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



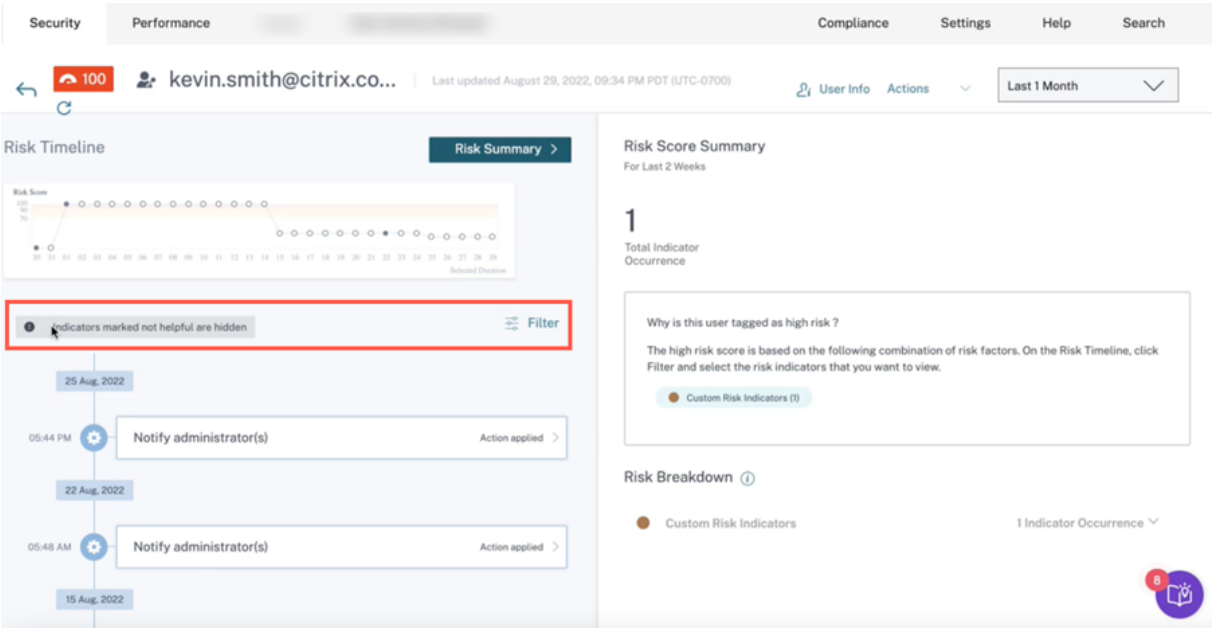
Sie können die folgenden Ergebnisse anzeigen, wenn ein Indikator als nicht hilfreich markiert ist:

- Dieser spezielle Indikator ist in der Zeitleiste verborgen.
- Die Risikobewertung wird neu kalibriert, da dieses Indikatorereignis in nachfolgenden Aktualisierungen aus der Berechnung der Risikobewertung ausgeschlossen wurde.
- Alle zusätzlichen Informationen, die als Textfeedback gegeben werden, werden zur späteren Bezugnahme beibehalten.

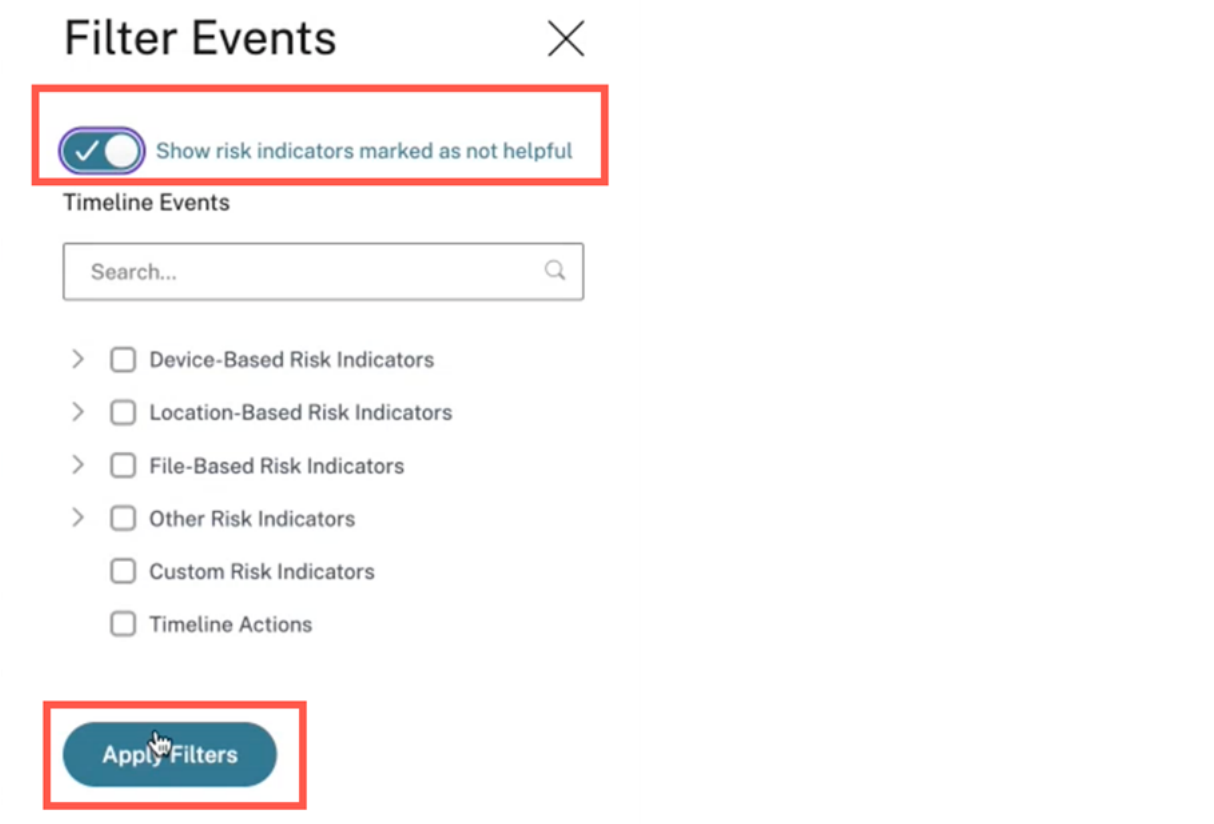
Filter anzeigen

Indikatoren, die als nicht hilfreich markiert sind, werden standardmäßig ausgeblendet.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

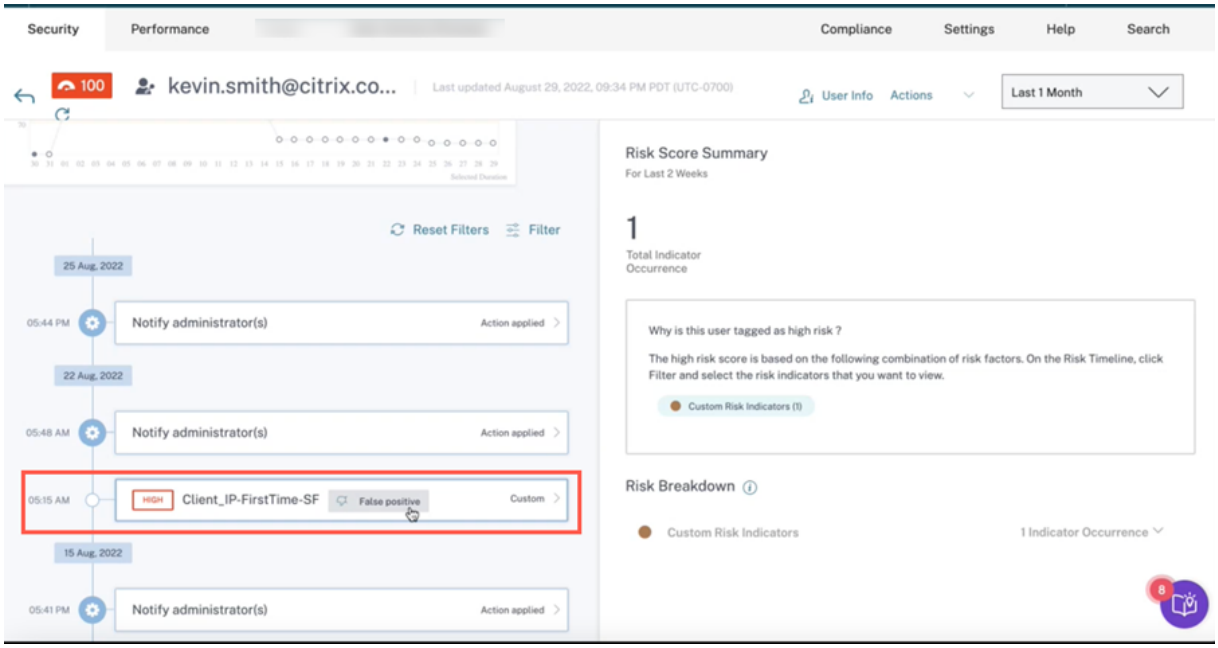


Um die ausgeblendeten Indikatoren anzuzeigen, klicken Sie auf **Filter**. Aktivieren Sie im daraufhin angezeigten Fenster **Ereignisse filtern** die Option **Als nicht hilfreich markierte Risikoindikatoren anzeigen**.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Sie können die Indikatoren anhand von Kategorien durchsuchen. Um beispielsweise die standortbasierten versteckten Risikoindikatoren anzuzeigen, wählen Sie die Kategorie aus und klicken Sie auf **Filter anwenden**. Sie können alle standortbezogenen Indikatoren anzeigen, die für die Feedback-Details nicht hilfreich sind.



Als Administrator können Sie bei Bedarf auch die folgenden Aktionen ausführen:

- Feedback ändern
- Überprüfen Sie vorheriges Feedback und die zugehörigen Metadaten
- Überprüfen Sie das Feedback anderer Administratoren und die zugehörigen Metadaten

> **Hinweis**
>
> - Sie können das Feedback pro Benutzerebene und nicht auf Mandantenebene bereitstellen. Das Feedback für einen Risikoindikator gilt nicht für alle Fälle dieses bestimmten Risikoindikators.
> - Das Feedback für einen Benutzer gilt nicht für andere Benutzer.

Microsoft Graph Sicherheitsrisikoindikatoren

September 24, 2021

Microsoft Graph Security empfängt Daten von **Azure AD Identity Protection** oder **Microsoft Defender für Endpunkt-Sicherheitsanbieter** und sendet die Informationen an Citrix Analytics.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Azure AD Identity Protection löst die folgenden Risikoindikatoren aus und sendet die Informationen an Microsoft Graph Security:

- Anonyme IP-Adresse
- Unmögliche Reisen zu atypischen Orten
- Benutzer mit durchgesickerten Anmeldeinformationen
- Anmeldungen von infizierten Geräten
- Melden Sie sich von IP-Adressen mit verdächtigen Aktivitäten an
- Melden Sie sich von unbekannten Orten aus an

Informationen zu Defender for Endpoint finden Sie unter Microsoft Defender for Endpoint.

Der mit den Risikoindikatoren verbundene Risikofaktor sind die IP-basierten Risikoindikatoren. Weitere Informationen zu den Risikofaktoren finden Sie unter Citrix Benutzerrisikoindikatoren.

So analysieren Sie Microsoft Graph Sicherheitsrisikoindikatoren

Stellen Sie sich eine Benutzerin Maria Brown vor, die eines der zuvor erwähnten riskanten Verhaltensweisen aufweist. Microsoft erkennt den Vorfall und generiert eine Warnung. Citrix Analytics ruft diese Warnung ab und weist Maria Brown einen aktualisierten Risiko-Score zu. Außerdem wird der Risikozeitraum von Maria Brown um den entsprechenden Risikoindikator erweitert.

Um den Eintrag für den Risikoindikator Microsoft Graph Security für einen Benutzer anzuzeigen, navigieren Sie zu **Sicherheit** > **Benutzer**und wählen Sie den Benutzer aus.

Aus Marias Zeitleiste können Sie den neuesten Risikoindikatoreintrag aus der Risikozeitleiste auswählen. Das entsprechende detaillierte Informationsfeld wird im rechten Bereich angezeigt. Der Abschnitt **WAS PASSIERT IST**, bietet eine kurze Zusammenfassung des Risikoindikators.

So erhalten Sie weitere Informationen über die Risikoindikatoren

Weitere Informationen finden Sie unter Azure Active Directory-Risikoereignisse.

Welche Aktionen können Sie auf den Benutzer anwenden

Derzeit ist die Möglichkeit, über die Microsoft Graph Security-Datenquelle geeignete Maßnahmen für das Konto des Benutzers zu ergreifen, nicht verfügbar.

Informationen zum Onboarding von Microsoft Graph Security finden Sie unter Microsoft Graph-Sicherheit.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Benutzerdefinierte Risikoindikatoren

December 12, 2023

Es gibt zwei Arten von Risikoindikatoren, die Sie in Citrix Analytics for Security sehen:

- **Ausfallrisikoindikatoren**: Diese Risikoindikatoren basieren auf dem Algorithmus für maschinelles Lernen. Weitere Informationen finden Sie unter Citrix Benutzerrisikoindikatoren.
- **Benutzerdefinierte Risikoindikatoren**: Diese Risikoindikatoren werden von den Administratoren manuell erstellt.

Wenn Sie einen benutzerdefinierten Risikoindikator erstellen, können Sie die Auslösebedingungen und die Parameter basierend auf Ihren Anwendungsfällen definieren. Wenn die Benutzerereignisse Ihren definierten Kriterien entsprechen, löst Citrix Analytics den benutzerdefinierten Risikoindikator aus und zeigt ihn auf der Risikozeitleiste des Benutzers an.

Erstellen Sie benutzerdefinierte Risikoindikatoren für die folgenden Datenquellen:

- Citrix Gateway
- Citrix Secure Private Access
- Citrix Virtual Apps and Desktops on-premises
- Citrix DaaS (früher Citrix Virtual Apps and Desktops Service)
- Citrix Secure Browser

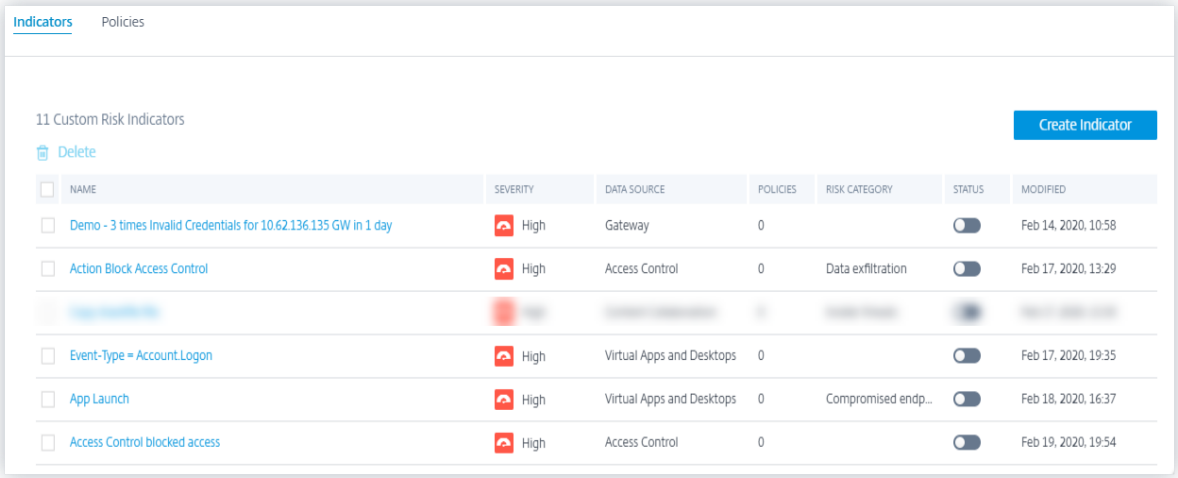
Vorkonfigurierte individuelle Risikoindikatoren

Citrix bietet auch einige benutzerdefinierte Risikoindikatoren mit vorkonfigurierten Bedingungen, mit denen Sie die Sicherheit Ihrer Citrix Infrastruktur überwachen können. Sie können die vorkonfigurierten Bedingungen basierend auf Ihren Anwendungsfällen ändern. Weitere Informationen finden Sie unter Vorkonfigurierte benutzerdefinierte Risikoindikatoren.

Seite Benutzerdefinierte Risikoindikatoren

Die Seite **Benutzerdefinierte Risikoindikatoren** bietet Einblicke in alle benutzerdefinierten Risikoindikatoren, die für einen Benutzer generiert wurden, den Schweregrad, die Datenquelle, die Anzahl der Richtlinien, die Risikokategorie, den Status sowie das Datum und die Uhrzeit der letzten Änderung des Indikators. Um einen benutzerdefinierten Risikoindikator zu erstellen, siehe Erstellen eines benutzerdefinierten Risikoindikators.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Wenn Sie den Risikoindikator auswählen, werden Sie zur Seite **Risikoindikator ändern** weitergeleitet. Weitere Informationen finden Sie unter Ändern eines benutzerdefinierten Risikoindikators.

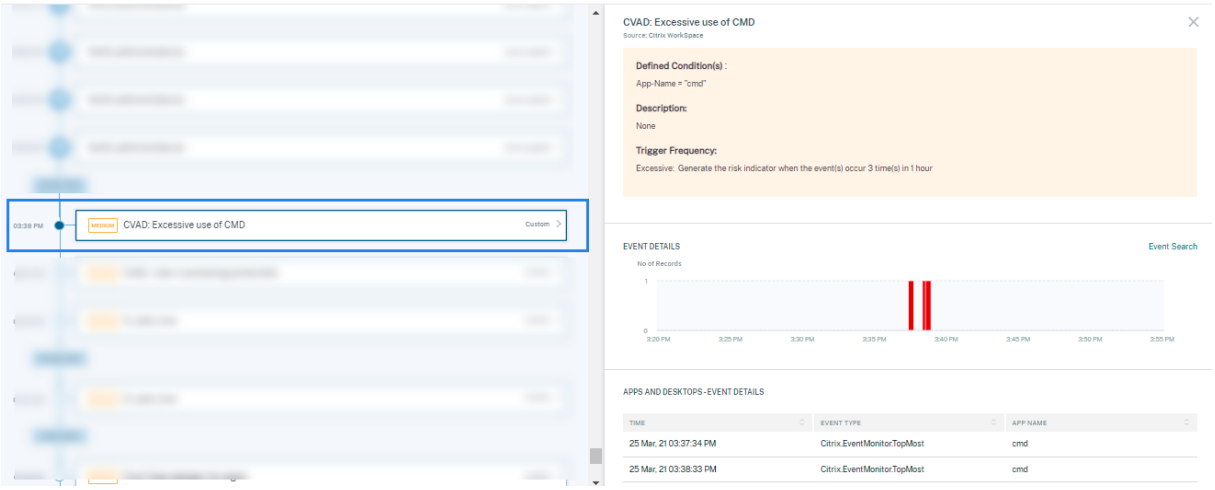
Analyse eines benutzerdefinierten Risikoindikators

Betrachten Sie einen Benutzer, dessen Aktion einen von Ihnen definierten benutzerdefinierten Risikoindikator ausgelöst hat. Citrix Analytics zeigt den benutzerdefinierten Risikoindikator auf der Risikozeitleiste des Benutzers an.

Wenn Sie den benutzerdefinierten Risikoindikator auf der Risikozeitleiste des Benutzers auswählen, werden im rechten Bereich die folgenden Informationen angezeigt:

- **Definierte Bedingung (en)**: Zeigt eine Zusammenfassung der Bedingungen an, die Sie beim Erstellen eines benutzerdefinierten Risikoindikators definieren.
- **Beschreibung**: Bietet eine Zusammenfassung der Beschreibung, die Sie beim Erstellen des benutzerdefinierten Risikoindikators angeben. Wenn beim Erstellen des benutzerdefinierten Risikoindikators keine Beschreibung angegeben wird, spiegelt dieser Abschnitt **Keine**wider.
- **Triggerfrequenz**: Zeigt die Option an, die Sie beim Erstellen des benutzerdefinierten Risikoindikators im Abschnitt **Erweiterte Optionen**auswählen.
- **Ereignisdetails**: Zeigt die Zeitleiste und die Details der Benutzerereignisse an, die den benutzerdefinierten Risikoindikator ausgelöst haben. Sie können auf **Ereignissuche** klicken, um die Benutzerereignisse auf der Self-Service-Suchseite anzuzeigen. Auf der Self-Service-Suchseite werden die mit dem Benutzer verbundenen Ereignisse und der benutzerdefinierte Risikoindikator angezeigt. Die Suchanfrage zeigt die Bedingungen an, die für den benutzerdefinierten Risikoindikator definiert sind.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



> **Hinweis**
>
> Benutzerdefinierte Risikoindikatoren werden mit einem Etikett auf der Zeitleiste des Benutzerrisikos dargestellt.

Aktionen, die Sie auf den Benutzer anwenden können

Wenn ein benutzerdefinierter Risikoindikator für einen Benutzer ausgelöst wird, können Sie eine Aktion manuell anwenden oder eine Richtlinie erstellen, um eine Aktion automatisch anzuwenden. Weitere Informationen finden Sie unter Richtlinien und Aktionen.

Benutzerdefinierte Vorlagen für Risikoindikatoren

Sie können einen benutzerdefinierten Risikoindikator erstellen, indem Sie eine der vordefinierten Vorlagen verwenden, oder ohne Vorlage fortfahren.

Die Vorlagen dienen als Ausgangspunkt für die Erstellung eines benutzerdefinierten Risikoindikators. Es hilft Ihnen, einen benutzerdefinierten Risikoindikator zu erstellen, indem vordefinierte Abfragen und Parameter bereitgestellt werden, die Sie basierend auf Ihren Anwendungsfällen auswählen können.

Sie können eine Vorlage unverändert verwenden oder sie an Ihre Anforderungen anpassen. Mithilfe der Vorlagen können Administratoren ohne zusätzliche Schulung Risikoindikatoren für Interesse erstellen.

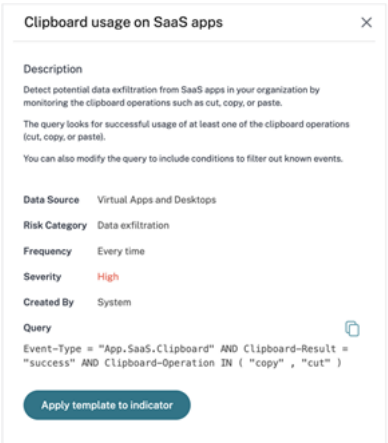
Eine Vorlage besteht aus den folgenden Informationen:

- **Beschreibung**: Zeigt den Zweck der in der Vorlage definierten Abfrage an.
- **Datenquelle**: Gibt die Datenquelle an, für die die Vorlage gilt.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Risikokategorie**: Zeigt die Risikokategorie an, die mit den von der Abfrage durchsuchten Ereignissen verknüpft Es gibt vier Kategorien von riskanten Ereignissen: Datenexfiltration, Insider-Bedrohungen, kompromittierte Benutzer und Endpunkte für kompromittierte Daten. Weitere Informationen finden Sie unter Risikokategorien.
- **Frequenz**: Gibt die Häufigkeit an, mit der die Abfrage ausgelöst wird.
- **Schweregrad**: Zeigt den Schweregrad des mit dem Ereignis verbundenen Risikos an. Das Risiko kann hoch, mittel oder niedrig sein.
- **Erstellt von**: Zeigt den Ersteller der Vorlage an. Die Vorlagen sind immer vom System definiert.
- **Abfrage**: Zeigt die in der Vorlage definierten Bedingungen an. Die Abfrage ruft die Benutzerereignisse ab, die die Bedingungen erfüllen.

Das folgende Bild zeigt die Vorlage für die Verwendung von Anwendungsfall-Zwischenablage in SaaS-Apps.

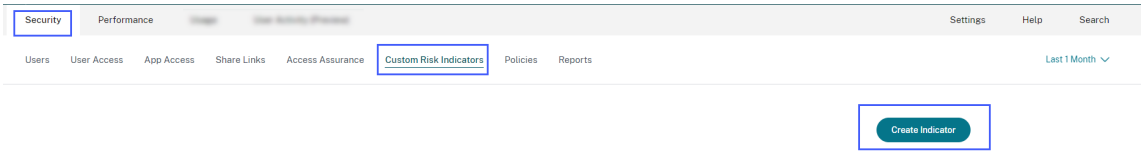


Wenn Sie keine Vorlage für Ihren Anwendungsfall finden oder eine eigene Abfrage definieren möchten, können Sie ohne Vorlage fortfahren.

Erstellen eines benutzerdefinierten Risikoindikators

So erstellen Sie einen benutzerdefinierten Risikoindikator:

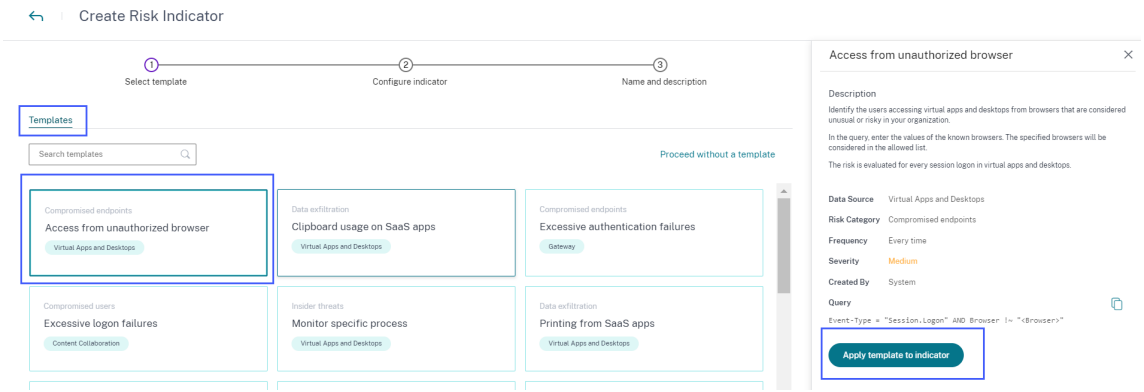
1. Navigieren Sie zu **Sicherheit > Benutzerdefinierte Risikoindikatoren > Indikator erstellen**.



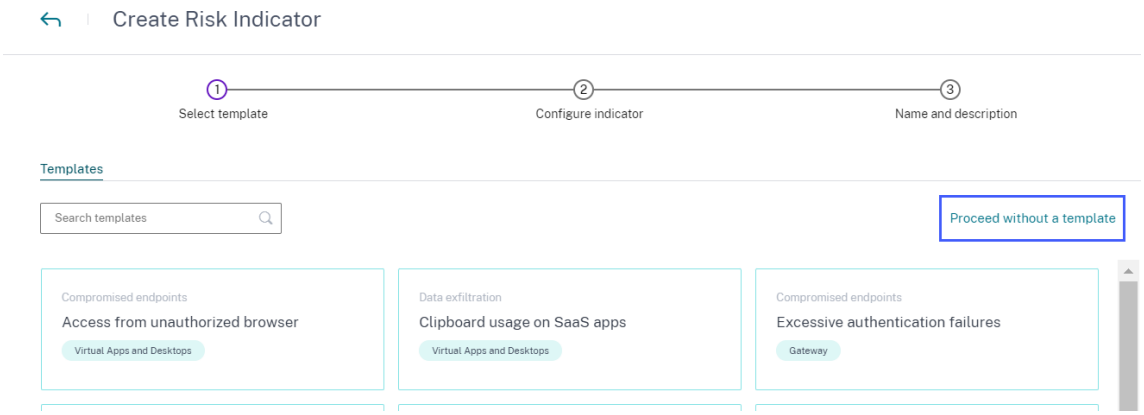
2. Wählen Sie eine Vorlage aus, um den Anwendungsfall anzuzeigen. Wenn es Ihre Anforderung erfüllt, wählen Sie **Vorlage auf Indikator anwenden**aus.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Hinweis**
>
> Sie können auch die vordefinierten Bedingungen und die Parameter einer Vorlage ändern.



3. Wenn Sie keine gewünschte Vorlage finden oder eine eigene Bedingung erstellen möchten, wählen Sie **Ohne Vorlage fortfahren**.



4. Befolgen Sie die Anweisungen auf dem Bildschirm, um einen Indikator zu erstellen.

> **Hinweise**
>
> - Sie können benutzerdefinierte Risikoindikatoren bis zu einer Höchstgrenze von 50 erstellen. Wenn Sie diese Höchstgrenze erreichen, müssen Sie alle vorhandenen benutzerdefinierten Risikoindikatoren löschen oder bearbeiten, um einen benutzerdefinierten Risikoindikator zu erstellen.
> - Wenn ein benutzerdefinierter Risikoindikator ausgelöst wird, wird er sofort in der Benutzerzeitleiste angezeigt. Die Risikoübersicht und die Risikobewertung des Benutzers werden jedoch nach einigen Minuten (ca. 15-20 Minuten) aktualisiert.

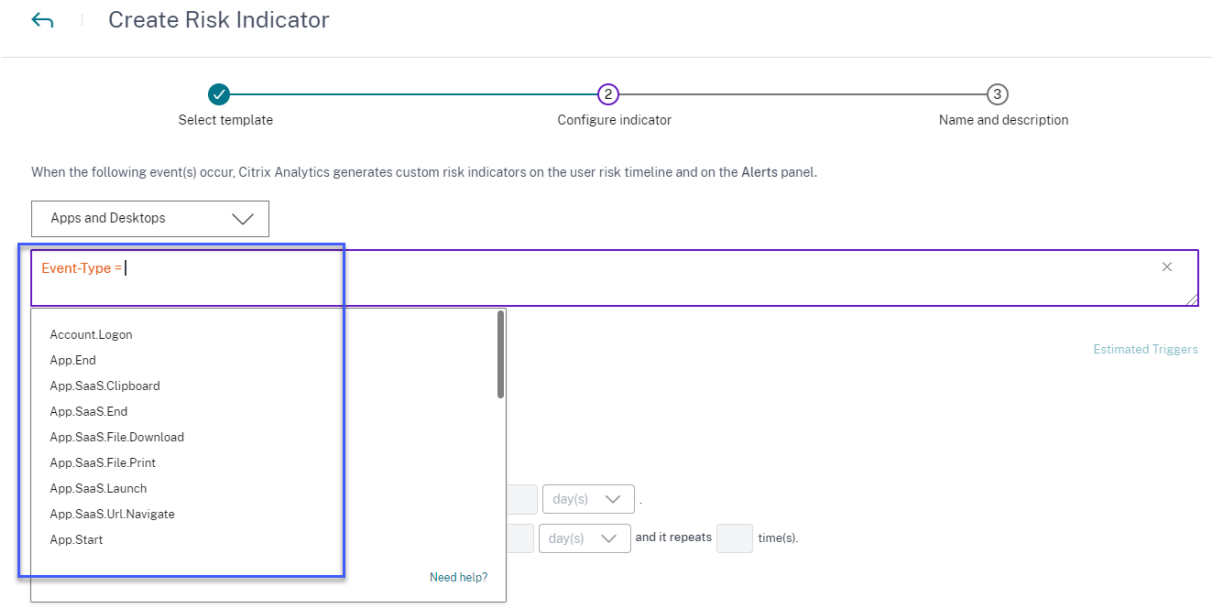
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Definieren einer Bedingung für einen benutzerdefinierten Risikoindikator

Verwenden Sie das Abfragefeld, um Ihre Bedingungen für den benutzerdefinierten Risikoindikator zu definieren. Abhängig von der ausgewählten Datenquelle erhalten Sie die entsprechenden Dimensionen und die gültigen Operatoren zum Definieren Ihrer Bedingungen.

Wenn Sie bestimmte Dimensionen wie `Event-Type` und `Clipboard-Operation` zusammen mit einem gültigen Operator auswählen, werden die Werte der Dimension automatisch angezeigt. Sie können einen Wert aus den vorgeschlagenen Optionen auswählen oder je nach Ihren Anforderungen einen neuen Wert eingeben.

Die folgende Abbildung zeigt die vorgeschlagenen Werte der Bemaßung `Event-Type`.



Wenn Sie eine Vorlage verwenden, ist die Bedingung vordefiniert. Sie können die vordefinierte Bedingung jedoch basierend auf Ihrem Anwendungsfall anhängen oder ändern.

Unterhalb des Abfragefeldes sehen Sie den Link **Geschätzte Auslöser** . Klicken Sie auf den Link, um die ungefähren Instanzen des benutzerdefinierten Risikoindikators vorherzusagen, die für die definierten Bedingungen ausgelöst würden. Diese Instanzen werden basierend auf den historischen Daten berechnet, die Citrix Analytics verwaltet und die definierten Bedingungen erfüllt.

Stellen Sie sicher, dass Sie auf **Geschätzte Auslöser** klicken, um die Anzahl der benutzerdefinierten Risikoindikatoren für die zuletzt definierte Bedingung vorherzusagen.

Verwenden der erweiterten Optionen

Wählen Sie im Abschnitt **Erweiterte Optionen** die Häufigkeit des Ereignisses aus, um den benutzerdefinierten Risikoindikator auszulösen. Wenn Sie keine Option auswählen, berücksichtigt

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Citrix Analytics **Jedes Mal: Generieren Sie den Risikoindikator jedes Mal, wenn die Ereignisse auftreten**, als Standardoption und generiert den benutzerdefinierten Risikoindikator. Sie können eine der folgenden Optionen auswählen:

- **Jedes Mal**: Der Risikoindikator wird immer dann ausgelöst, wenn die Ereignisse die definierten Bedingungen erfüllen.
- **Erstes Mal**: Der Risikoindikator wird ausgelöst, wenn die Ereignisse zum ersten Mal die definierten Bedingungen erfüllen.
  - **Erstes Mal für eine neue**: Aktivieren Sie diese Option, um Ereignisse zu erkennen, die zum ersten Mal von einer neuen Entität empfangen wurden. Einige Beispiele für die Entitäten sind Client-IP, Land, Stadt und Geräte-ID. Sie können nur eine Entität basierend auf der Datenquelle auswählen. Mit dieser Option können Sie einen Risikoindikator erstellen, ohne einen expliziten Wert für die Entitäten anzugeben. Wenn Sie beispielsweise die Entität als "Stadt"auswählen, müssen Sie den Namen der Stadt nicht angeben. Der Risikoindikator wird ausgelöst, wenn Ereignisse zum ersten Mal aus einer neuen Stadt eingehen.

    Die folgende Tabelle listet die Entitäten auf, die jeder Datenquelle entsprechen, und beschreibt die Triggerbedingungen.

Datenquelle	Entität	Trigger Zustand
Secure Private Access	Ort	Wenn sich ein Benutzer zum ersten Mal von einer neuen Stadt aus anmeldet.
	Client-IP	Wenn sich ein Benutzer zum ersten Mal von einer neuen IP-Adresse aus anmeldet.
	Land	Wenn sich ein Benutzer zum ersten Mal aus einem neuen Land anmeldet.
Apps und Desktops	App-Name	Wenn ein Benutzer zum ersten Mal eine neue virtuelle Anwendung oder eine SaaS-Anwendung öffnet.
	App-URL	Wenn ein Benutzer zum ersten Mal eine neue App-URL in einem Browser in seinem virtuellen Desktop eingibt.

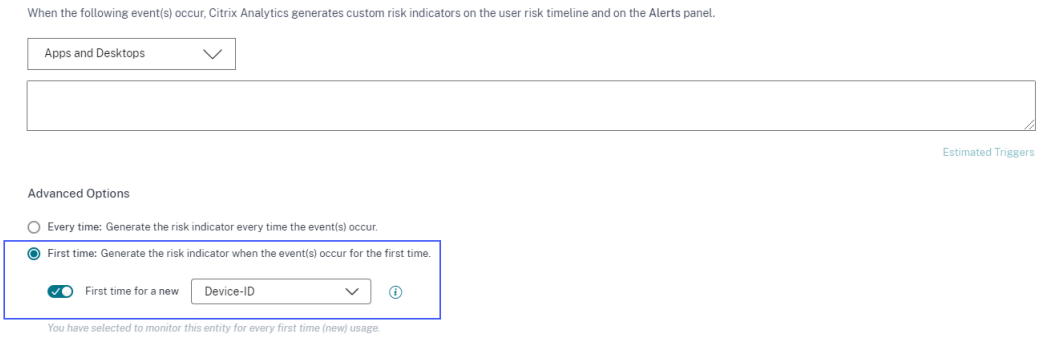
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Datenquelle	Entität	Trigger Zustand
	Ort	Wenn ein Benutzer zum ersten Mal Apps oder Desktops aus einer neuen Stadt startet.
	Client-IP	Wenn sich ein Benutzer zum ersten Mal von einer neuen IP-Adresse aus anmeldet.
	Land	Wenn ein Benutzer zum ersten Mal Apps oder Desktops aus einem neuen Land startet.
	Geräte-ID	Wenn ein Benutzer virtuelle Apps oder virtuelle Desktops zum ersten Mal von einem neuen Gerät wie einem Handy, Laptop oder Desktop-Computer aus startet.
	Download-Gerätetyp	Wenn ein Benutzer zum ersten Mal ein neues Speichermedium wie ein USB-Laufwerk verwendet.
	Druck-Dateiformat	Format der gedruckten Datei.
	Druck-Datei-Größe	Größe der gedruckten Datei in Byte.
	Druck-Dateiname	Name der gedruckten Datei.
	Drucker-Name	Name des verwendeten Druckers.
	Total-Copies-Printed	Gesamtzahl der vom Benutzer gedruckten Exemplare.
	Total-Pages-Printed	Gesamtzahl der vom Benutzer gedruckten Dokumentseiten.
Gateway	Client-IP	Wenn sich ein Benutzer zum ersten Mal von einer neuen IP-Adresse aus anmeldet.
Secure Browser	Benutzername	Der Name des Benutzers, der das Ereignis initiiert hat.
	Access-Allowed	Ob dem Benutzer der Zugriff auf den Hostdienst gewährt oder verweigert wird.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Datenquelle	Entität	Trigger Zustand
	Client-IP	Die IP-Adresse des Benutzergeräts.
	Host-Name-Accessed	Der Host-Service, auf den der Benutzer über das Netzwerk zugegriffen hat.
	Session-ID	Die eindeutige Nummer, die der Benutzersitzung zugewiesen wurde.

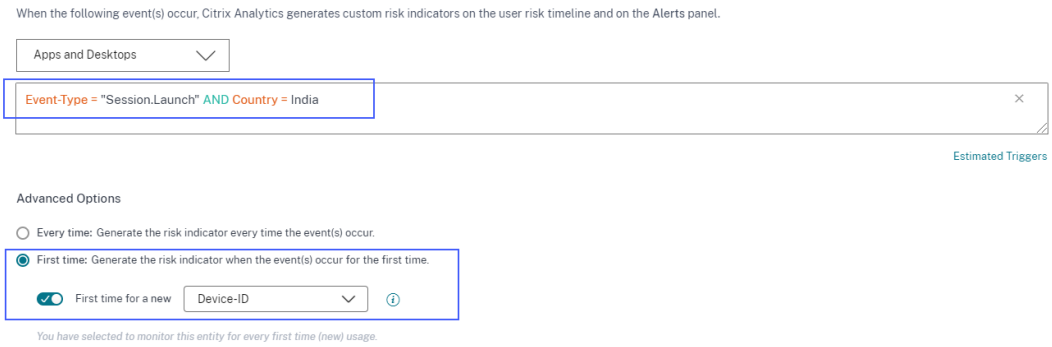
Das folgende Beispiel zeigt einen benutzerdefinierten Risikoindikator, der für die Datenquelle Apps und Desktops erstellt wurde. Der Risikoindikator wird ausgelöst, wenn ein Benutzer zum ersten Mal einen virtuellen Desktop oder eine virtuelle App von einem neuen Gerät aus startet.



Sie können auch eine Bedingung zusammen mit dem **Ersten Mal für eine neue** Option hinzufügen. In diesem Fall wird der Risikoindikator ausgelöst, wenn er die Ereignisse der neuen Entität zum ersten Mal erkennt und wenn die Ereignisse die definierte Bedingung erfüllen.

Das folgende Beispiel zeigt eine Bedingung, die für den benutzerdefinierten Risikoindikator und die Option **Erstes Mal für eine neue Device-ID** definiert wurde. Der Risikoindikator wird ausgelöst, wenn ein in Indien ansässiger Benutzer zum ersten Mal eine virtuelle Desktop-Sitzung von einem neuen Gerät aus startet.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



- **Übermäßig**: Der Risikoindikator wird ausgelöst, nachdem die folgenden Bedingungen erfüllt sind:
  - Ereignisse erfüllen die definierten Bedingungen.
  - Ereignisse treten während des angegebenen Zeitraums für eine bestimmte Anzahl von Malen auf.
- **Häufig**: Der Risikoindikator wird ausgelöst, nachdem die folgenden Bedingungen erfüllt sind:
  - Die Ereignisse erfüllen die definierten Bedingungen.
  - Die Ereignisse treten während des angegebenen Zeitraums für die angegebene Anzahl von Malen auf.
  - Das Ereignismuster wiederholt sich für die angegebene Anzahl von Malen.

Auswahl der Risikokategorie

Wählen Sie die Risikokategorie für Ihren benutzerdefinierten Risikoindikator aus.

Risikoindikatoren werden auf der Grundlage der Art der Risikoexposition des benutzerdefinierten Risikoindikators gruppiert. Unterstützung bei der Auswahl der Risikokategorie finden Sie unter Risikokategorien.

Auswahl des Schweregrads

Der Schweregrad gibt an, wie schwerwiegend ein riskantes Ereignis ist, das durch den Risikoindikator erkannt wird. Wenn Sie einen benutzerdefinierten Risikoindikator erstellen, wählen Sie einen Schweregrad —hoch, mittel oder niedrig.

Wenn Sie eine Vorlage anwenden, ist die Option Schweregrad vorausgewählt. Sie können diese Vorauswahl je nach Anwendungsfall ändern.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Unterstützte Operatoren für die Definition einer Bedingung

Sie können die folgenden Operatoren verwenden, während Sie eine Bedingung definieren.

Betreiber	Beschreibung	Beispiel	Ausgabe
	Weisen Sie der Suchanfrage einen Wert zu.	Benutzername: John	Zeigt Ereignisse für den Benutzer John an.
=	Weisen Sie der Suchanfrage einen Wert zu.	Benutzername = John	Zeigt Ereignisse für den Benutzer John an.
~	Suche nach ähnlichen Werten.	Benutzername ~ test	Zeigt Ereignisse mit ähnlichen Benutzernamen an.
””	Schließen Sie Werte getrennt durch Leerzeichen ein.	Benutzername = “John Smith”	Zeigt Ereignisse für den Benutzer John Smith an.
<, >	Suchen Sie nach einem relationalen Wert.	Datenvolumen > 100	Zeigt Ereignisse an, bei denen das Datenvolumen größer als 100 GB ist.
UND	Suchwerte, bei denen beide Bedingungen zutreffen.	Benutzername: John AND Datenvolumen > 100	Zeigt Ereignisse von Benutzer John an, bei denen das Datenvolumen größer als 100 GB ist.
*	Sucht Werte, die dem Zeichen Null oder öfter entsprechen.	Benutzername = John*	Zeigt Ereignisse für alle Benutzernamen an, die mit John beginnen.
		Benutzername = *John*	Zeigt Ereignisse für alle Benutzernamen an, die John enthalten.
		Benutzername = *Smith	Zeigt Ereignisse für alle Benutzernamen an, die mit Smith enden.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Betreiber	Beschreibung	Beispiel	Ausgabe
!~	Überprüft die Benutzerereignisse auf das von Ihnen angegebene übereinstimmende Muster. Dieser NOT LIKE Operator gibt die Ereignisse zurück, die das übereinstimmende Muster nirgendwo in der Ereigniszeichenfolge enthalten.	Benutzername! ~ John	Zeigt Ereignisse für die Benutzer an, außer John, John Smith oder solche Benutzer, die den übereinstimmenden Namen “John” enthalten.
!=	Überprüft die Benutzerereignisse auf die genaue Zeichenfolge, die Sie angeben. Dieser NOT EQUAL-Operator gibt die Ereignisse zurück, die die genaue Zeichenfolge nicht irgendwo in der Ereigniszeichenfolge enthalten.	Country != USA	Zeigt Ereignisse für Länder mit Ausnahme der USA an.
IN	Weisen Sie einer Dimension mehrere Werte zu, um die Ereignisse abzurufen, die sich auf einen oder mehrere Werte beziehen.	Benutzername IN (John, Kevin)	Finden aller Ereignisse im Zusammenhang mit John oder Kevin.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Betreiber	Beschreibung	Beispiel	Ausgabe
NOT IN	Weisen Sie einer Dimension mehrere Werte zu und suchen Sie die Ereignisse, die die angegebenen Werte nicht enthalten.	Benutzername NICHT IN (John, Kevin)	Finde die Events für alle Benutzer außer John und Kevin.
IST LEER	Sucht nach Nullwert oder leerem Wert für eine Dimension. Dieser Operator funktioniert nur für Dimensionen vom Typ Zeichenfolge wie `App-NameBrowser`, und `Country`. Es funktioniert nicht für Dimensionen vom Typ Nicht-Zeichenfolge (Zahl) wie `Upload-File-SizeDownload-File-Size`, und `Client-IP`.	Land IST LEER	Finden Sie Ereignisse, bei denen der Ländername nicht verfügbar oder leer ist (nicht angegeben).

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Betreiber	Beschreibung	Beispiel	Ausgabe
IST NICHT LEER	Überprüft, ob kein Nullwert oder ein bestimmter Wert für eine Dimension vorhanden ist. Dieser Operator funktioniert nur für Dimensionen vom Typ Zeichenfolge wie `App-NameBrowser`, und `Country`. Es funktioniert nicht für Dimensionen vom Typ Nicht-Zeichenfolge (Zahl) wie `Upload-File-SizeDownload-File-Size`, und `Client-IP`.	Land IST NICHT LEER	Finden von Ereignissen, bei denen der Ländername verfügbar oder angegeben ist.
ODER	Sucht nach Werten, bei denen eine oder beide Bedingungen zutreffen.	(User-Name = `John*` OR User-Name = `*Smith`) AND Event-Type = “Session.Logon”	Zeigt `Session.Logon`-Ereignisse für alle Benutzernamen an, die mit John beginnen oder mit Smith enden.

> **Hinweis**
>
> Verwenden Sie für den Operator NOT **EQUAL**, während Sie die Werte für die Dimensionen in Ihrem Zustand eingeben, die genauen Werte, die auf der Self-Service-Suchseite für eine Datenquelle verfügbar sind. Bei den Dimensionswerten wird die Groß-/Kleinschreibung

Ändern eines benutzerdefinierten Risikoindikators

1. Navigieren Sie zu **Sicherheit > Benutzerdefinierte Risikoindikatoren**.
2. Wählen Sie den benutzerdefinierten Risikoindikator aus, den Sie ändern möchten.
3. Ändern Sie auf der Seite **Indikator ändern** die Informationen nach Bedarf.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

4. Klicken Sie auf **Änderungen speichern**.

> **Hinweis**
>
> Wenn Sie die Attribute wie Zustand, Risikokategorie, Schweregrad und Name eines vorhandenen benutzerdefinierten Risikoindikators auf der Benutzerzeitleiste ändern, können Sie weiterhin die vorherigen Vorkommen des benutzerdefinierten Risikoindikators (mit den alten Attributen) anzeigen, die für den Benutzer ausgelöst wurden.
>
> Beispielsweise haben Sie einen benutzerdefinierten Risikoindikator mit der Bedingung *Country != India*. Dieser benutzerdefinierte Risikoindikator wird also ausgelöst, wenn sich ein Benutzer von außerhalb des Landes Indien anmeldet. Jetzt ändern Sie den Zustand des benutzerdefinierten Risikoindikators in *Country != ‘‘United States’’*. In diesem Fall können Sie weiterhin die vorherigen Vorkommen des benutzerdefinierten Risikoindikators mit der Bedingung *Country != India* über die Benutzerzeitpläne, die den Risikoindikator ausgelöst haben.

Löschen eines benutzerdefinierten Risikoindikators

1. Navigieren Sie zu **Sicherheit > Benutzerdefinierte Risikoindikatoren**.
2. Wählen Sie den benutzerdefinierten Risikoindikator aus, den Sie löschen möchten.
3. Klicken Sie auf **Löschen**.
4. Bestätigen Sie im Dialog Ihre Anfrage, den benutzerdefinierten Risikoindikator zu löschen.

> **Hinweis**
>
> Wenn Sie einen benutzerdefinierten Risikoindikator löschen, können Sie auf der Benutzerzeitleiste weiterhin die vorherigen Vorkommen des benutzerdefinierten Risikoindikators anzeigen, die für den Benutzer ausgelöst wurden.
>
> Beispielsweise löschen Sie einen vorhandenen benutzerdefinierten Risikoindikator mit der Bedingung *Land! = Indien*. In diesem Fall können Sie weiterhin die vorherigen Vorkommen des benutzerdefinierten Risikoindikators mit der Bedingung *Country != India* über die Benutzerzeitpläne, die den Risikoindikator ausgelöst haben.

Kontinuierliche Risikobewertung

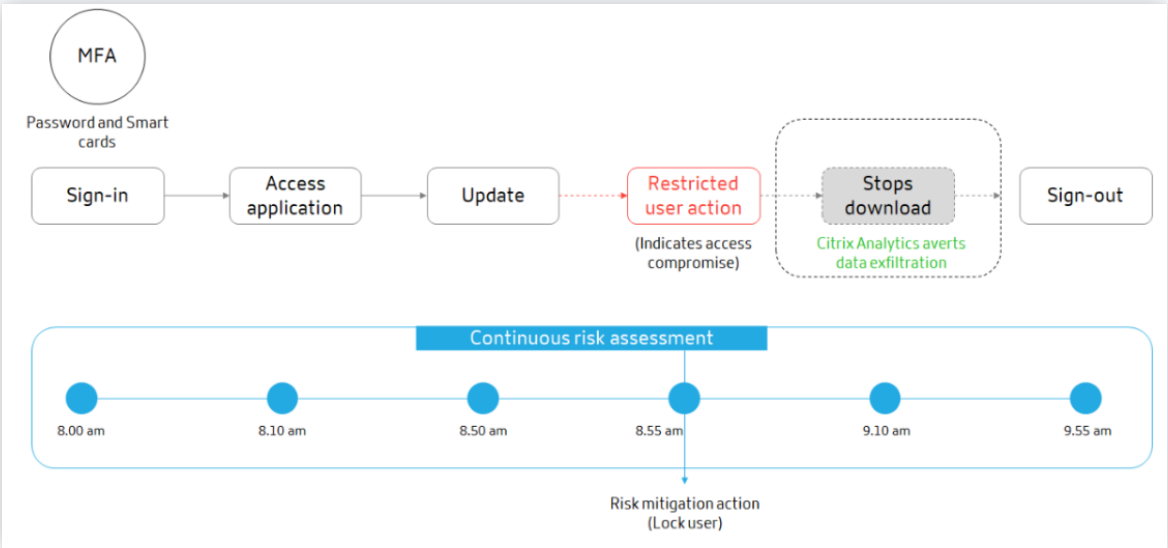
December 12, 2023

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Eine verstärkte Nutzung tragbarer Computergeräte und des Internets ermöglicht es Citrix Workspace-Benutzern, von fast jedem Ort und auf jedem Gerät aus zu arbeiten. Die Herausforderung bei dieser Flexibilität besteht darin, dass der Fernzugriff sensible Daten durch cyberkriminelle Aktivitäten wie Datenexfiltration, Diebstahl, Vandalismus und Serviceunterbrechungen Sicherheitsrisiken aussetzt. Mitarbeiter innerhalb von Organisationen werden wahrscheinlich ebenfalls zu diesem Schaden beitragen.

Einige herkömmliche Methoden zur Bewältigung solcher Risiken sind die Implementierung einer Multifaktor-Authentifizierung, kurzer Anmeldesitzungen usw. Obwohl diese Risikobewertungsmethoden ein höheres Sicherheitsniveau gewährleisten, bieten sie nach der ersten Validierung der Benutzer keine vollständige Sicherheit. Wenn ein böswilliger Benutzer erfolgreich Zugriff auf das Netzwerk erhält, missbraucht er sensible Daten, die für eine Organisation schädlich sind.

Um den Sicherheitsaspekt zu verbessern und eine bessere Benutzererfahrung zu gewährleisten, führt Citrix Analytics die Lösung einer kontinuierlichen Risikobewertung ein. Diese Lösung schützt Ihre Daten sowohl vor externen Cyberkriminellen als auch vor böswilligen Insidern, indem sichergestellt wird, dass das Risiko der Benutzer, die Citrix Virtual Apps and Desktops oder Citrix DaaS (ehemals Citrix Virtual Apps and Desktops Service) verwenden, dasselbe bleibt wie bei der Überprüfung in der Anfangsphase, ohne dass der Benutzer dies jedes Mal nachweisen muss. Diese Lösung wird erreicht, indem ein riskantes Ereignis während einer Sitzung kontinuierlich bewertet und automatisch Maßnahmen ergriffen werden, um zu verhindern, dass die Ressourcen der Organisation weiter missbraucht werden.



Anwendungsfälle

Stellen Sie sich einen Benutzer Adam Maxwell vor, der nach mehreren fehlgeschlagenen Anmeldeversuchen von einem ungewöhnlichen Ort aus, der seinem üblichen Verhalten widerspricht, zum er-

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

sten Mal auf ein Netzwerk zugreifen konnte. Außerdem weist der Standort eine Erfolgsbilanz bei Cyberangriffen auf. In diesem Szenario müssen Sie sofort Maßnahmen ergreifen, um zu verhindern, dass Adams Konto weiter missbraucht wird. Sie können Adams Konto sperren und ihn über die ergriffenen Maßnahmen informieren. Diese Aktion kann vorübergehend zu Dienstunterbrechungen für das Konto des Benutzers führen. Der Benutzer kann sich an den Administrator wenden, um Unterstützung bei der Wiederherstellung des Kontos zu erhalten.

Stellen Sie sich ein anderes Szenario vor, in dem Adam zum ersten Mal von einem neuen Gerät und von einer neuen IP auf ein Netzwerk zugegriffen hat. Sie können Adam kontaktieren und um Bestätigung bitten, ob er diese Aktivität identifiziert. Wenn ja, könnte es sein, dass Adam sein Arbeitsgerät gewechselt hat und von seinem Heimnetzwerk aus arbeitet. Diese Aktivität schadet der Sicherheit Ihres Unternehmens nicht und kann ignoriert werden. Wenn der Benutzer diese Aktivität jedoch nicht ausgeführt hat, ist es wahrscheinlich, dass das Konto kompromittiert wurde. In diesem Szenario können Sie das Konto des Benutzers sperren, um weitere Schäden zu vermeiden.

Hauptfeatures

Kontinuierliche Risikobewertung automatisiert einige der Funktionen, die mit Richtlinien und Sichtbarkeits-Dashboards verbunden sind:

Unterstützt mehrere Bedingungen

Wenn Sie eine Richtlinie erstellen oder ändern, können Sie bis zu vier Bedingungen hinzufügen. Die Bedingungen können Kombinationen aus Standardrisikoindikatoren und benutzerdefinierten Risikoindikatoren, Benutzerrisikobewertungen oder beidem enthalten.

Weitere Informationen finden Sie unter Was sind Richtlinien.

Benachrichtigen Sie Benutzer, bevor Sie Aktionen anwenden

Bevor Sie eine entsprechende Aktion auf das Konto eines Benutzers anwenden, können Sie den Benutzer benachrichtigen und die Art einer erkannten ungewöhnlichen Aktivität beurteilen.

Weitere Informationen finden Sie unter Endbenutzer-Antwort anfordern.

Benutzer nach dem Anwenden von Aktionen benachrichtigen

Bei einigen Aktivitäten kann das Warten auf die Benutzerantwort vor dem Anwenden einer Aktion das Benutzerkonto und die Sicherheit Ihres Unternehmens gefährden. In solchen Szenarien können Sie eine störende Aktion anwenden, wenn Sie eine ungewöhnliche Aktivität feststellen, und den Benutzer darüber informieren.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Weitere Informationen finden Sie unter Benutzer nach Anwendung einer störenden Aktion benachrichtigen.

Durchsetzung und Monitormodi

Sie können Richtlinien basierend auf Ihren Anforderungen auf Durchsetzungs- oder Überwachungsmodi festlegen. Richtlinien im Erzwingungsmodus wirken sich direkt auf die Benutzerkonten aus. Wenn Sie jedoch die Auswirkungen oder das Ergebnis Ihrer Richtlinien beurteilen möchten, bevor Sie sie implementieren, können Sie Ihre Richtlinien auf den Überwachungsmodus einstellen.

Weitere Informationen finden Sie unter Unterstützte Modi.

Einblick in Zugriff und Richtlinien-Dashboards

Mithilfe des Dashboards **"Zugriffsübersicht** "können Sie Einblicke in die Anzahl der Zugriffsversuche von Benutzern erhalten. Weitere Informationen finden Sie unter Zugriffsübersicht.

Mithilfe des Dashboards **Richtlinien und Aktionen** können Sie Einblicke in die Richtlinien und Aktionen erhalten, die auf Benutzerkonten angewendet werden. Weitere Informationen finden Sie unter Richtlinien und Aktionen.

Standardrichtlinien

Citrix Analytics führt vordefinierte Richtlinien ein, die standardmäßig im **Richtlinien-Dashboard** aktiviert sind. Diese Richtlinien werden erstellt, indem Risikoindikatoren und Benutzerrisikobewertungen als vordefinierte Bedingungen verwendet werden. Jeder Standardrichtlinie wird eine globale Aktion zugewiesen.

> **Hinweis**
>
> Die in Ihrer Umgebung aufgeführten Richtlinien können je nachdem, wann Sie Citrix Analytics zum ersten Mal verwendet haben und ob Sie lokale Änderungen vorgenommen haben, variieren.

Weitere Informationen finden Sie unter Was sind Richtlinien.

Sie können die folgenden Standardrichtlinien verwenden oder sie basierend auf Ihren Anforderungen ändern:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Richtlinienname	Bedingung	Datenquelle	Aktion
Erfolgreicher Berechtigungs-Exploit	Wenn die übermäßigen Authentifizierungsfehler und Risikoindikatoren für verdächtige Anmeldung ausgelöst werden	Citrix Gateway	Benutzer sperren
Potenzielle Datenexfiltration	Wenn der Risikoindikator für potenzielle Datenexfiltration ausgelöst wird	Citrix Virtual Apps and Desktops von Citrix und Citrix DaaS	Benutzer abmelden
Ungewöhnlicher Zugriff von einer verdächtigen IP	Wenn die verdächtige Anmeldung und Anmeldung über verdächtige IP-Risikoindikatoren ausgelöst werden	Citrix Gateway	Benutzer sperren
Erster Zugriff vom Gerät	Wenn der CVAD-Erstzugriff von einem neuen Gerät ausgelöst wird	Citrix Virtual Apps and Desktops von Citrix und Citrix DaaS	Antwort des Endbenutzers anfragen
Unmögliche Reise bei Zugriff	Wenn die Risikoanzeige Impossible Travel ausgelöst wird.	Citrix Virtual Apps and Desktops von Citrix und Citrix DaaS	Antwort des Endbenutzers anfragen
Unmögliche Reise bei Authentifizierung	Wenn die Risikoanzeige Impossible Travel ausgelöst wird.	Citrix Gateway	Antwort des Endbenutzers anfragen

Richtlinien und Maßnahmen

December 12, 2023

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

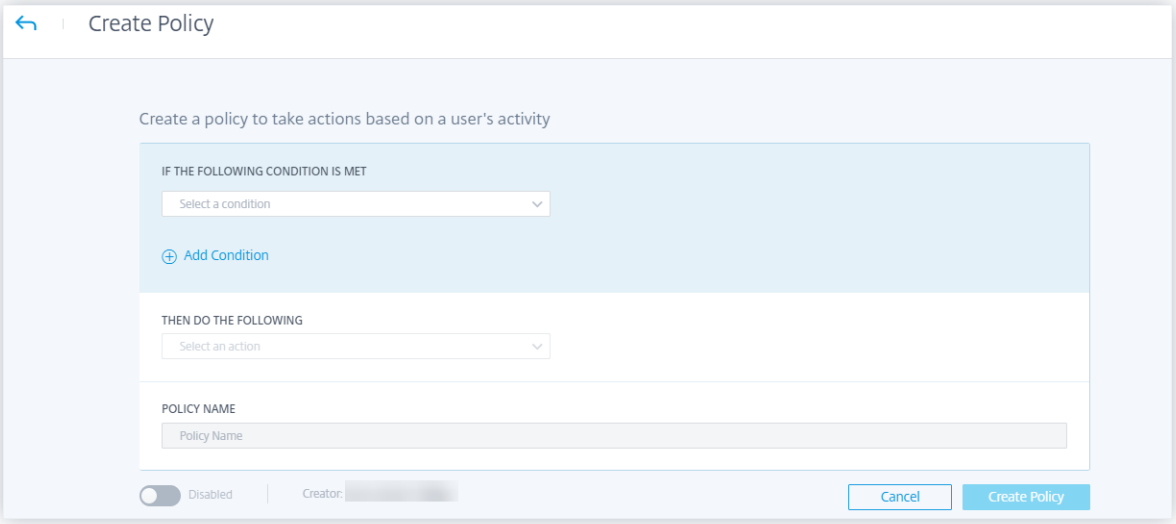
> **Hinweis**
>
> **Achtung**: Citrix Content Collaboration und ShareFile haben das Ende ihrer Lebensdauer erreicht und stehen Benutzern nicht mehr zur Verfügung.

Sie können Richtlinien in Citrix Analytics erstellen, mit denen Sie Aktionen für Benutzerkonten ausführen können, wenn ungewöhnliche oder verdächtige Aktivitäten auftreten. Mithilfe von Richtlinien können Sie den Prozess der Anwendung von Aktionen wie dem Deaktivieren eines Benutzers und dem Hinzufügen von Benutzern zu einer Beobachtungsliste automatisieren. Wenn Sie Richtlinien aktivieren, wird eine entsprechende Aktion sofort angewendet, nachdem ein anomales Ereignis eingetreten ist und die Richtlinienbedingung erfüllt ist. Sie können Aktionen auch manuell auf Benutzerkonten mit anomalen Aktivitäten anwenden.

Was sind die Richtlinien?

Eine Richtlinie ist eine Reihe von Bedingungen, die erfüllt sein müssen, um eine Aktion anwenden zu können. Eine Richtlinie enthält eine oder mehrere Bedingungen und eine einzelne Aktion. Sie können eine Richtlinie mit mehreren Bedingungen und einer Aktion erstellen, die auf das Konto eines Benutzers angewendet werden kann.

Risikobewertung ist eine globale Bedingung. Globale Bedingungen können auf einen bestimmten Benutzer für eine bestimmte Datenquelle angewendet werden. Sie können Benutzerkonten beobachten, die ungewöhnliche Aktivitäten zeigen. Andere Bedingungen sind spezifisch für Datenquellen und ihre Risikoindikatoren. Die Bedingungen enthalten Kombinationen aus Risikobewertungen, Standartrisikoindikatoren und benutzerdefinierten Risikoindikatoren. Sie können beim Erstellen einer Richtlinie bis zu 4 Bedingungen hinzufügen.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Wenn Ihre Organisation beispielsweise vertrauliche Daten verwendet, können Sie die Menge der Daten einschränken, die von Benutzern intern freigegeben oder freigegeben werden. Wenn Sie jedoch eine große Organisation haben, ist es für einen einzelnen Administrator nicht möglich, viele Benutzer zu verwalten und zu überwachen. Sie können eine Richtlinie erstellen, bei der jeder, der sensible Daten übermäßig weitergibt, zu einer Beobachtungsliste hinzugefügt werden oder sein Konto sofort deaktiviert werden kann.

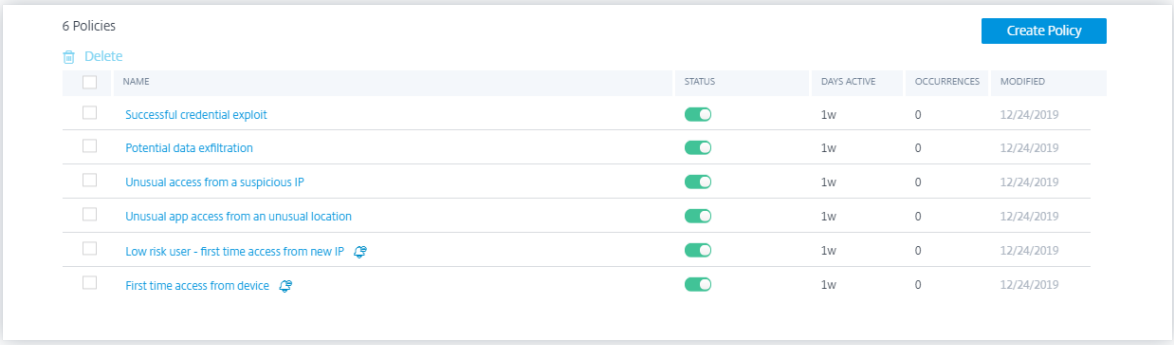
Standardrichtlinien

Standardrichtlinien sind im **Richtlinien-Dashboard** vordefiniert und aktiviert. Sie werden basierend auf vordefinierten Bedingungen erstellt und jeder Standardrichtlinie wird eine entsprechende Aktion zugewiesen. Sie können entweder eine Standardrichtlinie verwenden oder sie basierend auf Ihren Anforderungen ändern.

Citrix Analytics unterstützt die folgenden Standardrichtlinien:

- Erfolgreicher Exploit für Anmeldedaten
- Potenzielle Datenexfiltration
- Ungewöhnlicher Zugriff von einer verdächtigen IP
- Erster Zugriff vom Gerät
- Virtual Apps and Desktops und Citrix DaaS —Unmögliche Reise bei Zugriff
- Gateway —Unmögliche Reise bei Authentifizierung

Informationen zu den voreingestellten Bedingungen und Aktionen in Bezug auf die vorangegangenen Standardrichtlinien finden Sie unter Kontinuierliche Risikobewertung.



Informationen zur vordefinierten Richtlinie für den Geofencing-Anwendungsfall finden Sie unter Vorkonfigurierte Richtlinie.

Wie kann man Bedingungen hinzufügen oder entfernen?

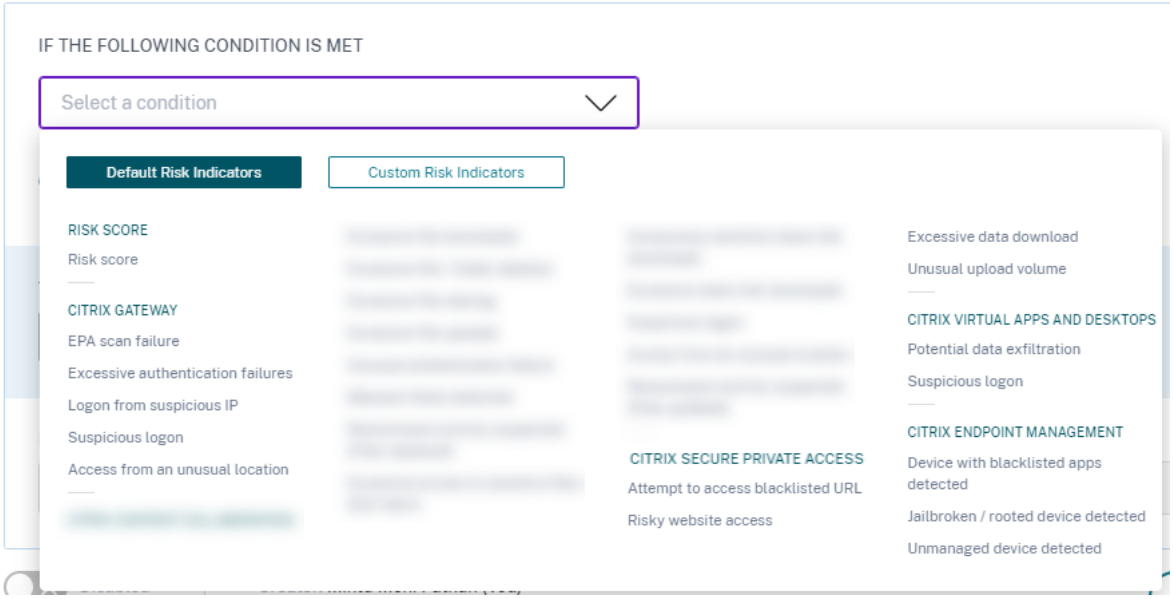
Um weitere Bedingungen hinzuzufügen, wählen Sie **Bedingung hinzufügen** im Abschnitt **WENN DIE FOLGENDE BEDINGUNG ERFÜLLT IST** der Seite **Richtlinie erstellen** . Um eine Bedingung zu entfer-

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

nen, wählen Sie das **-** -Symbol aus, das neben der Bedingung angezeigt wird.

Standard- und benutzerdefinierte Risikoindikatoren

Das Menü "Bedingungen"wird basierend auf den Registerkarten **Standardrisikoindikatoren** und **Benutzerdefinierte Risikoindikatoren** auf der Seite **"Richtlinie erstellen** "getrennt. Auf diesen Registerkarten können Sie leicht den Typ des Risikoindikators identifizieren, den Sie bei der Auswahl einer Bedingung für die Richtlinienkonfiguration auswählen möchten.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Was sind die Aktionen?

Aktionen sind Reaktionen auf verdächtige Ereignisse, die das Auftreten zukünftiger anomaler Ereignisse verhindern. Sie können Aktionen auf Benutzerkonten anwenden, die ungewöhnliches oder verdächtiges Verhalten anzeigen. Sie können entweder Richtlinien so konfigurieren, dass Aktionen automatisch auf das Benutzerkonto angewendet werden, oder eine bestimmte Aktion manuell aus der Risikozeitleiste des Benutzers anwenden.

Sie können globale Aktionen oder Aktionen für jede Citrix Datenquelle anzeigen. Sie können auch zuvor angewendete Aktionen für einen Benutzer jederzeit deaktivieren.

> **Hinweis**
>
> Unabhängig von der Datenquelle, die einen Risikoindikator auslöst, können Aktionen in Bezug auf andere Datenquellen angewendet werden.

In der folgenden Tabelle werden die Aktionen beschrieben, die Sie ergreifen können.

Bezeichnung der Aktion	Beschreibung	Anwendbare Datenquellen
Globale Aktionen		
Zur Watchlist hinzufügen	Wenn Sie einen Benutzer auf zukünftige potenzielle Bedrohungen überwachen möchten, können Sie ihn einer Watchlist hinzufügen. Im Bereich **Benutzer in Watchlist** werden alle Benutzer angezeigt, die Sie auf potenzielle Bedrohungen basierend auf der ungewöhnlichen Aktivität ihres Kontos überwachen möchten. Basierend auf den Richtlinien Ihrer Organisation können Sie mit der Aktion Zur Watchlist hinzufügen einen Benutzer zur Watchlist hinzufügen.	Alle Datenquellen

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Bezeichnung der Aktion	Beschreibung	Anwendbare Datenquellen
	Um einen Benutzer zur Watchlist hinzuzufügen, navigieren Sie zum Benutzerprofil und wählen Sie im Menü **Aktionen** die Option **Zur Watchlist hinzufügen**aus. Klicken Sie auf **Übernehmen**, um die Aktion zu erzwingen.	

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Bezeichnung der Aktion	Beschreibung	Anwendbare Datenquellen
Administrator (en) benachrichtigen	Wenn ein Risikoindikator für einen Benutzer ausgelöst wird, können Sie die Administratoren manuell benachrichtigen oder eine Richtlinie für die automatische Benachrichtigung erstellen. Sie können die Administratoren aus der Citrix Cloud-Domäne und anderen Nicht-Citrix Cloud-Domänen in Ihrer Organisation auswählen. Wenn Sie ein Citrix Cloud-Administrator mit vollen Zugriffsberechtigungen sind, sind die E-Mail-Benachrichtigungen standardmäßig für Ihr Citrix Cloud-Konto deaktiviert. Um E-Mail-Benachrichtigungen zu erhalten, aktivieren Sie sie in Ihrem Citrix Cloud-Konto. Weitere Informationen finden Sie unter Empfangen von Benachrichtigungen per E-Mail. Wenn Sie ein Citrix Cloud-Administrator mit benutzerdefinierten Zugriffsberechtigungen (schreibgeschützt und Vollzugriff) zur Verwaltung von Security Analytics sind, sind die E-Mail-Benachrichtigungen für Ihr Citrix Cloud-Konto aktiviert. Um keine E-Mail-Benachrichtigungen von Citrix Analytics mehr zu erhalten, bitten Sie Ihren Citrix Cloud-Administrator mit vollem Zugriff, Ihren Namen aus der Verteilerliste der Benachrichtigungsadministra-toren zu entfernen. Weitere Informationen zu finden Sie	

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Bezeichnung der Aktion	Beschreibung	Anwendbare Datenquellen
Antwort des Endbenutzers anfragen	Wenn das Benutzerkonto ungewöhnliche oder verdächtige Aktivitäten enthält, können Sie den Benutzer benachrichtigen, um zu bestätigen, ob der Benutzer die Aktivität identifiziert. Basierend auf der Aktivität können Sie die nächste Aktion bestimmen, die für das Konto des Benutzers durchgeführt werden soll. Weitere Informationen finden Sie unter Endbenutzer-Antwort anfordern.	
Endbenutzer benachrichtigen	Wenn ungewöhnliche oder verdächtige Aktivitäten auf dem Konto des Benutzers auftreten, können Sie den Endbenutzer per E-Mail-Benachrichtigung benachrichtigen. Weitere Informationen finden Sie unter Endbenutzer benachrichtigen.	
NetScaler Gateway Aktionen		
Aktive Sitzungen abmelden	Wenn die Aktion angewendet wird, meldet sie die derzeit aktive Benutzersitzung ab. Es blockiert keine zukünftigen Benutzersitzungen.	On-premises Citrix Gateway und Citrix Application Delivery Management

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Bezeichnung der Aktion	Beschreibung	Anwendbare Datenquellen
Benutzerkonto sperren	Wenn das Konto eines Benutzers aufgrund eines ungewöhnlichen Verhaltens gesperrt ist, kann er nicht über Citrix Gateway auf Ressourcen zugreifen, bis der Gateway-Administrator das Konto entsperrt.	Citrix Gateway (on-premises)
Benutzerkonto entsperren	Wenn das Konto eines Benutzers versehentlich gesperrt wurde, obwohl kein anomales Verhalten erkannt wurde, können Sie diese Aktion anwenden, um es zu entsperren und den Zugriff auf das Konto wiederherzustellen.	Citrix Gateway (on-premises)
Citrix Virtual Apps and Desktops und Citrix DaaS-Aktionen		
Aktive Sitzungen abmelden	Wenn die Aktion angewendet wird, meldet sie die derzeit aktive Benutzersitzung ab. Es blockiert keine zukünftigen Benutzersitzungen.	Citrix DaaS (früher Citrix Virtual Apps and Desktops Service)

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Bezeichnung der Aktion	Beschreibung	Anwendbare Datenquellen
Starten Sie die Aufzeichnung	Wenn ein ungewöhnliches Ereignis im Virtual Desktops-Konto des Benutzers auftritt, kann der Administrator mit der Aufzeichnung der aktuell aktiven Sitzungen des Benutzers beginnen. Wenn der Benutzer Citrix Virtual Apps and Desktops 7.18 oder einer höheren Version verwendet und bei der virtuellen Sitzung angemeldet ist, kann ein Administrator die Aktion "Sitzungsaufzeichnung starten" in Citrix Analytics for Security dynamisch auslösen, mit der die Aufzeichnung der aktuellen aktiven Sitzung des Benutzers gestartet wird.	Citrix DaaS (früher Citrix Virtual Apps and Desktops Service)

Hinweise

- Sie können unabhängig von den Datenquellen jede Aktion auf einen Risikoindikator anwenden.
- Administratoren können jetzt dynamische Sitzungsaufzeichnungsaktionen auf Citrix DaaS-Sites ausführen und die virtuellen Sitzungen der Benutzer dynamisch aufzeichnen.
- Die Aktionen „ **Endbenutzerantwort anfordern** "und „ **Endbenutzer benachrichtigen** "können nicht auf anonyme Benutzer angewendet werden, da diese keine E-Mail-Adressen in **Active Directory**haben. Stellen Sie daher sicher, dass entweder die E-Mail-Adressen Ihrer Benutzer im **Active Directory** verfügbar sind, wenn eine Verbindung zwischen Ihrem Active Directory und Citrix Cloud hergestellt wurde.

Nur-View-Sharing

Bevor Sie die Aktion **Links zur Freigabe mit Leserechten ändern** auf das Konto eines Benutzers anwenden, stellen Sie sicher, dass die folgenden Bedingungen erfüllt sind:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Voraussetzungen

- Der Administrator muss über ein Enterprise-Konto in Content Collaboration verfügen, um die Aktion **Links zur schreibgeschützten Freigabe ändern** verwenden zu können.
- Die schreibgeschützte Freigabe ist eine Funktion, die auf Anfrage in den Enterprise-Konten von Citrix Content Collaboration verfügbar ist. Bevor Sie die Aktion **Links ändern auf schreibgeschützte Freigabe** in Citrix Analytics anwenden, stellen Sie sicher, dass die Funktion "Nur schreibgeschützte Freigabe"bereits in den Content Collaboration Enterprise-Konten des Benutzers und des Administrators aktiviert ist. Weitere Informationen finden Sie im Citrix Supportartikel CTX208601.

Unterstützte Dateitypen Die Aktion zur schreibgeschützten Freigabe gilt nur für die folgenden Dateitypen:

- Microsoft Office-Dateien
- PDF
- Bilddateien (benötigt SZC v3.4.1 oder höher):
  - BMP
  - GIF
  - JPG
  - JPEG
  - PNG
  - TIF
  - TIFF
- Audio- und Videodateien, die in einer von Citrix verwalteten Storage Zone gespeichert sind.

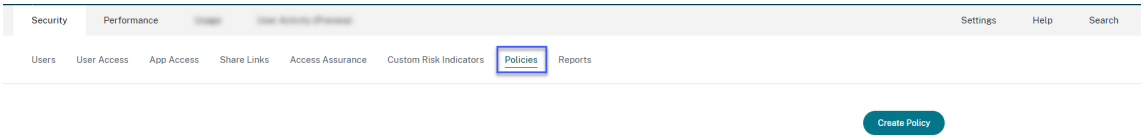
Konfigurieren von Richtlinien und Aktionen

Gehen Sie beispielsweise wie folgt vor, um eine Richtlinie für exzessives Filesharing zu erstellen. Wenn ein Benutzer in Ihrer Organisation eine ungewöhnlich große Datenmenge gemeinsam verwendet, sind die Freigabelinks automatisch abgelaufen. Sie werden benachrichtigt, wenn ein Benutzer Daten teilt, die das normale Verhalten dieses Benutzers übersteigen. Indem Sie die Richtlinie für übermäßige Dateifreigabe anwenden und sofortige Maßnahmen ergreifen, können Sie die Datenexfiltration aus dem Konto eines Benutzers verhindern.

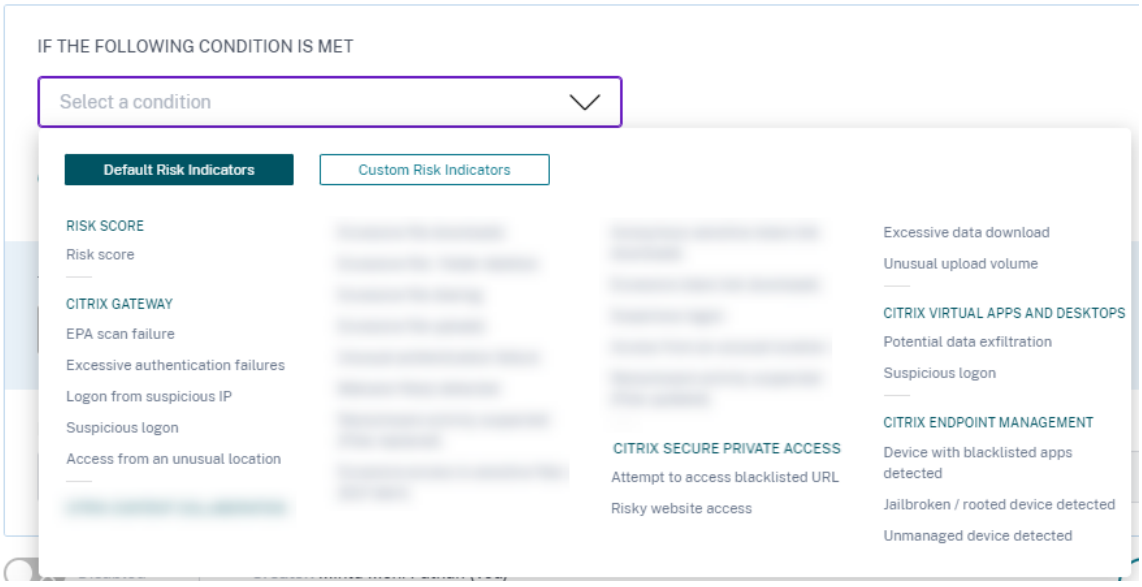
Gehen Sie folgendermaßen vor, um eine Richtlinie zu erstellen:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

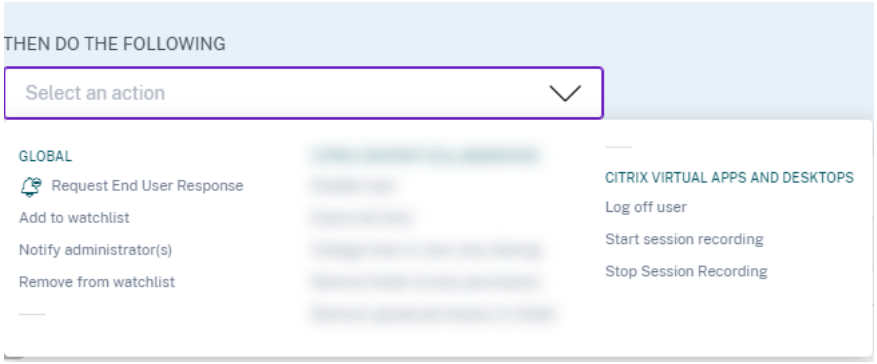
1. Nachdem Sie sich bei Citrix Analytics angemeldet haben, gehen Sie zu **Sicherheit > Richtlinien > Richtlinie erstellen**.



2. Wählen **Sie im Listenfeld WENN DIE FOLGENDE BEDINGUNG ERFÜLLT IST**, die standardmäßigen oder benutzerdefinierten Risikoindikatorbedingungen aus, auf die eine Aktion angewendet werden soll.

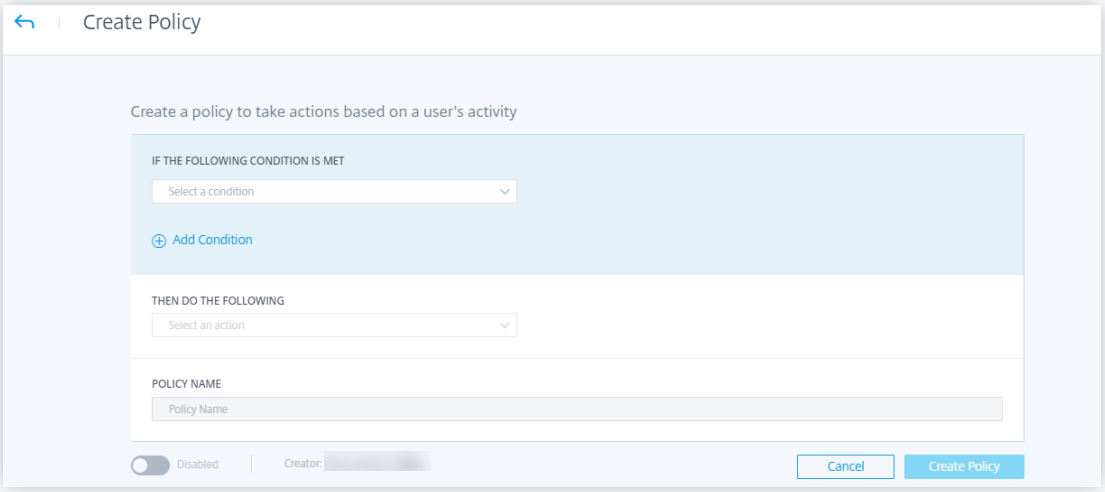


3. Wählen **Sie aus der Liste DANN FOLGENDES** eine Aktion aus.



4. Geben Sie im Textfeld **Richtlinienname** einen Namen ein und aktivieren Sie die Richtlinie mithilfe der bereitgestellten Umschaltfläche.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



5. Klicken Sie auf **Richtlinie erstellen**.

Nach dem Erstellen einer Richtlinie wird die Richtlinie im Dashboard **Richtlinien** angezeigt.

Das **Richtlinien-Dashboard** zeigt die Richtlinien an, die mit den Datenquellen verknüpft sind, die erfolgreich erkannt und mit Citrix Analytics verbunden wurden. Das Dashboard zeigt nicht die Richtlinien an, für die Bedingungen für die unentdeckten Datenquellen definiert sind.

Das Deaktivieren der Datenverarbeitung für eine bereits verbundene Datenquelle wirkt sich jedoch nicht auf die vorhandenen Richtlinien im **Richtlinien**-Dashboard aus.

Antwort des Endbenutzers anfragen

Endbenutzerantwort anfordern ist eine globale Aktion, mit der Sie einen Benutzer sofort benachrichtigen können, nachdem Sie eine ungewöhnliche Aktivität in seinem Citrix Konto festgestellt haben. Wenn Sie die Aktion anwenden, wird eine E-Mail-Benachrichtigung an den Benutzer gesendet. Der Benutzer muss per E-Mail über die Legitimität seiner Aktivität antworten.

Bestimmen Sie, welche Aktion Sie für Ihre Benutzer anwenden möchten:

Anhand der Antwort des Benutzers können Sie die nächste Vorgehensweise festlegen, die Sie ergreifen möchten. Sie können eine globale Aktion wie "Zur Watchlist hinzufügen"oder "Administratoren benachrichtigen"anwenden. Oder Sie können eine datenquellenspezifische Aktion anwenden, z. B. Citrix Gateway —Benutzer sperren.

Wenn Sie eine Antwort erhalten, dass der Benutzer die gemeldete Aktivität ausgeführt hat, ist die Aktivität nicht verdächtig und Sie müssen keine Maßnahmen für das Konto des Benutzers ergreifen. Das tägliche Limit für das Senden von Sicherheitswarnungen an den Benutzer beträgt drei E-Mails.

Betrachten Sie einen Citrix Content Collaboration Benutzer, dessen Risikobewertung 80 in einer Dauer von 80 Minuten überschritten hat. Sie können den Benutzer über dieses ungewöhnliche Verhalten

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

warnen, indem Sie die Aktion **Endbenutzerantwort anfordern** anwenden. Eine Sicherheitswarnung wird von der E-Mail-ID an den Benutzer gesendet `security-analytics@cloud.com`.

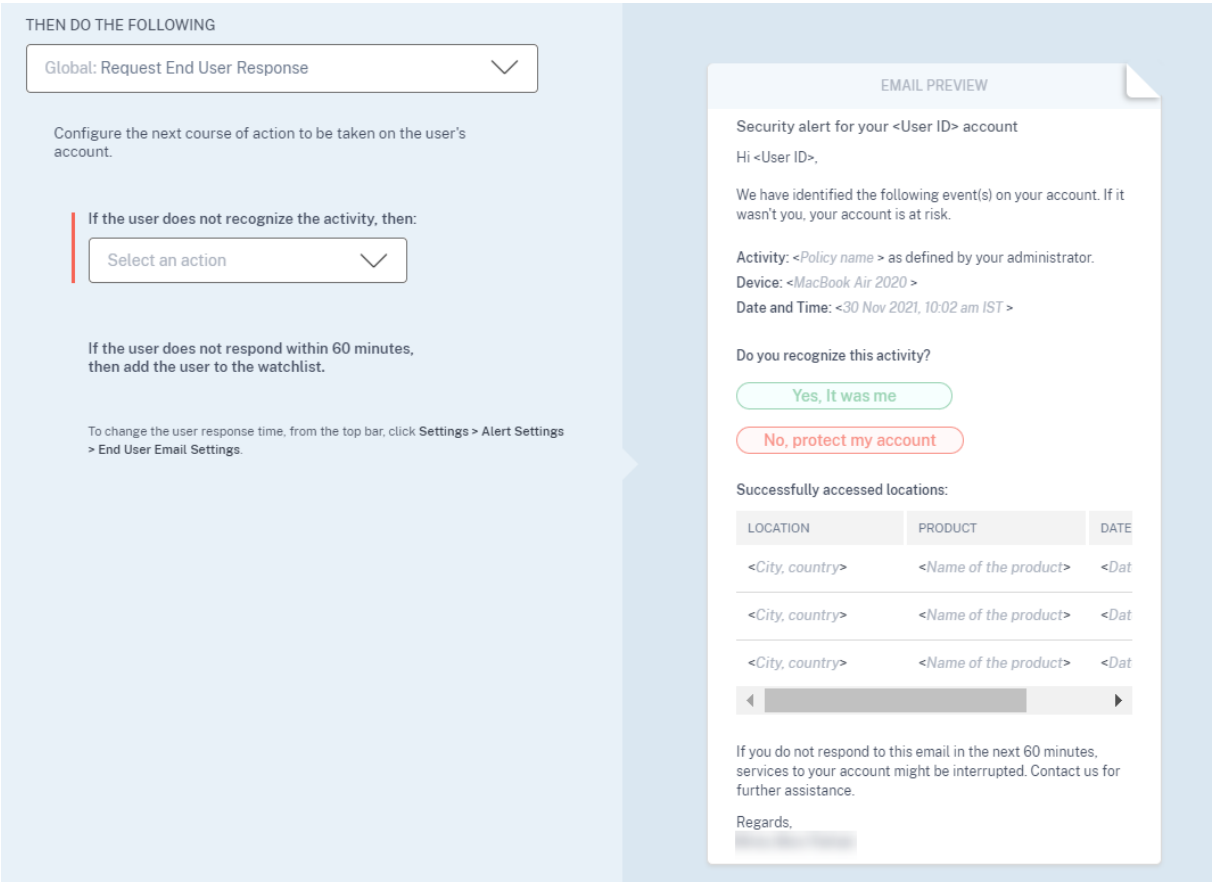
Die E-Mail enthält die folgenden Informationen:

- Aktivität des Benutzers, die den Risikoindikator ausgelöst hat
- Gerät des Benutzers
- Datum und Uhrzeit der Benutzeraktivität
- Standorte (Städte und Länder), von denen aus erfolgreich auf Produkte oder Dienstleistungen zugegriffen wird. Wenn die Stadt oder das Land nicht verfügbar ist, wird der entsprechende Wert als "Unbekannt"angezeigt

Die Aktion "**Antwort vom Endbenutzer anfordern** "wird der Risikozeitleiste des Benutzers hinzugefügt.

Wenn der Benutzer die in seinem Citrix Konto erkannte Aktivität nicht erkennt, wendet Citrix Analytics die von Ihnen definierte Aktion an.

Wenn der Benutzer seine Antwort nicht innerhalb einer Stunde nach Erhalt der E-Mail sendet, fügt Citrix Analytics den Benutzer zur Beobachtungsliste hinzu. Sie können den Benutzer und sein Konto auf verdächtige Aktivitäten überwachen und entsprechende Maßnahmen ergreifen.

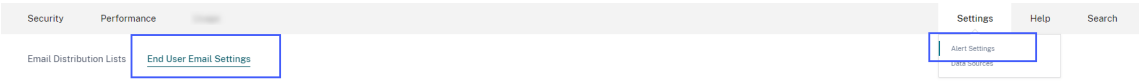


© 1999–2024 Cloud Software Group, Inc. All rights reserved.

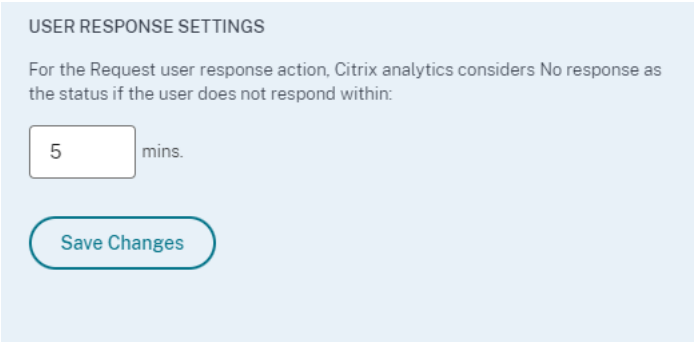
Wie stellt man die Reaktionszeit des Benutzers ein? Sie können die Reaktionszeit des Benutzers auf Ihre Sicherheitswarnungs-E-Mail konfigurieren. Wenn der Benutzer innerhalb des angegebenen Zeitraums nicht auf die gemeldete Aktivität reagiert, wird er zur Überwachung zur Beobachtungsliste hinzugefügt.

Folgen Sie den Schritten, um die Reaktionszeit des Benutzers zu konfigurieren:

1. Klicken Sie auf **Einstellungen > Warnungseinstellungen > E-Mail-Einstellungen für Endbenutzer**.



2. Geben Sie auf der Seite **E-Mail-Einstellungen für Endbenutzer** die Anzahl der Minuten in dem Textfeld ein.

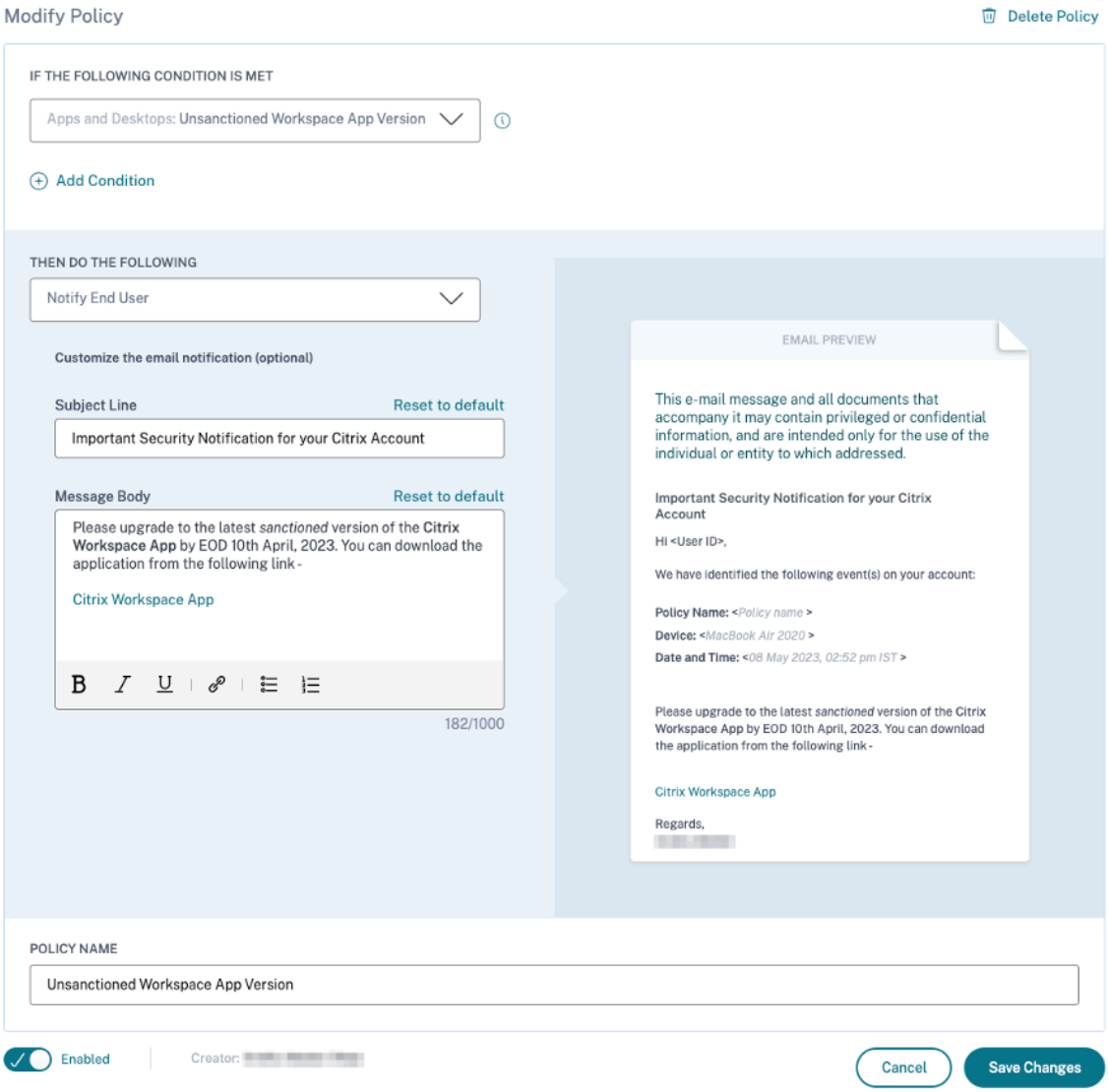


3. Klicken Sie auf **Änderungen speichern**.

Sie können der Sicherheitswarnungs-E-Mail auch ein Banner, einen Kopfzeilentext und einen Fußzeilentext hinzufügen, damit sie legitim aussieht, die Aufmerksamkeit der Benutzer auf sich zieht und die Reaktionszeit verlängert wird. Weitere Informationen finden Sie unter E-Mail-Einstellungen für Endbenutzer.

Endbenutzer benachrichtigen **Endbenutzer benachrichtigen** ist eine globale Aktion, mit der Sie E-Mail-Benachrichtigungen an Endbenutzer senden können, wenn in ihren Citrix-Konten ungewöhnliches oder verdächtiges Verhalten festgestellt wird. Die E-Mail-Betreffzeile und der Nachrichtentext sind anpassbar. Wenn die Aktion angewendet wird, nachdem eine Richtlinie ausgelöst wurde, wird eine E-Mail-Benachrichtigung an den Benutzer gesendet. Der Endbenutzer wird nicht um eine Antwort gebeten und es werden keine störenden Aktionen auf dem Konto des Benutzers ausgeführt.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Diese Aktion kann dazu beitragen, verschiedene Compliance-Anwendungsfälle zu erfüllen, die auf einem oder mehreren integrierten oder benutzerdefinierten Risikoindikator-Triggern basieren. Mit der anpassbaren Betreffzeile und dem Nachrichtentext der E-Mail ist es auch flexibel genug, um viele allgemeine Anwendungsfälle für Endbenutzerbenachrichtigungen zu bedienen, für die keine Reaktion oder störende Aktion auf dem Konto des Benutzers erforderlich ist.

Die E-Mail enthält die folgenden Informationen:

- Der Aktion zugeordneter Richtlinienname.
- Gerät des Benutzers (falls verfügbar)
- Datum und Uhrzeit der Benutzeraktivität

Die E-Mail-Benachrichtigung des Endbenutzers wird von der E-Mail-ID aus gesendet `security-`

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

analytics@cloud.com.

> **Hinweis:**
>
> Das tägliche Limit für alle Richtlinien liegt bei **drei** E-Mails pro Benutzer. Sobald dieser Schwellenwert überschritten ist, wird die Aktion nicht angewendet und es wird keine E-Mail-Benachrichtigung an den Endbenutzer gesendet. Die Aktion ist in der Timeline-Ansicht des Benutzers mit der Nachricht sichtbar, dass das **tägliche E-Mail-Limit für den Benutzer erreicht wurde**.

Die Aktion wird dem Risikozeitplan des Benutzers hinzugefügt. Es handelt sich jedoch nicht um eine manuelle Aktion und kann nicht von der Timeline-Ansicht aus auf einen Benutzer angewendet werden.

Anpassung des E-Mail-Inhalts von Endbenutzern Zuvor wandten sich Citrix Analytics-Administratoren manuell an die Endbenutzer, um Anweisungen zur Behebung vermuteter Aktivitäten zu geben. Dies war ein zeitaufwändiger Prozess, um einen Vorfall zu schließen.

Die Funktion **zur Anpassung von E-Mail-Inhalten für Endbenutzer** wurde eingeführt, um Antworten von Endbenutzern anzufordern, Endbenutzer zu benachrichtigen und Informations-E-Mails zu senden. In der Antwort-E-Mail des Endbenutzers wird der Benutzer um eine Validierung/Antwort gebeten. Eine Informations-E-Mail zeigt jedoch, welche Art von verdächtigen Aktivitäten und welche Abhilfemaßnahmen bereits ergriffen wurden. Die E-Mail zur Benachrichtigung des Endbenutzers informiert den Endbenutzer über Compliance-Verstöße/verdächtige Aktivitäten in seinem Citrix-Konto, ohne ihn um eine Antwort zu bitten.

Mit der Funktion **Anpassung des E-Mail-Inhalts von Endbenutzern** können Citrix Analytics-Administratoren eine benutzerdefinierte Nachricht in die Textvorlage „Antwort des Endbenutzers anfordern/Endbenutzer benachrichtigen“/Informations-E-Mail hinzufügen. Mithilfe des Rich-Text-Feld-Editors kann ein Administrator den Inhalt pro Richtlinie mithilfe verschiedener Bearbeitungswerkzeuge wie Fett, Kursiv, Hyperlink usw. ändern.

> **Hinweis:**
>
> Die Funktion zum Anpassen von E-Mail-Inhalten für Endbenutzer ist nur für richtlinienbasierte Aktionen und nicht für manuelle Aktionen verfügbar.

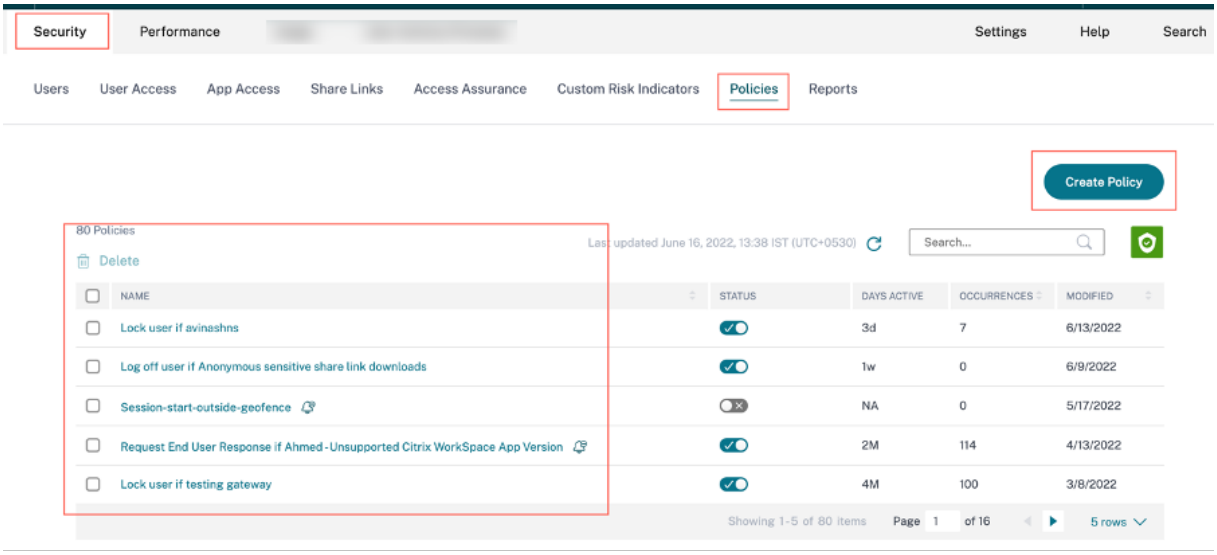
Sie können den Inhalt für drei Arten von E-Mails anpassen:

- Fordern Sie die Antwort-E-Mail des Endbenutzers an.
- E-Mail des Endbenutzers benachrichtigen
- E-Mail wird gesendet, wenn eine der folgenden Endbenutzeraktionen ausgeführt wird:
  - Aktion “Abmelden”unter **Citrix Apps und Desktop**

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

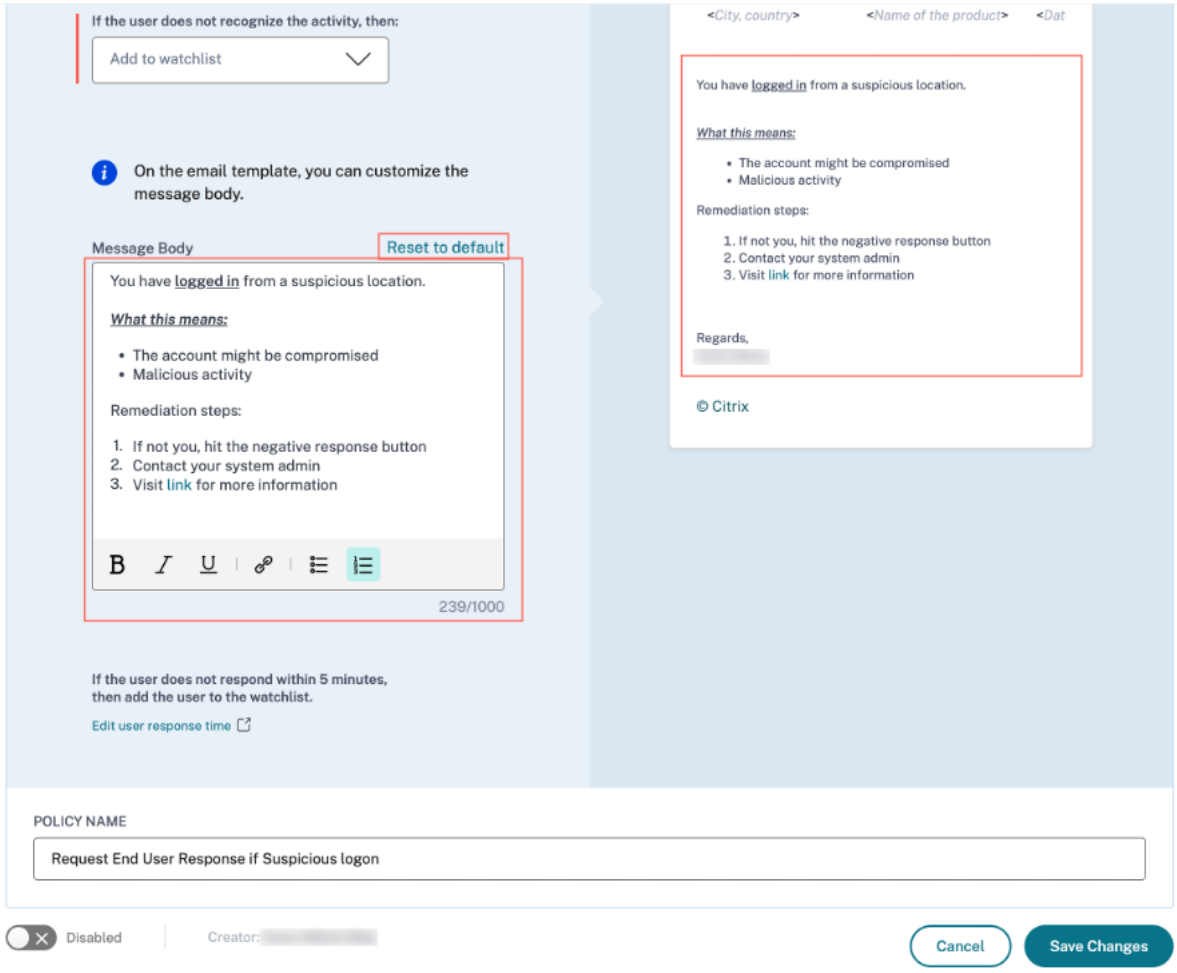
- Benutzer unter **NetScaler Gateway**abmelden und sperren

Sie können die Liste der Richtlinien auf der Registerkarte **Sicherheit > Richtlinien** anzeigen.



Sie können den benutzerdefinierten E-Mail-Text einsehen, indem Sie auf die bestehende Richtlinie klicken oder eine neue Richtlinie erstellen. Im rechten Bereich erhalten Sie eine Vorschau des aktualisierten E-Mail-Inhalts.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Hinweis

- Der Administrator kann den Inhalt auf die Standardvorlage setzen, indem er auf den Link Auf **Standard zurücksetzen** klickt. Die Zeichenbeschränkung für den benutzerdefinierten Textkörper ist 1000.
- Für die Aktion **Endbenutzer benachrichtigen** kann das Feld **Betreffzeile** auch vom Administrator angepasst werden. Sie kann auf die Standardeinstellungen zurückgesetzt werden, indem Sie auf den Link Auf **Standard zurücksetzen** klicken. Das Zeichenlimit für den benutzerdefinierten E-Mail-Betreff beträgt 500.

Klicken Sie auf **Änderungen speichern**, um die Richtlinie zu erstellen/zu aktualisieren. Wenn die Richtlinie ausgelöst wird, wird die folgende E-Mail-Benachrichtigung an den Endbenutzer gesendet:

- **Antwort-E-Mail des Endbenutzers anfordern**: Eine Richtlinienaktion, mit der eine E-Mail gesendet wird, in der eine Benutzerantwort angefordert wird.
- **Endbenutzer-E-Mail benachrichtigen**: Eine E-Mail-Benachrichtigung, die an Endbenutzer

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

gesendet wird und sie über Compliance-Probleme, verdächtige Aktivitäten usw. in ihrem Citrix-Konto informiert.

- **Informations-E-Mail**: Eine Informations-E-Mail, die nach einer Endbenutzeraktion gesendet wird.

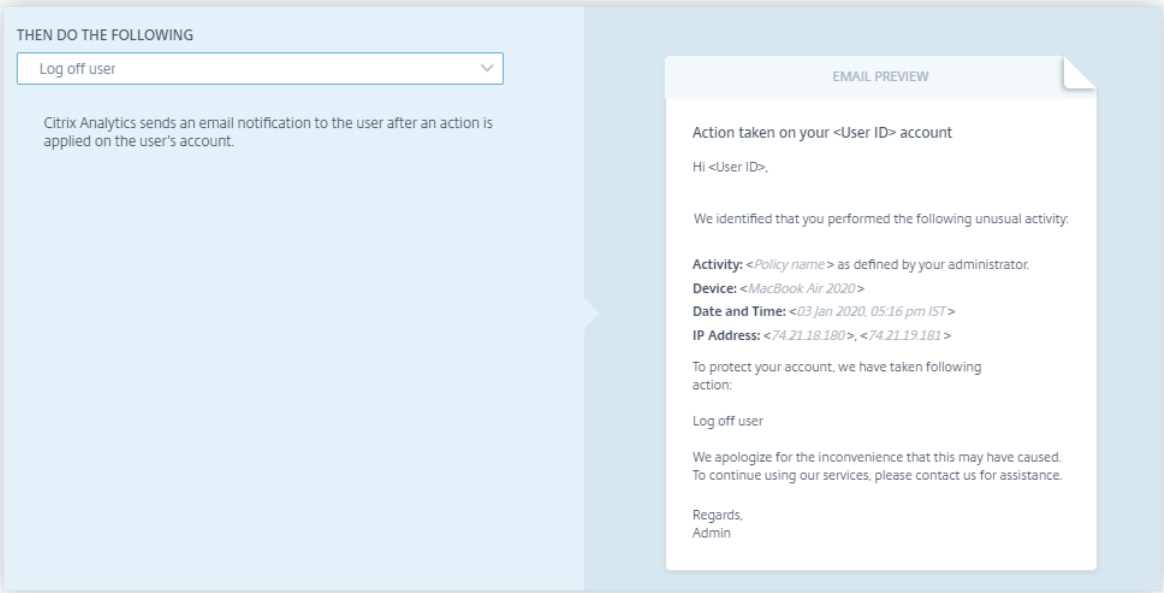
Der Endbenutzer kann die E-Mail lesen und die Korrekturmaßnahmen auf Anfrage des Administrators durchführen.

> **Hinweis:**
>
> Der Administrator mit schreibgeschütztem Zugriff kann den E-Mail-Text nicht bearbeiten/hinzufügen.

Benutzer benachrichtigen, nachdem Sie störende Aktionen angewendet haben

Bei diesem Aktionstyp können Sie eine störende Aktion wie **Benutzer abmelden** und **Benutzer sperren** auf das Benutzerkonto anwenden, wenn eine ungewöhnliche Aktivität erkannt wird. Wenn eine Aktion auf das Konto des Benutzers angewendet wird, können die Dienste für sein Konto unterbrochen werden. In solchen Fällen muss der Benutzer den Administrator kontaktieren, um wie zuvor auf sein Konto zugreifen zu können.

Betrachten Sie einen Citrix Content Collaboration Benutzer, dessen Risikobewertung 80 in einer Dauer von 80 Minuten überschritten hat. Sie können den Benutzer abmelden. Sobald diese Aufgabe ausgeführt wurde, kann der Benutzer nicht auf sein Konto zugreifen und eine E-Mail-Benachrichtigung wird über die E-Mail-ID an den Benutzer gesendet `security-analytics@cloud.com`. Die E-Mail enthält Details des Ereignisses wie Aktivität, Gerät, Datum und Uhrzeit sowie die IP-Adresse. Der Benutzer muss sich wie zuvor an den Administrator wenden, um auf sein Konto zuzugreifen.



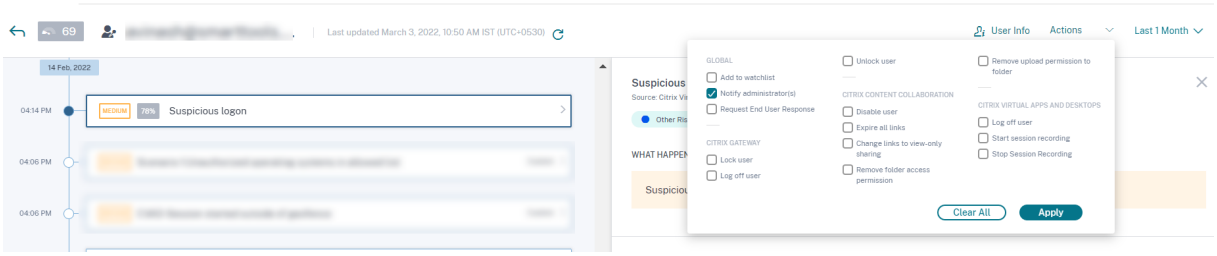
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Wenden Sie eine Aktion manuell an

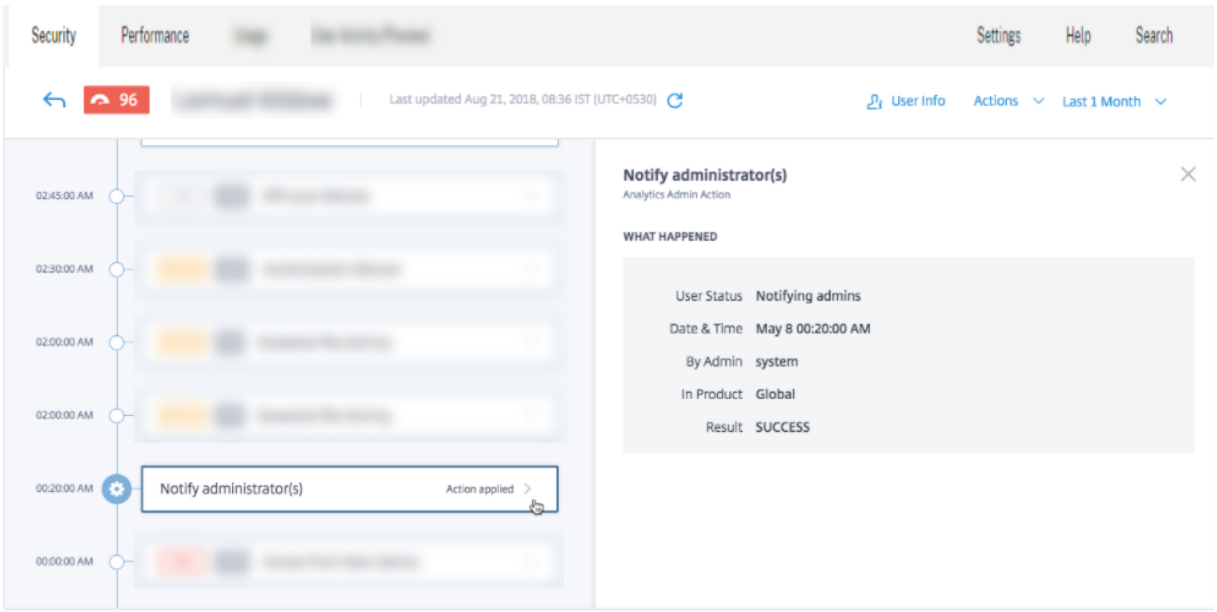
Stellen Sie sich einen Benutzer vor, Lemuel, der sich zum ersten Mal mit einem neuen Gerät bei einem Netzwerk anmeldet. Um ihr Konto zu überwachen, da ihr Verhalten ungewöhnlich ist, können Sie die Aktion **Administrator (n) benachrichtigen** verwenden.

Um die Aktion manuell auf den Benutzer anzuwenden, müssen Sie:

Navigieren Sie zum Profil eines Benutzers und wählen Sie den entsprechenden Risikoindikator aus. Wählen Sie im Menü **Aktionen** die Aktion **Administratoren benachrichtigen** aus und klicken Sie auf **Übernehmen**.



Eine E-Mail-Benachrichtigung wird an alle oder ausgewählte Administratoren gesendet, um ihr Konto zu überwachen. Die angewendete Aktion wird ihrer Risikozeitachse hinzugefügt, und die Aktionsdetails werden im rechten Fensterbereich der Risikozeitachse angezeigt.



Hinweise

- Wenn Sie ein Citrix Cloud-Administrator mit vollen Zugriffsberechtigungen sind, sind die E-Mail-Benachrichtigungen standardmäßig für Ihr Citrix Cloud-Konto deaktiviert. Um E-Mail-Benachrichtigungen zu erhalten, aktivieren Sie sie in Ihrem Citrix Cloud-Konto. Weitere Informationen finden Sie unter Empfangen von Benachrichtigungen per E-Mail.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> - Wenn Sie ein Citrix Cloud-Administrator mit benutzerdefinierten Zugriffsberechtigungen (schreibgeschützt und Vollzugriff) zur Verwaltung von Security Analytics sind, sind die E-Mail-Benachrichtigungen für Ihr Citrix Cloud-Konto aktiviert. Um keine E-Mail-Benachrichtigungen von Citrix Analytics mehr zu erhalten, bitten Sie Ihren Citrix Cloud-Administrator mit vollem Zugriff, Ihren Namen aus der Verteilerliste der Benachrichtigungsadministratoren zu entfernen. Weitere Informationen zu finden Sie unter E-Mail-Verteilerliste.

Richtlinien verwalten

Sie können das Richtlinien-Dashboard anzeigen, um alle in Citrix Analytics erstellten Richtlinien zu verwalten, um Inkonsistenzen in Ihrem Netzwerk zu überwachen und zu identifizieren. Im Dashboard Richtlinien können Sie:

1. Zeigen Sie die Liste der Richtlinien an
2. Einzelheiten der Richtlinie
    - Name der Richtlinie
    - Status —Aktiviert oder deaktiviert.
    - Dauer der Police —Anzahl der Tage, an denen die Police aktiv oder inaktiv war.
    - Vorkommnisse —Die Häufigkeit, mit der die Policy ausgelöst wird.
    - Geändert —Zeitstempel, nur wenn die Richtlinie geändert wurde.
3. Löschen Sie die Richtlinie
    - Um eine Richtlinie zu löschen, können Sie die Richtlinie auswählen, die Sie löschen möchten, und auf **Löschen**klicken.
    - Oder Sie können auf den Namen der Richtlinie klicken, um zur Seite Richtlinie ändern weitergeleitet zu werden. Klicken Sie auf **Richtlinie löschen**. Bestätigen Sie im Dialog Ihre Anfrage zum Löschen der Richtlinie.
4. Erstellen einer Richtlinie
5. Klicken Sie auf den Namen einer Richtlinie, um weitere Details anzuzeigen. Sie können die Richtlinie auch ändern, wenn Sie auf ihren Namen klicken. Andere Änderungen, die vorgenommen werden können, sind wie folgt:
    - Ändern Sie den Namen der Richtlinie.
    - Bedingungen der Richtlinie.
    - Die anzuwendenden Aktionen.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Aktivieren oder deaktivieren Sie die Richtlinie.
- Löschen Sie die Richtlinie.

> **Hinweis**
>
> - Wenn Sie Ihre Richtlinie nicht löschen möchten, können Sie die Richtlinie deaktivieren.
> - Gehen Sie wie folgt vor, um die Richtlinie im Richtlinien-Dashboard wieder zu aktivieren:
>   - On the Policies dashboard, click the **Status** slider button and refresh the page. The **Status** slider button turns green.
>   - On the Modify Policy page, click the **Enabled** slider button on the bottom of the page.

Unterstützte Modi

Citrix Analytics unterstützt die folgenden Richtlinienmodi:

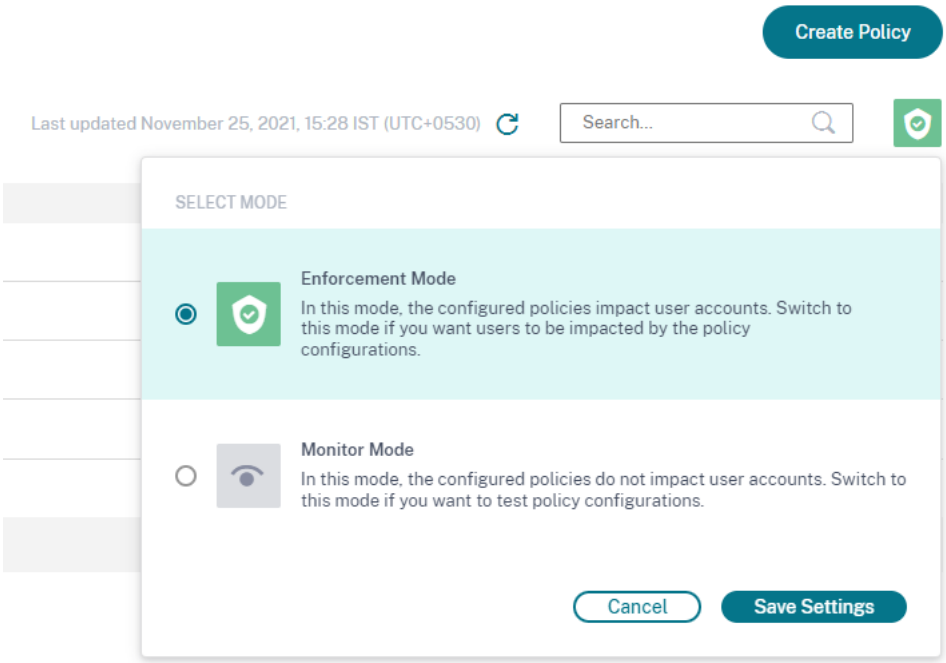
- **Durchsetzungsmodus** - In diesem Modus wirken sich die konfigurierten Richtlinien auf Benutzerkonten aus.
- **Überwachungsmodus** - In diesem Modus wirken sich die konfigurierten Richtlinien nicht auf Benutzerkonten aus. Sie können Richtlinien auf diesen Modus setzen, wenn Sie Richtlinienkonfigurationen testen möchten.

Verwenden Sie die folgenden Anweisungen, um Modi für Richtlinien zu konfigurieren:

1. Navigieren Sie zu **Sicherheit** > **Richtlinien**.
2. Wählen Sie auf der Seite **Richtlinien** das Symbol in der oberen rechten Ecke aus, das neben der **Suchleiste** angezeigt wird. Das Fenster **SELECT MODE** wird angezeigt.
3. Wählen Sie den Modus Ihrer Wahl aus und klicken Sie auf **Einstellungen speichern**.

> **Hinweis**
>
> Die von Analytics erstellten Standardrichtlinien sind auf den Überwachungsmodus eingestellt. Infolgedessen erben die bestehenden Richtlinien diesen Modus auch. Sie können die Auswirkungen aller Richtlinien gemeinsam beurteilen und dann in den Durchsetzungsmodus ändern.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Self-Service-Suche für Richtlinien

Auf der Self-Service-Suchseite können Sie die Benutzerereignisse anzeigen, die die in den Richtlinien definierten Bedingungen erfüllt haben. Auf der Seite werden auch die Aktionen angezeigt, die auf diese Benutzerereignisse angewendet wurden. Filtern Sie die Benutzerereignisse basierend auf den angewendeten Aktionen.

Vorkonfigurierte benutzerdefinierte Risikoindikatoren und Richtlinien

December 12, 2023

Citrix Analytics for Security bietet eine Liste vorkonfigurierter benutzerdefinierter Risikoindikatoren und eine Richtlinie, mit der Sie die Sicherheit Ihrer Citrix Infrastruktur überwachen können. Die Bedingungen dieser vorkonfigurierten benutzerdefinierten Risikoindikatoren und der Richtlinie sind bereits nach bestimmten Sicherheitsrisikoszenarien wie kompromittierten Benutzern, Insiderbedrohungen und Datenexfiltration definiert. Sie können diese vorkonfigurierten Bedingungen auch ändern oder Ihre eigenen Bedingungen entsprechend Ihren Sicherheitsanforderungen hinzufügen und die benutzerdefinierten Risikoindikatoren verwenden, um die Risiken zu mindern.

Derzeit sind die vorkonfigurierten benutzerdefinierten Risikoindikatoren für die folgenden Szenarien verfügbar:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Geofencing
- Zum ersten Mal Zugriff

Vorkonfigurierte benutzerdefinierte Risikoindikatoren für das Geofencing-Szenario

Verwenden Sie die folgenden vorkonfigurierten benutzerdefinierten Risikoindikatoren, um Benutzerereignisse von außerhalb der geografisch abgegrenzten Bereiche zu erkennen.

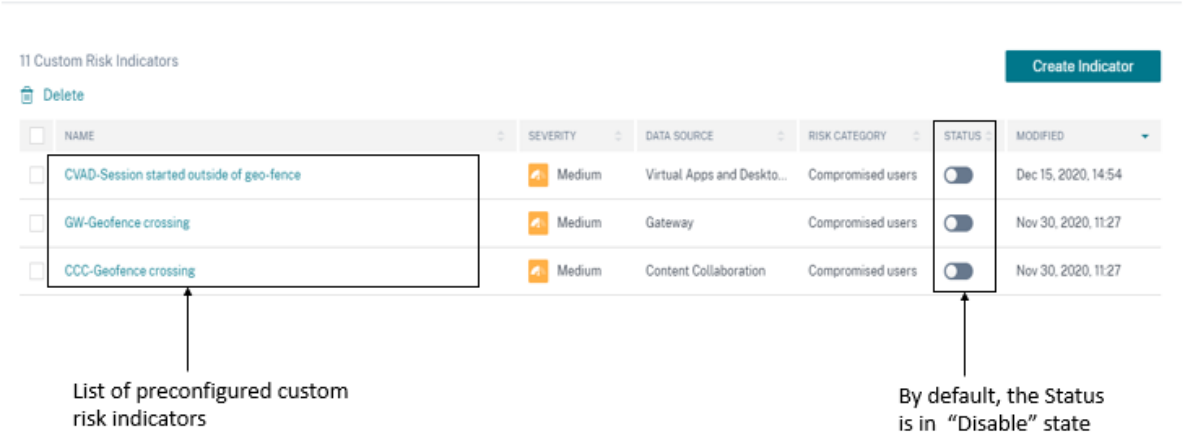
- CVAD-Sitzung begann außerhalb von Geofence
- GW-Geofence-Überfahrt

Die vorkonfigurierten benutzerdefinierten Risikoindikatoren werden ausgelöst, wenn Benutzer von außerhalb ihres üblichen Betriebslandes oder des Geofence auf die Citrix Produkte zugreifen. Standardmäßig ist der Geofence auf "Vereinigte Staaten"eingestellt. Sie können Ihr gewünschtes Land als Geofence festlegen.

> **Hinweis**
>
> Die *außerhalb des Geofence-Risikoindikators gestartete CVAD-Sitzung* ist mit den **Geofence-Einstellungen** der Funktion Access Assurance Location verknüpft. Sie können die Geofence-Länder also nicht direkt unter dem Zustand des Risikoindikators ändern. Um die Geofence-Länder im Risikoindikator zu aktualisieren, wählen Sie die Länder in den **Geofence-Einstellungen** des Dashboards Access Assurance Location aus. Weitere Informationen finden Sie im Dashboard für den Standort der Zugriffssicherung.

Um die vorkonfigurierten benutzerdefinierten Risikoindikatoren anzuzeigen, wählen Sie **Sicherheit > Benutzerdefinierte Risikoindikatoren**.

Standardmäßig sind die vorkonfigurierten benutzerdefinierten Risikoindikatoren deaktiviert. Verwenden Sie die Schaltfläche **STATUS**, um sie zu aktivieren.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

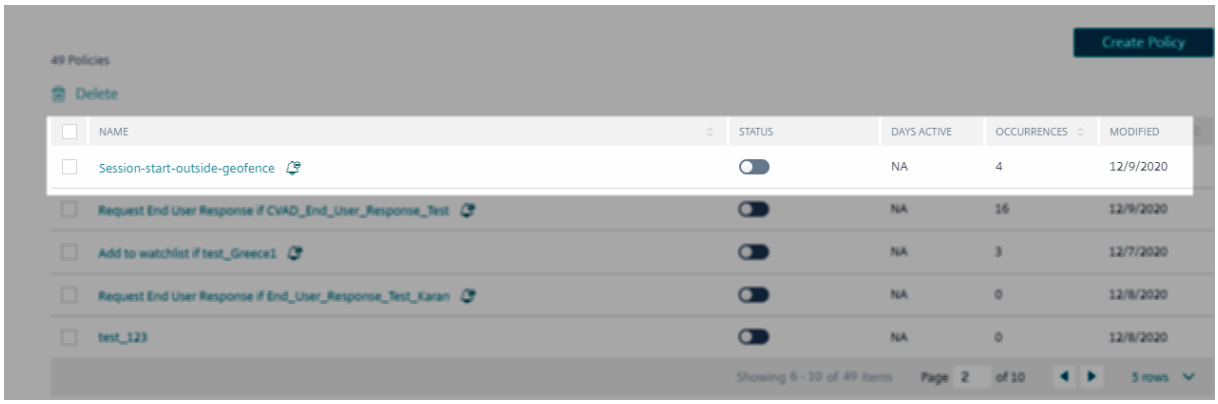
In der folgenden Tabelle werden die verschiedenen vorkonfigurierten benutzerdefinierten Risikoindikatoren für Geofencing beschrieben.

Name des benutzerdefinierten Risikoindikators	Szenario	Benutzerdefinierte Indikatorbedingungen	Datenquelle	Risiko-Kategorie
CVAD-Sitzung begann außerhalb von Geofence	Der Benutzer hat eine virtuelle Sitzung außerhalb seines Betriebslandes gestartet	Event-Type = Session.logon Country != “United States”	Citrix Workspace-App	Kompromittierte Benutzer
GW-Geofence-Überfahrt	Der Benutzer hat eine erfolgreiche Authentifizierung von außerhalb seines Betriebslandes	Event-Type = “VPN_AI”AND Country != “United States”	NetScaler Gateway (on-premises)	Kompromittierte Benutzer

Vorkonfigurierte Richtlinie für das Geofencing-Szenario

Citrix bietet eine vorkonfigurierte Richtlinie, die die Aktion **Endbenutzerantwort anfordern** auf ein Benutzerkonto anwendet, wenn der Benutzer eine virtuelle Sitzung außerhalb seines Betriebslandes startet. Der Benutzer erhält eine E-Mail und basierend auf der Antwort des Benutzers wird eine geeignete Maßnahme ergriffen, z. B. das Hinzufügen des Benutzers zur Beobachtungsliste oder die Benachrichtigung des Administrators über weitere Maßnahmen. Weitere Informationen finden Sie unter Endbenutzer-Antwort anfordern.

Um die vorkonfigurierte Richtlinie anzuzeigen, wählen Sie **Sicherheit > Richtlinien** aus.



In der folgenden Tabelle wird die vorkonfigurierte Richtlinie für Geofencing beschrieben.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Richtlinienname	Szenario	Bedingung der Richtlinie	Angewandte Aktion
Sitzungsstart außerhalb von Geofence	Möglichkeit für einen Administrator, die Legitimität des Benutzers durch die Aktion “Antwort des Endbenutzers anfordern”zu überprüfen, wenn der Benutzer die virtuelle Sitzung außerhalb seines Betriebslandes startet	Verwendung mit vorkonfiguriertem benutzerdefiniertem Risikoindikator - “CVAD-Sitzung wurde außerhalb von Geofence gestartet”	Antwort des Endbenutzers anfordern Basierend auf der Antwort des folgenden Benutzers wird die entsprechende Aktion angewendet Wenn der Benutzer die Aktivität nicht erkennt: **Zur Watchlist hinzufügen** Wenn der Benutzer die Aktivität erkennt: **Keine Aktion erforderlich** Wenn der Benutzer nicht innerhalb von 60 Minuten nach Erhalt der E-Mail antwortet: **Fügen Sie den Benutzer zur Watchlist**hinzu

> **Hinweis**
>
> Die Aktion “**Endbenutzer-Antwort anfordern** “wird nur in der Region USA unterstützt. Wenn Ihre Organisation in Citrix Cloud in die Region Europäische Union eingebunden ist, wird die

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> vorkonfigurierte Richtlinie nicht auf Ihr Konto angewendet. Um die vorkonfigurierte Richtlinie zu verwenden, ändern Sie die Richtlinie und wählen Sie eine andere Aktion Ihrer Wahl aus.

Erstellen Sie Ihre eigene Richtlinie mit vorkonfigurierten benutzerdefinierten Risikoindikatoren für Geofencing

Sie können mit diesen vorkonfigurierten benutzerdefinierten Risikoindikatoren auch Ihre eigenen Richtlinien erstellen und Aktionen wie das Sperren von Benutzern oder das Abmelden von Benutzern anwenden, wenn die Indikatoren ausgelöst werden. Informationen zum Erstellen von Richtlinien finden Sie unter Konfigurieren von Richtlinien und Aktionen.

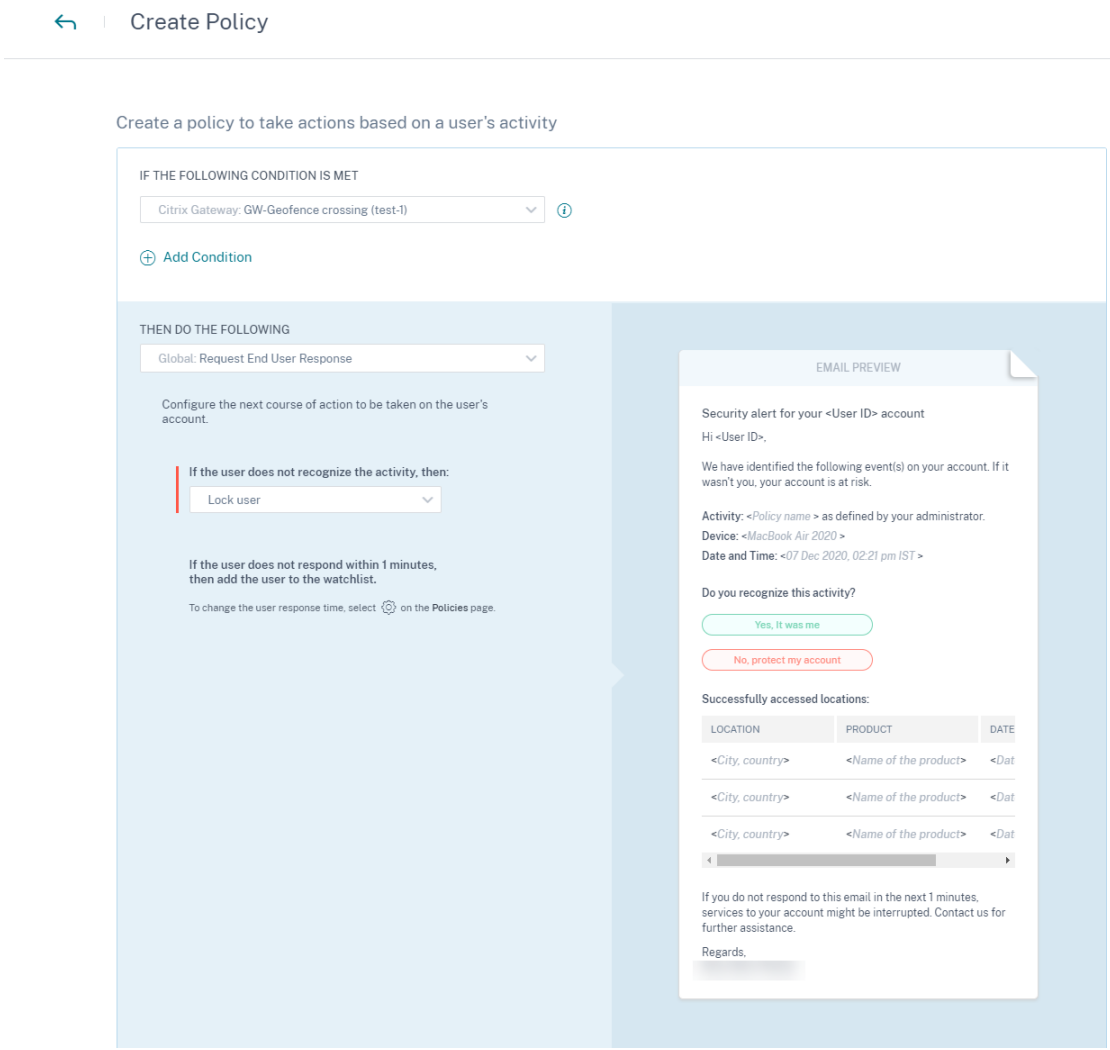
Das folgende Beispiel zeigt eine Richtlinie, die Benutzer sperrt, die versuchen, von außerhalb der USA auf Citrix-Dienste zuzugreifen. Der Benutzerzugriff ist gesperrt, wenn der Benutzer seine Zugriffsaktivität nicht erkennt.

Zustand: GW-Geofence crossing

Aktion: Antwort des Endbenutzers anfordern

Nächste Aktion: Sperren Sie den Benutzer, wenn der Benutzer die Aktivität nicht erkennt

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



> **Hinweis**
>
> Die Aktion "**Endbenutzer-Antwort anfordern** "wird nur in der Region USA unterstützt. Wenn Ihre Organisation also in die Region der Europäischen Union eingebunden ist, wählen Sie anstelle der Aktion "**Endbenutzer-Antwort anfordern** "eine andere Aktion Ihrer Wahl aus.

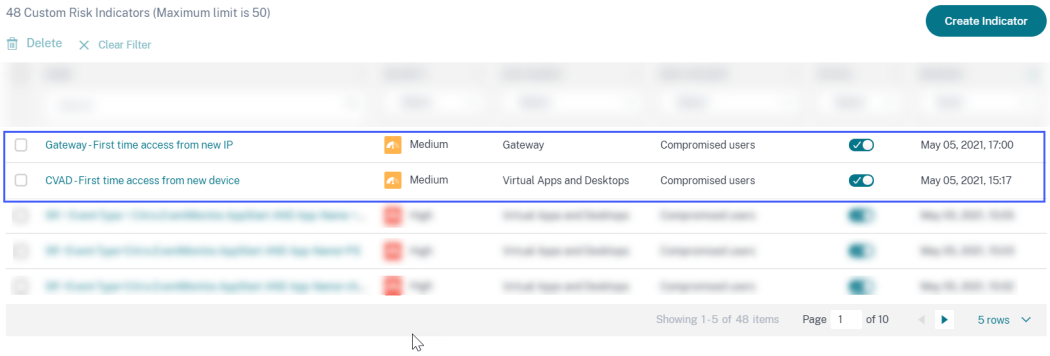
Vorkonfigurierte benutzerdefinierte Risikoindikatoren für das erste Zugriffsszenario

Verwenden Sie die folgenden benutzerdefinierten Risikoindikatoren, um Benutzerereignisse für Erstzugriffsszenarien zu erkennen:

- CVAD-Erstzugriff von neuem Gerät
- Gateway-Erstzugriff von neuer IP

Standardmäßig befinden sich diese vorkonfigurierten benutzerdefinierten Risikoindikatoren im Status "Aktiviert". Verwenden Sie die Schaltfläche **STATUS**, wenn Sie sie deaktivieren möchten.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



In der folgenden Tabelle werden die vorkonfigurierten benutzerdefinierten Risikoindikatoren für den ersten Zugriff beschrieben.

Name des benutzerdefinierten Indikators	Szenario	Vorkonfigurierte Bedingungen	Datenquelle	Risiko-Kategorie
CVAD-Erstzugriff von neuem Gerät	Wenn sich ein Benutzer der Citrix Workspace-App von einer der folgenden Optionen anmeldet Ein neues Gerät	Die folgenden Bedingungen sind standardmäßig aktiviert Das erste Mal für eine neue Geräte-ID.	Citrix Virtual Apps and Desktops on-premises und Citrix DaaS (früher Citrix Virtual Apps and Desktops Service)	Kompromittierte Benutzer

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Name des benutzerdefinierten Indikators	Szenario	Vorkonfigurierte Bedingungen	Datenquelle	Risiko-Kategorie
	Ein vorhandenes Gerät, das seit 90 Tagen nicht benutzt wurde.	`Event-Type = "Session.Logon"AND Client-Type IN ("XA.Receiver.Windows", "XA.Receiver.Mac", "XA.Receiver.Chrome", "XA.Receiver.Android", "XA.Receiver.Linux", "XA.Receiver.iOS")`		
Gateway-Erstzugriff von neuer IP	Wenn sich ein NetScaler Gateway-Benutzer erfolgreich von einer der folgenden Optionen anmeldet	Die folgenden Bedingungen sind standardmäßig aktiviert	Citrix Gateway	Kompromittierte Benutzer
	Eine neue öffentliche IP-Adresse	Das erste Mal für eine neue Client-IP		

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Name des benutzerdefinierten Indikators	Szenario	Vorkonfigurierte Bedingungen	Datenquelle	Risiko-Kategorie
	Eine vorhandene öffentliche IP-Adresse, die in den letzten 90 Tagen nicht verwendet wurde.	`Event-Type = "Authentication"AND Status-Code = "Successful login"AND Client-IP-Type != "private"AND Access-Insight-Flags = 1`		

In der Bedingungsleiste können Sie zusätzlich zu den vorkonfigurierten Bedingungen auch Ihre eigenen Bedingungen hinzufügen, um Bedrohungen gemäß Ihren Anforderungen zu identifizieren.

Wenn Sie beispielsweise die Benutzerereignisse aus einem bestimmten Land identifizieren möchten, können Sie die Länderdimension zusammen mit der vorkonfigurierten Bedingung hinzufügen:

- `Event-Type = "Session.Logon"AND Client-Type IN ("XA.Receiver.Windows", "XA.Receiver.Mac", "XA.Receiver.Chrome", "XA.Receiver.Android", "XA.Receiver.Linux", "XA.Receiver.iOS")AND Country = “United States”`
- `Event-Type = "Authentication"AND Status-Code = "Successful login" AND Client-IP-Type != "private"AND Access-Insight-Flags = 1 AND Country = “United States”`

E-Mail-Einstellungen für Endbenutzer

December 12, 2023

Die E-Mail-Einstellungen für Endbenutzer steuern die E-Mail-Vorlage, die mit der globalen Aktion Endbenutzer-Antwort anfordernverknüpft ist. Sie wenden diese Aktion an, um von den Benutzern

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

eine Antwort auf jede ungewöhnliche Aktivität zu erhalten, die in ihrem Konto festgestellt wurde. Die Benutzer antworten mit den E-Mails, die sie von Citrix Analytics for Security erhalten.

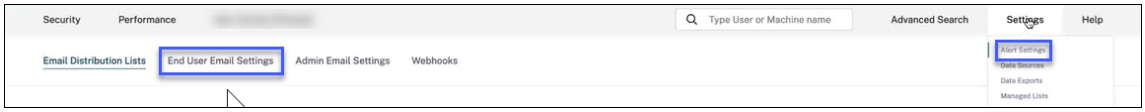
Sie können die E-Mail-Einstellungen verwenden, um:

- Fügen Sie ein passendes Banner, Kopfzeilentext und Fußzeilentext hinzu, um die Aufmerksamkeit des Benutzers zu erregen und seine Antwort zu erhalten. Dadurch sieht Ihre E-Mail auch legitimer aus.
- Fügen Sie eine Zeitdauer (in Minuten) hinzu, innerhalb derer der Benutzer auf Ihre E-Mail antworten muss. Wenn der Benutzer nicht innerhalb der Reaktionszeit antwortet, wendet Citrix Analytics die angegebene Aktion auf den Benutzer an.

E-Mail-Einstellungen ändern

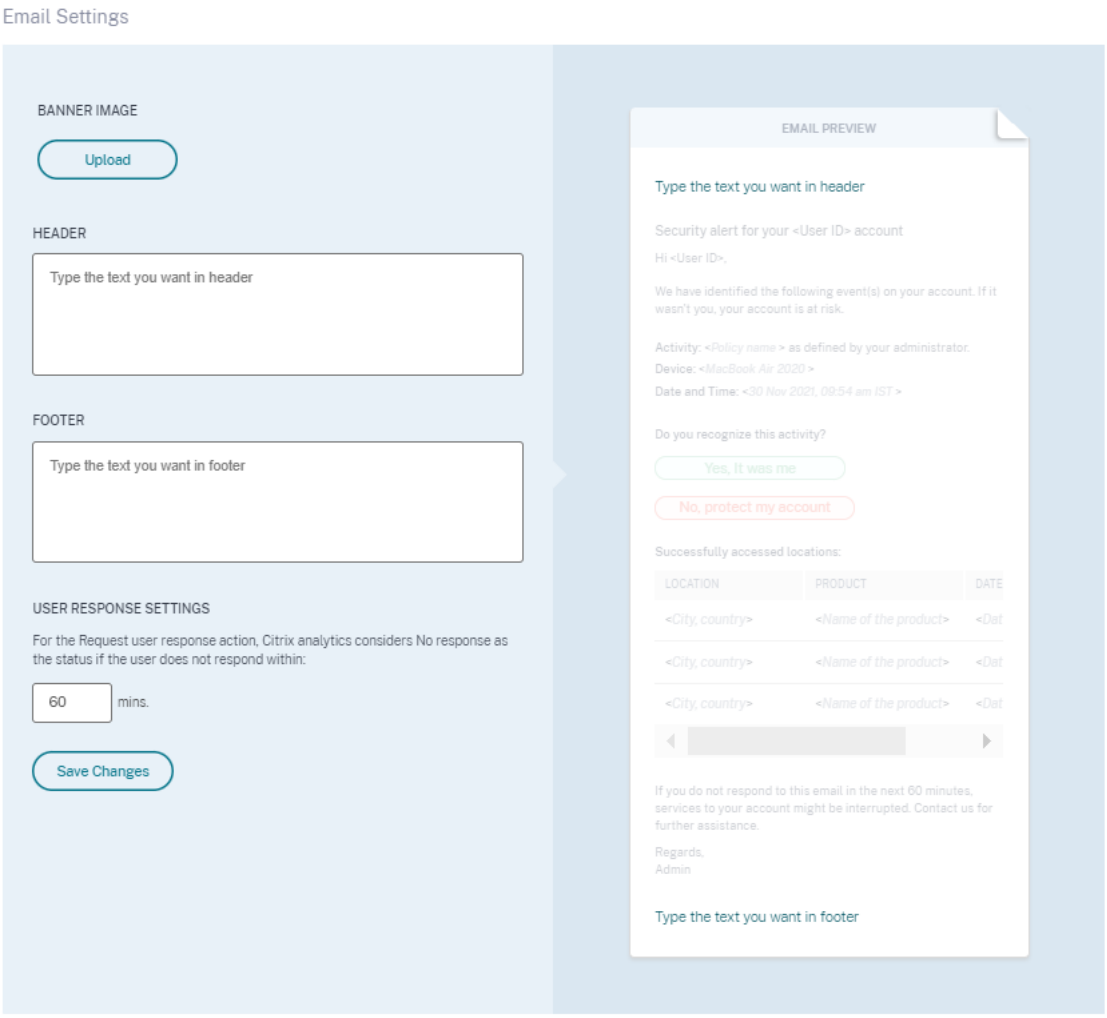
So ändern Sie die E-Mail-Einstellungen:

1. Klicken Sie in der oberen Leiste auf **Einstellungen > Warnungseinstellungen > E-Mail-Einstellungen für Endbenutzer**.



2. Klicken Sie auf Bearbeiten, um ein Bannerbild hochzuladen oder zu durchsuchen. Stellen Sie beim Hochladen einer Bilddatei sicher, dass das Image die folgenden Anforderungen erfüllt:
    - Unterstützte Formate: JPEG oder PNG
    - Maximale Abmessungen: 400* 100 Pixel
    - Maximale Dateigröße: 5 MB
3. Geben Sie Ihre Texte in die Felder **HEADER** und **FOOTER** ein. Diese Felder sind optional.
4. Geben Sie die Uhrzeit in den Einstellungen für die Benutzerantwort ein.
5. Zeigen Sie eine Vorschau der E-Mail an und klicken **Sie auf Änderungen speichern**

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



E-Mail-Einstellungen für Administratoren

December 12, 2023

Auf der Seite **Admin Email Settings** können Sie benutzerdefinierte Verteilerlistenempfänger für Systemwarnungen konfigurieren. Dadurch wird sichergestellt, dass Administratoren Systemwarnungen erhalten, die für sie nützlich sind.

Die Funktion **Admin Email Settings** bietet die folgenden Funktionen:

Sehen Sie sich die Systemwarnungen, die E-Mail-Verteilerlisten an, die die Warnung erhalten, den letzten Benutzer, der die Warnungseinstellungen geändert hat, und das Datum, an dem die Warnung zuletzt geändert wurde.
Ändern Sie die Warnungseinstellungen. Ändern Sie die Zielverteilerliste für verschiedene Systemwar-

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

nungen.

Warnungseinstellungen ändern

So ändern Sie die Warnungseinstellungen:

1. Klicken Sie in der oberen Leiste auf **Einstellungen > Warnungseinstellungen > Admin Email Settings**.

2. Klicken Sie auf die Warnung, deren E-Mail-Verteilerliste Sie ändern möchten.
3. Wählen Sie in der Dropdownliste **E-Mail-Verteilerliste auswählen die Verteilerlisten aus, die die** Warnung erhalten müssen.
   Sie können auch Ihre eigene Verteilerliste erstellen, indem Sie auf **E-Mail-Verteilerliste erstellen**klicken. Weitere Informationen finden Sie unter E-Mail-Verteilerliste erstellen.
4. Klicken Sie auf **Änderungen speichern**.

Watchlist

February 14, 2023

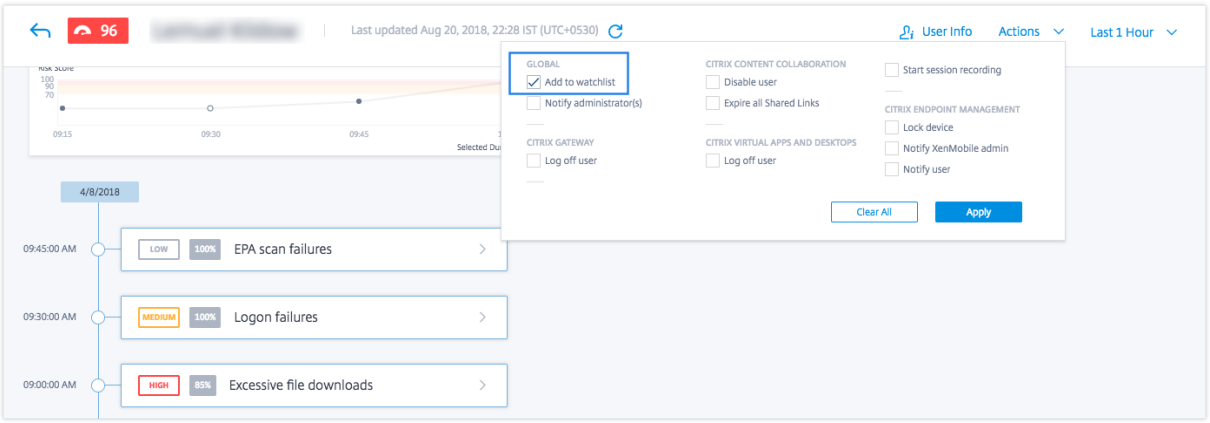
Verwenden Sie Beobachtungslisten, um die Aktivitäten bestimmter Benutzer im Hinblick auf potenzielle Bedrohungen zu überwachen. Sie können beispielsweise Benutzer überwachen, die keine Vollzeitbeschäftigten in Ihrer Organisation sind, oder Benutzer, die häufig einen bestimmten Risikoindikator auslösen.

Wie füge ich einen Benutzer zur Watchlist hinzu

Sie können entweder manuell einen Benutzer zur Watchlist hinzufügen, oder Sie können Richtlinien definieren, die, wenn sie ausgelöst werden, einen Benutzer zur Watchlist hinzufügen.

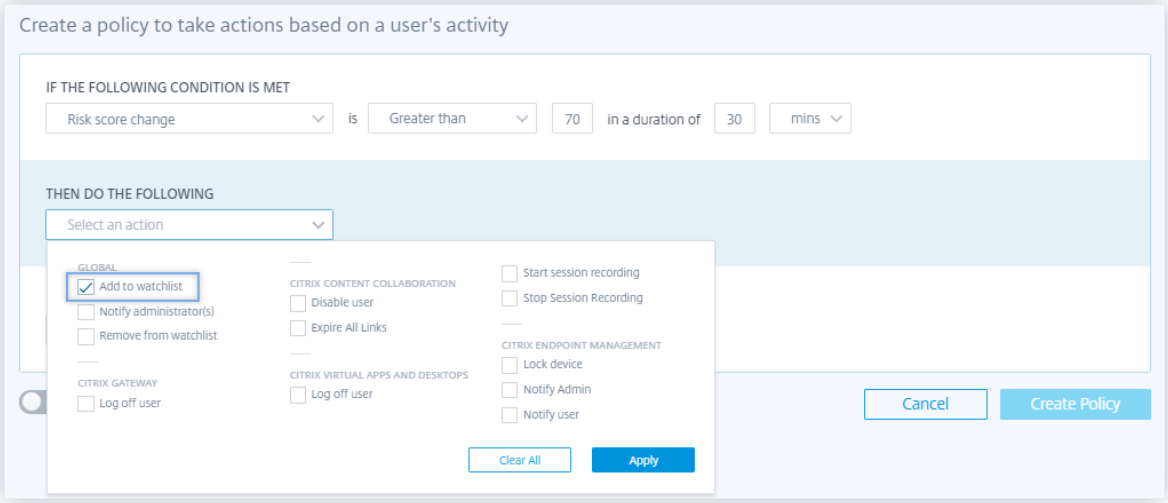
Um einen Benutzer manuell zur Beobachtungsliste hinzuzufügen, navigieren Sie in der Risiko-Timeline zum Benutzerprofil. Wählen Sie dann im Menü **Aktionen** die Option **Zur Beobachtungsliste hinzufügen**aus. Klicken Sie auf **Anwenden** und folgen Sie den Anweisungen, um die Aktion zu erzwingen.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Um einen Benutzer mithilfe von Richtlinien zur Watchlist hinzuzufügen, erstellen Sie eine Richtlinie mit einer Reihe von Bedingungen, die erfüllt sein müssen. Wählen Sie die Aktion **Zur Beobachtungsliste hinzufügen** aus. Wenn die Bedingungen erfüllt sind, wird der Benutzer zur Watchlist hinzugefügt. Beispielsweise möchten Sie möglicherweise einen Benutzer zur Beobachtungsliste hinzufügen, wenn die Änderung der Risikobewertung des Benutzers innerhalb von 30 Minuten um mehr als 70 erfolgt.

Weitere Informationen zum Erstellen von Richtlinien finden Sie unter Konfigurieren von Richtlinien und Aktionen.



So entfernen Sie einen Benutzer von der Watchlist

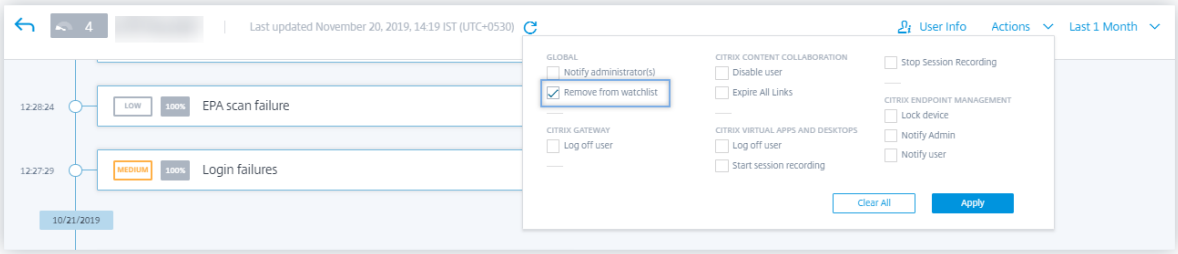
Sie können einen Benutzer entweder manuell aus der Watchlist entfernen, oder Sie können Richtlinien definieren, die, wenn sie ausgelöst werden, einen Benutzer aus der Watchlist entfernen.

Um einen Benutzer manuell von der Beobachtungsliste zu entfernen, navigieren Sie in der Risiko-Timeline zu seinem Profil. Wählen Sie dann im Menü **Aktionen** die Option Aus der **Beobachtungsliste**

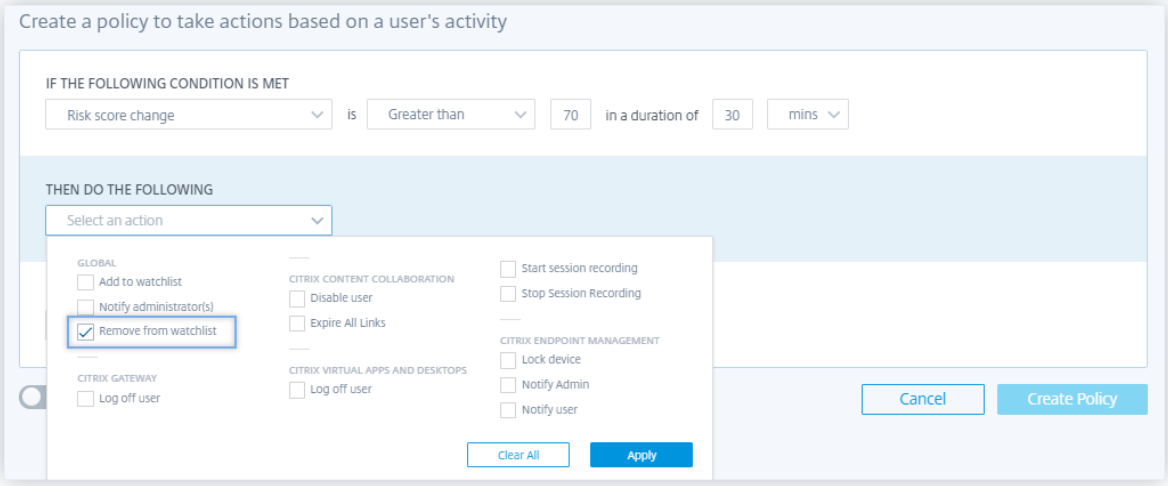
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

entfernen aus. Klicken Sie auf **Anwenden** und folgen Sie den Anweisungen, um die Aktion zu erzwingen.

> **Hinweis**
>
> Wenn ein Benutzer auf der Beobachtungsliste steht und Sie ihn entfernen möchten, wird im Menü **Aktionen** die Option **Aus der Beobachtungsliste entfernen** angezeigt.



Um einen Benutzer mithilfe von Richtlinien von der Watchlist zu entfernen, erstellen Sie eine Richtlinie mit einer Reihe von Bedingungen, die erfüllt sein müssen. Wählen Sie die Aktion **Aus der Beobachtungsliste entfernen** . Wenn die Bedingungen erfüllt sind, wird der Benutzer von der Watchlist entfernt. Beispielsweise möchten Sie möglicherweise einen Benutzer von der Beobachtungsliste entfernen, wenn die Änderung der Risikobewertung des Benutzers innerhalb von 60 Minuten weniger als 70 beträgt. Weitere Informationen zum Erstellen von Richtlinien finden Sie unter Richtlinien und Aktionen konfigurieren.



So überwachen Sie Benutzer in einer Watchlist

Sehen Sie sich im Dashboard **Sicherheit > Benutzer** Folgendes an:

- Zusammenfassung der Anzahl der Benutzer auf der Watchlist der letzten 13 Monate. Klicken Sie

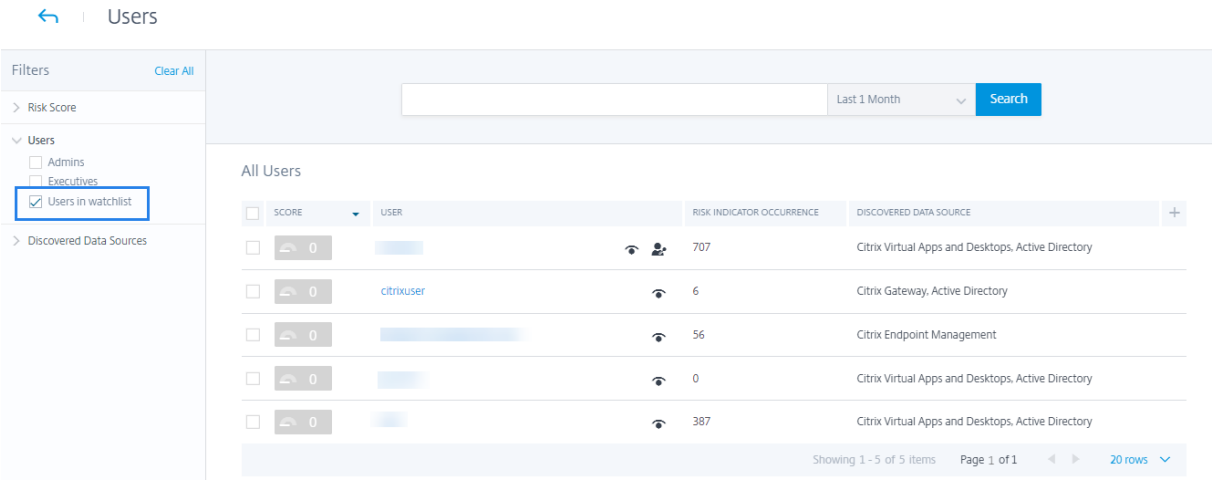
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

auf das Feld, um die Liste aller Benutzer in der Watchlist **im Bereich Benutzer auf der Watchlist** anzuzeigen.

- Die fünf besten Benutzer auf der Beobachtungsliste, basierend auf der Risikobewertung. Sehen Sie sich **im Bereich Benutzer auf der Beobachtungsliste** die Risikobewertung und das Vorkommen von Risikoindikatoren zusammen mit dem Namen des Benutzers an. Klicken Sie auf **Mehr** anzeigen, um die Liste aller Benutzer in der Watchlist auf der **Benutzerseite** anzuzeigen.
- Die riskantesten Benutzer, die auf der Watchlist stehen. Im Bereich **Riskante Benutzer** weist das „Auge"-Symbol neben einem Benutzer darauf hin, dass sich der Benutzer auf der Beobachtungsliste befindet.

Sehen Sie sich auf der Seite **Benutzer** die Liste aller Benutzer in der Watchlist an. Sehen Sie sich Details wie die Risikobewertung, die Anzahl der ausgelösten Risikoindikatoren und die zugehörigen Datenquellen für einen Benutzer an.

Verwenden Sie das Suchfeld, um Benutzer und deren Ereignisdetails zu finden. Wählen Sie den Zeitraum aus, um die Ereignisse der Risikoindikatoren für den bestimmten Zeitraum anzuzeigen.



Wöchentliche E-Mail-Benachrichtigung

December 12, 2023

Citrix Analytics sendet wöchentliche E-Mail-Benachrichtigungen, in denen die Sicherheitsrisiken in der IT-Infrastruktur Ihres Unternehmens zusammengefasst werden. Die wöchentliche Benachrichtigung informiert Sie über die riskanten Ereignisse und deren Ereignisse in der Vorwoche. Sie können herausfinden, ob Ereignisse Ihre Aufmerksamkeit oder Aktionen erfordern, ohne sich bei Citrix An-

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

alytics anzumelden. Diese Informationen halten Sie darüber auf dem Laufenden, was in Ihrem IT-Sicherheitsbereich passiert.

E-Mail-Benachrichtigungen aktivieren

- Wenn Sie ein Citrix Cloud-Administrator mit vollständiger oder benutzerdefinierter Zugriffsberechtigung sind, sind die E-Mail-Benachrichtigungen in Ihrem Citrix Cloud-Konto standardmäßig deaktiviert. Um E-Mail-Benachrichtigungen von Citrix Cloud-Diensten wie Citrix Analytics zu erhalten, aktivieren Sie die Benachrichtigungsoption in Ihrer Citrix Cloud. Weitere Informationen finden Sie unter Empfangen von Benachrichtigungen per E-Mail. Die Benachrichtigungseinstellungen sind für Administratoren, die über Active Directory/Azure AD-Gruppen hinzugefügt wurden, nicht verfügbar.
- Standardmäßig werden die E-Mail-Benachrichtigungen an die Standardliste der Citrix Sicherheitsadministratoren gesendet. Sie können dies ändern, indem Sie benutzerdefinierte Verteilerlistenempfänger für wöchentliche Benachrichtigungen konfigurieren. Weitere Informationen finden Sie unter E-Mail-Einstellungen für Administratoren.

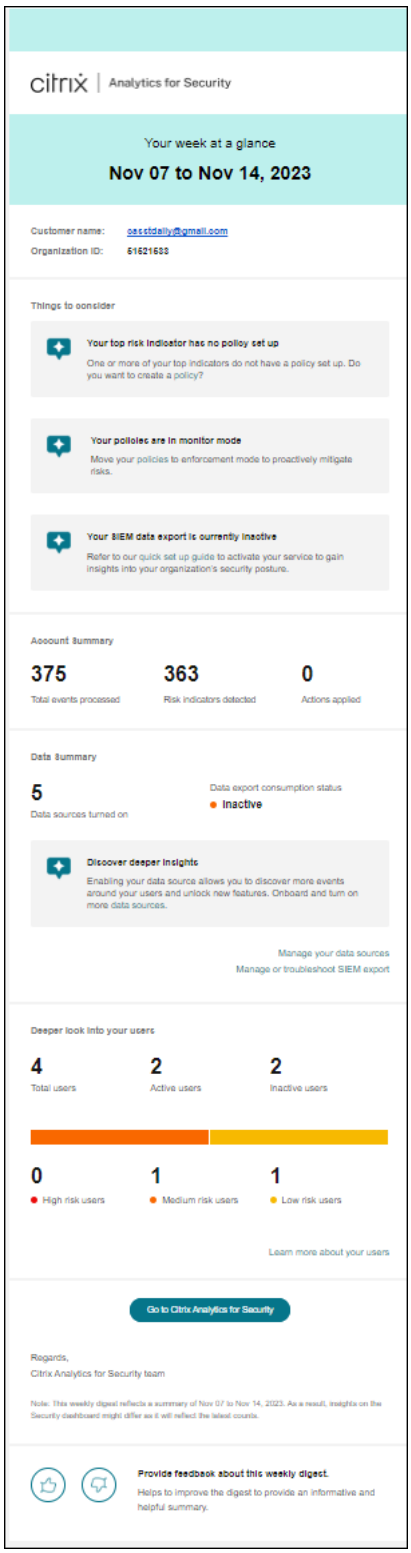
Wann erhalten Sie eine E-Mail von Citrix Analytics?

Jeden Dienstag wird Ihnen eine E-Mail-Benachrichtigung von Citrix Cloud gesendet < donotreplynotifications@citrix.com >.

Die E-Mail-Benachrichtigung enthält die folgenden Informationen:

- Zusammenfassung der Gesamtzahl der verarbeiteten Ereignisse, der erkannten Risikoindikatoren und der angewandten Maßnahmen
- Zusammenfassung der Gesamtzahl der aktiven Datenquellen und des Verbrauchsstatus des Datenexports
- Die drei wichtigsten Risikoindikatoren
- Die drei wichtigsten Maßnahmen im Zusammenhang mit den Risikoindikatoren
- Gesamtzahl der aktiven Benutzer und Gesamtzahl der riskanten Benutzer
- Alle Ereignisse oder Aktionen, die Ihre Aufmerksamkeit erfordern

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



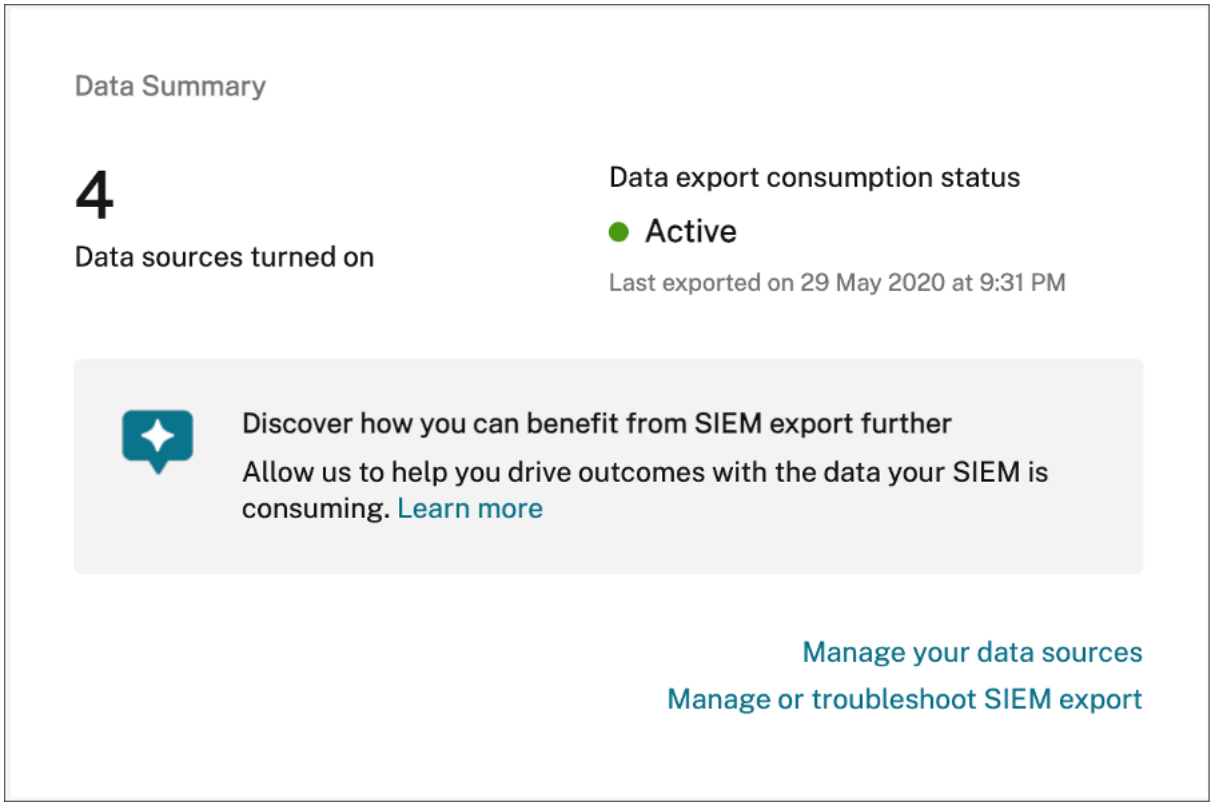
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Kontoübersicht

Die wöchentliche E-Mail enthält eine Zusammenfassung der Gesamtzahl der verarbeiteten Ereignisse, der erkannten Risikoindikatoren und der ergriffenen Maßnahmen.

Datenzusammenfassung

Die wöchentliche E-Mail bietet auch Einblicke in die aktivierten Datenquellen sowie den Status des Datenexportverbrauchs.



Klicken Sie in der E-Mail auf **Datenquellen verwalten**, um die Seite **Datenquellen** in Citrix Analytics aufzurufen. Sie können die Datenquelle einbinden und die Datenverarbeitung aktivieren, damit Citrix Analytics die Verarbeitung von Daten ermöglicht. Weitere Informationen zum Aktivieren von Analysen finden Sie unter Analytik für Datenquellen aktivieren .

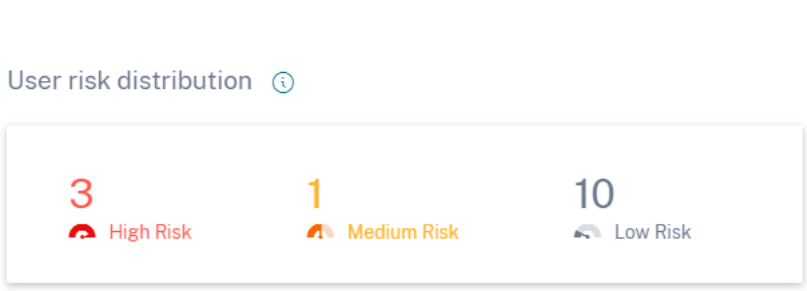
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Klicken Sie auf **SIEM-Export verwalten oder beheben**, um die Seite Datenexporte in Citrix Analytics anzuzeigen, auf der Sie Probleme in Ihrer Umgebung beheben und Ihre Datenexporteinstellungen verwalten können.

Informationen für Benutzer

Die wöchentliche E-Mail bietet Einblicke in die Gesamtzahl der Benutzer und Benutzer, die riskant gehandelt haben.

- **Anzahl der Benutzer mit hohem Risiko** —Rot gekennzeichnet. Sie stellen eine unmittelbare Bedrohung für die Organisation dar.
- **Zahl des mittleren Risikos** —Orange gekennzeichnet. Sie haben in der ausgewählten Woche mehrere schwerwiegende Verstöße auf ihrem Konto und müssen genau überwacht werden.
- **Anzahl der Benutzer mit geringem Risiko** —Gelb gekennzeichnet. Sie haben einige schwerwiegende Verstöße gegen ihr Konto, aber möglicherweise werden sie nicht als Bedrohung angesehen.



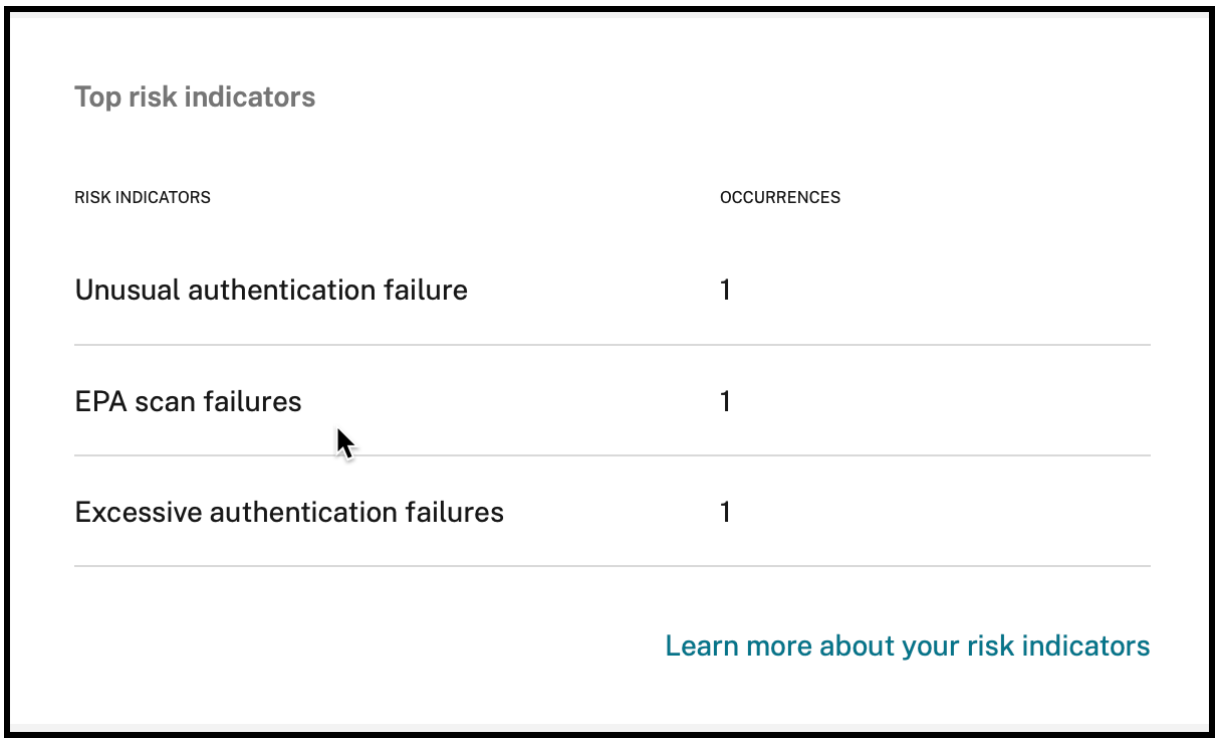
Weitere Informationen finden Sie unter Riskante Benutzer.

Klicken Sie auf **Erfahren Sie mehr über Ihre Benutzer**, um die Seite **Riskante Benutzer** in Citrix Analytics anzuzeigen. Sie können tiefere Einblicke in die aktiven Benutzer und die Risikokategorisierung erhalten.

Die wichtigsten Risikoindikatoren

Die wöchentliche E-Mail enthält Einblicke in die drei wichtigsten Risikoindikatoren und die Anzahl der Ereignisse in der ausgewählten Woche. Abhängig von der Anzahl der Ereignisse werden sowohl die standardmäßigen als auch die benutzerdefinierten Risikoindikatoren für die ausgewählte Woche angezeigt.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



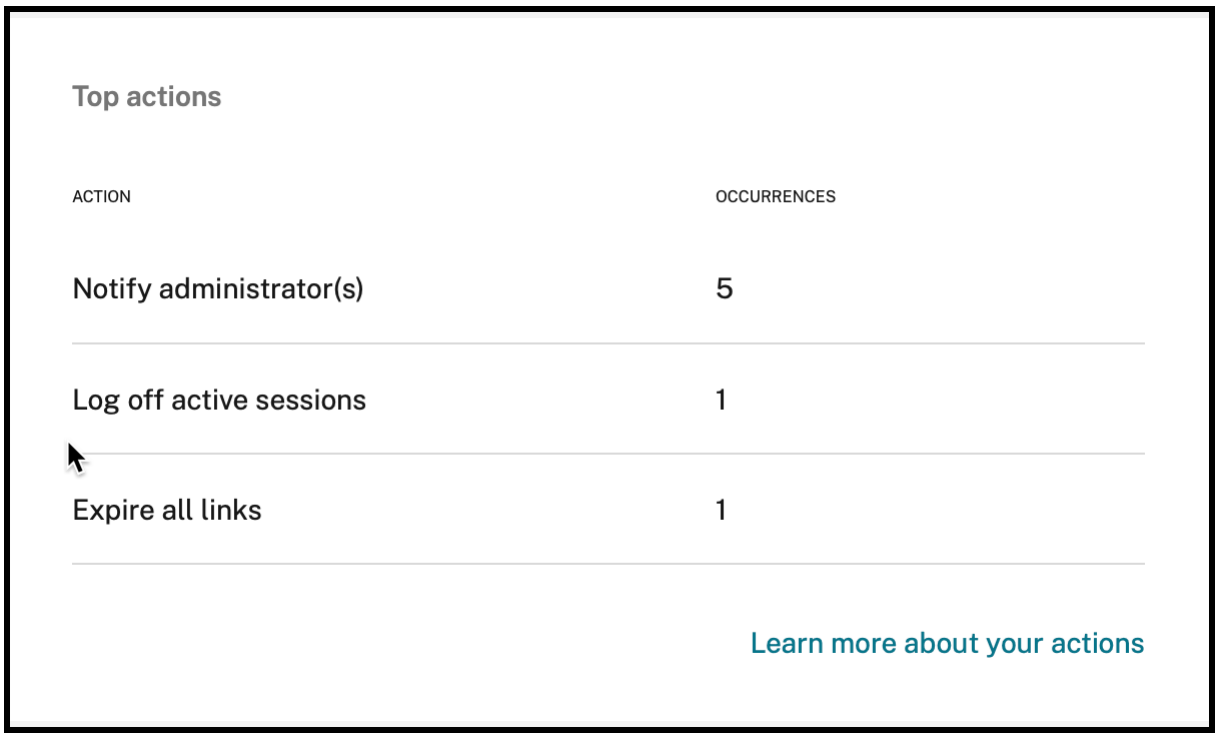
Weitere Informationen finden Sie unter Risikoindikatoren.

Klicken Sie in der E-Mail auf **Erfahren Sie mehr über Ihre Risikoindikatoren**, um die **Übersichtsseite mit den Risikoindikatoren** in Citrix Analytics aufzurufen.

Top Aktionen

Die wöchentliche E-Mail enthält Einblicke in die drei wichtigsten Maßnahmen, die als Reaktion auf die verdächtigen und ungewöhnlichen Bedrohungen der letzten Woche ergriffen wurden. Abhängig von der Anzahl der Ereignisse werden sowohl globale Aktionen als auch NetScaler Gateway-Aktionen für die ausgewählte Woche angezeigt.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



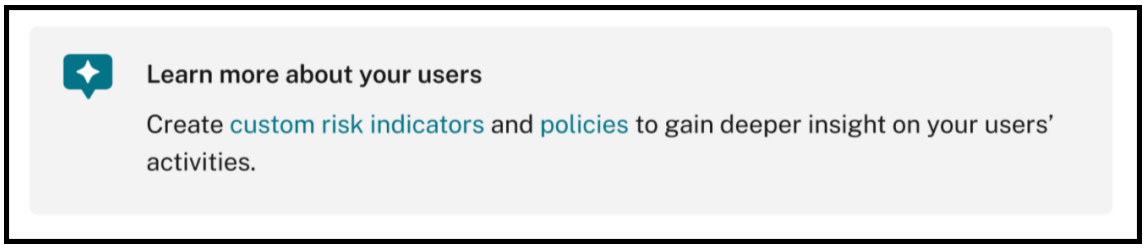
Weitere Informationen zu Aktionen und zum Konfigurieren einer Aktion finden Sie unter Richtlinien und Aktionen.

Klicken Sie in der E-Mail auf **Erfahren Sie mehr über Ihre Aktionen**, um die Seite mit den **wichtigsten Aktionen** in Citrix Analytics aufzurufen.

Welche Maßnahmen müssen Sie nach Erhalt der E-Mail ergreifen?

Mit wöchentlichen E-Mails können Sie herausfinden, ob Ereignisse oder Aktionen Ihre Aufmerksamkeit erfordern.

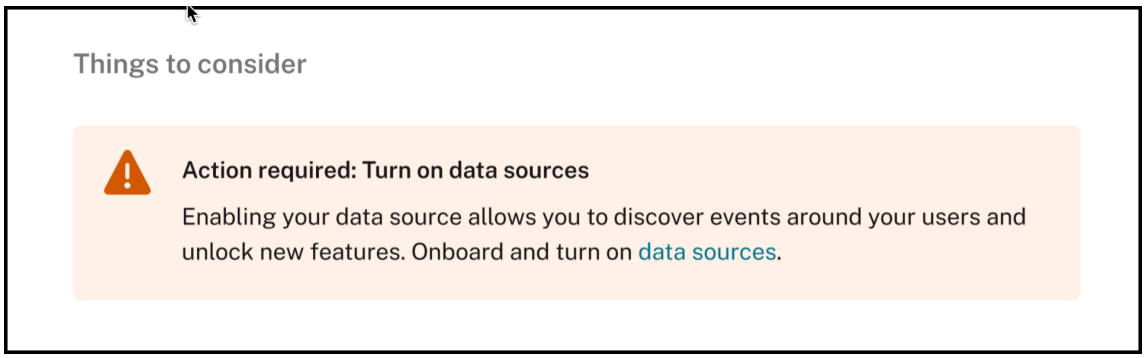
- Wenn für die Woche keine Risikoindikatoren erkannt wurden, erhalten Sie die folgende Meldung, in der Sie aufgefordert werden, weitere benutzerdefinierte Risikoindikatoren zu erstellen.



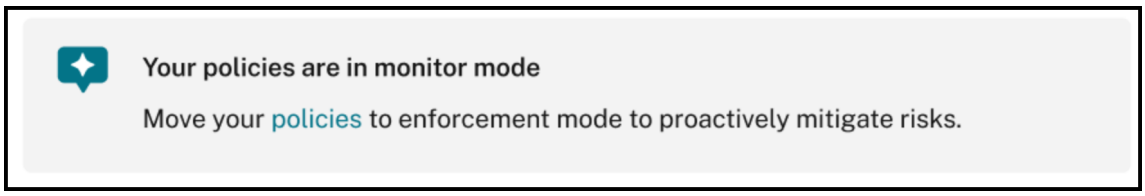
Sie können sich bei Citrix Analytics anmelden, um weitere benutzerdefinierte Risikoindikatoren zu erstellen.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

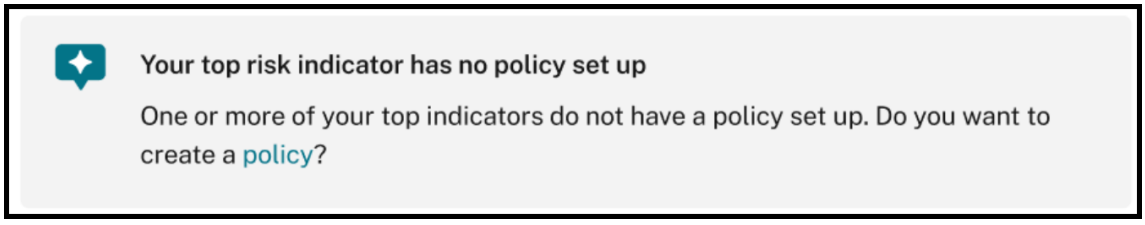
- Wenn keine der Datenquellen in Security Analytics aktiviert ist, wird die folgende Meldung angezeigt, in der Sie aufgefordert werden, die Datenverarbeitung für die Datenquellen zu aktivieren.



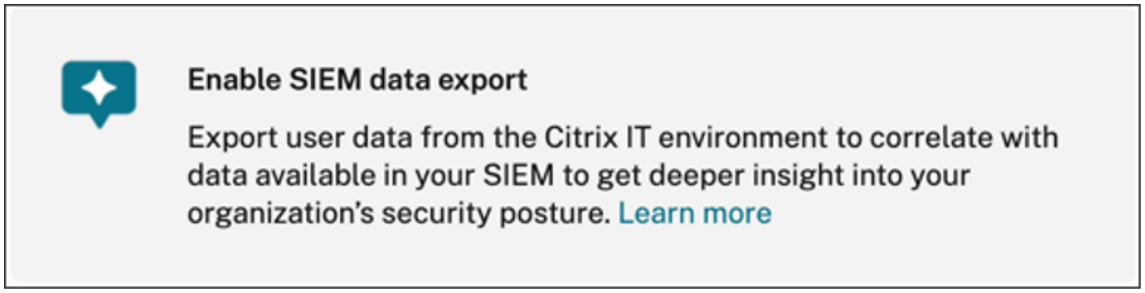
- Wenn sich keine der Richtlinien im Überwachungsmodus befindet, erhalten Sie die folgende Meldung, in der Sie aufgefordert werden, die Richtlinien in den Erzwingungsmodus zu versetzen.



- Wenn für einen der drei wichtigsten Risikoindikatoren der Woche keine Richtlinie festgelegt wurde, erhalten Sie die folgende Meldung, in der Sie aufgefordert werden, eine Richtlinie zu erstellen.



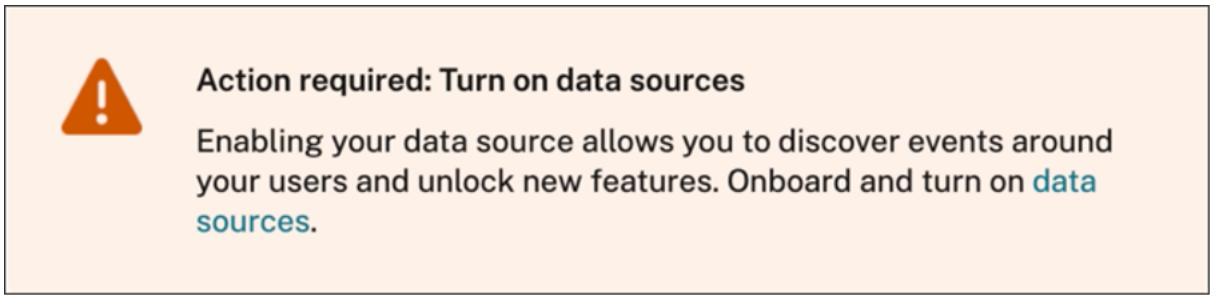
- Wenn Sie **Datenexporte** für Ihren Citrix Analytics-Mandanten nicht aktiviert haben, verweisen die folgenden Empfehlungen auf weitere Informationen zu unseren **Datenexportoptionen**, mit denen Sie Ihre Citrix-Daten in eine SIEM-Umgebung exportieren können.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Wenn der Datenexportverbrauchsstatus inaktiv ist, erhalten Sie die folgende Meldung, in der Sie aufgefordert werden, Ihren Dienst zu aktivieren.

> **Hinweis**
>
> Die Datenübertragung ist nur aktiviert, wenn die Datenverarbeitung für mindestens eine Datenquelle aktiviert ist. Wenn die Datenverarbeitung für alle Datenquellen deaktiviert ist, erhalten Sie die folgende Warnmeldung, um Ihre Datenquelle zu aktivieren.



Überwachungsprotokolle

February 6, 2020

In einem Überwachungsprotokoll werden Überwachungsinformationen für Ereignisse beschrieben, die in Citrix Analytics generiert werden. Hierbei kann es sich um Systemereignisse wie Fehler oder um einen Audit-Trail mit Konfigurationsaktionen handeln, die vom Citrix Analytics Administrator ausgeführt werden.

Wenn eine Konfiguration hinzugefügt, gelöscht oder aktualisiert wird, werden die Ereignisinformationen in das Überwachungsprotokoll geschrieben. Diese Informationen sind darüber, was geändert wurde, wann sie geändert wurde und wer sie geändert hat.

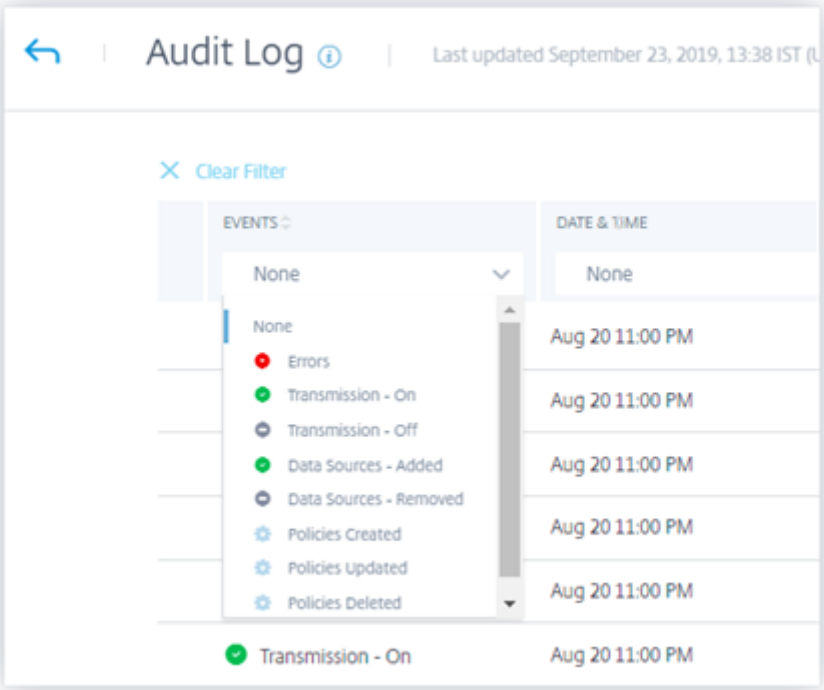
Sie können Überwachungsprotokollinformationen für die letzten drei Monate anzeigen.

Aktivitäten, die Überwachungsereignisse generieren

Die folgenden Ereignisse werden in Citrix Analytics registriert:

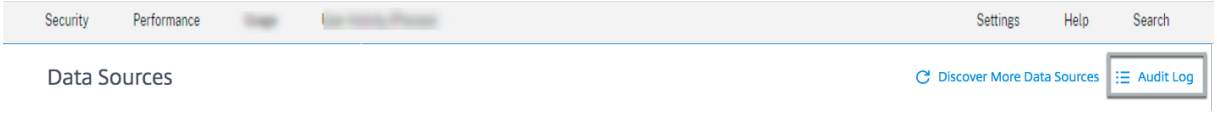
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Fehler generiert
- Übertragung eingeschaltet
- Übertragung ausgeschaltet
- Datenquellen hinzugefügt
- Datenquellen entfernt
- Erstellte Richtlinien
- Richtlinien aktualisiert
- Richtlinien gelöscht



Anzeigen des Überwachungsprotokolls

Melden Sie sich bei Citrix Analytics an, um Überwachungsprotokolle anzuzeigen. Navigieren Sie zu **Einstellungen > Datenquellen**. Klicken Sie auf der Seite **Datenquellen** oben rechts auf **Überwachungsprotokoll** .



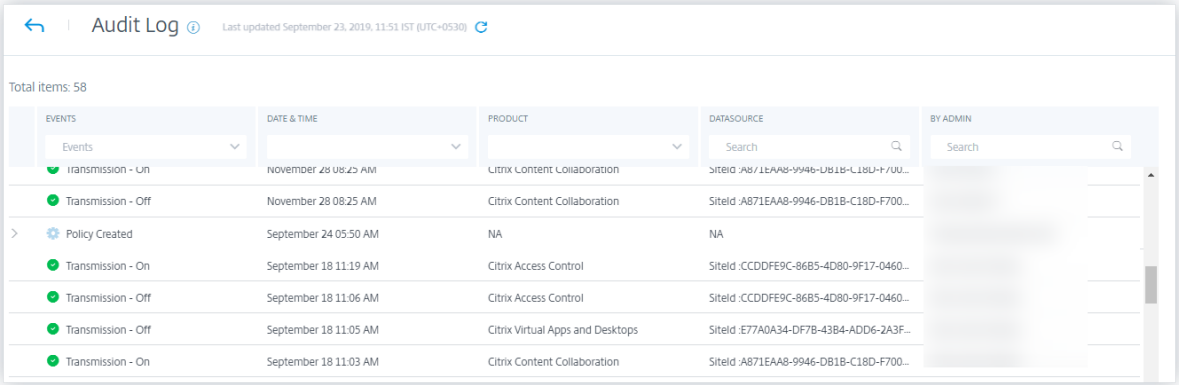
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Verwendung des Überwachungsprotokolls

Sie können das Überwachungsprotokoll verwenden, um Ereignisse in Citrix Analytics zu überprüfen und darauf zu achten. Aktualisieren Sie die Seite **Überwachungsprotokoll**, um die neuesten Überwachungsdaten abzurufen. Die Seite zeigt das Datum und die Uhrzeit an, zu der die Überwachungsdaten zuletzt aktualisiert wurden.

Sie können die folgenden Überwachungsinformationen auf der Seite **Überwachungsprotokoll** anzeigen. Sie können die Überwachungsdaten auch anhand dieser Felder filtern.

- **Ereignisse**. Ereignisse können vom Administrator auf Citrix Analytics generiert oder Konfigurationen angewendet werden. Ereignisse können auch Fehler darstellen, z. B. das fehlende Anwenden von Aktionen oder eine Datenquelle. Standardmäßig werden Protokolle für alle Ereignisse angezeigt. Sie können nach dem Ereignistyp filtern, das Sie anzeigen möchten.
- **Datum und Uhrzeit**. Die Daten und die Uhrzeit, zu der das Ereignis aufgetreten ist. Sie können nach dem Zeitraum filtern, für den Sie das Protokoll anzeigen möchten. Sie können Ereignisse für den aktuellen Tag, die letzten sieben Tage, die letzten 15 Tage, den letzten Monat und die letzten drei Monate anzeigen.
- **Produkt**. Das Produkt, für das das Ereignis generiert wurde. Die Ereignisse werden auf dem Produkt generiert und in Citrix Analytics aggregiert, wo sie angezeigt werden. Sie können das Protokoll anhand eines oder mehrerer Produkte filtern.
- **Datenquelle**. Der Name der Produktinstanz, die dem Überwachungseintrag zugeordnet ist. Sie können nach einer bestimmten Datenquelle suchen, um ihre Überwachungsdaten anzuzeigen.
- **Von Admin**. Der Citrix Analytics Administrator, der die Administratoraktivitäten ausgeführt hat. Sie können nach Aktivitäten suchen, die von einem bestimmten Administrator ausgeführt werden.

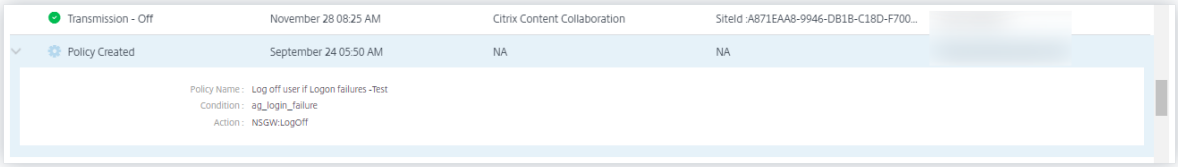


Wenn Ihr registriertes Ereignis auf einer Richtlinie basiert, können Sie auf das Pfeilsymbol klicken, um weitere Details anzuzeigen, z. B.:

- Richtlinienname

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Die angegebene Bedingung
- Die daraus resultierende Aktion



Benutzerdefinierte Berichte

June 18, 2024

Mithilfe der in Citrix Analytics for Security verfügbaren Ereignisse und Erkenntnisse können Sie benutzerdefinierte Berichte erstellen und planen. Benutzerdefinierte Berichte helfen Ihnen, Informationen von besonderem Interesse zu extrahieren und die Daten grafisch zu organisieren. Es hilft dabei, die Sicherheit der Datenquelle Ihrer Wahl im Laufe der Zeit zu analysieren.

Benutzerdefinierte Berichte unterstützen die folgenden Datenquellen:

- Apps und Desktops
- Gateway
- Secure Private Access
- Secure Browser
- Richtlinien
- Risikoindikatoren
- Risikobewertung

Unterstützte Felder in benutzerdefinierten Berichten

Einige Datenquellen sind auch in der Self-Service-Suche verfügbar. Um diese Ereignistypen und unterstützten Felder anzuzeigen, klicken Sie auf die folgenden Datenquellen.

- Apps und Desktops
- Gateway
- Secure Private Access
- Secure Browser
- Richtlinien

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Die folgenden Datenquellen sind nur in benutzerdefinierten Berichten verfügbar. In der folgenden Tabelle sind die unterstützten Felder in den benutzerdefinierten Berichten für die folgenden Datenquellen aufgeführt:

- Risikoindikatoren
- Risikobewertung

Datenquelle	Feld	Beschreibung
Risikoindikatoren	Kategorie	Gibt die Kategorie der Risikoindikatoren an. Die Risikoindikatoren sind in eine von vier Kategorien unterteilt: kompromittierte Endgeräte, kompromittierte Benutzer, Datenexfiltration oder interne Bedrohungen.
	Name des Risikoindikators	Der Name des Risikoindikators. Für einen benutzerdefinierten Risikoindikator wird der Name vom Administrator bei der Erstellung des Indikators definiert.
	Schweregrad	Gibt den Schweregrad des Risikos an. Es kann niedrig, mittel oder hoch sein.
	Benutzername	Der Benutzername oder die Domäne\ Benutzername, der für die Anmeldung verwendet wird.
Risikobewertung	Risiko-Score	Die dem Benutzer zugewiesene Risikobewertung. Die Risikobewertung variiert je nach Schweregrad der Bedrohung, die mit der Aktivität des Benutzers verbunden ist, zwischen 0 und 100.

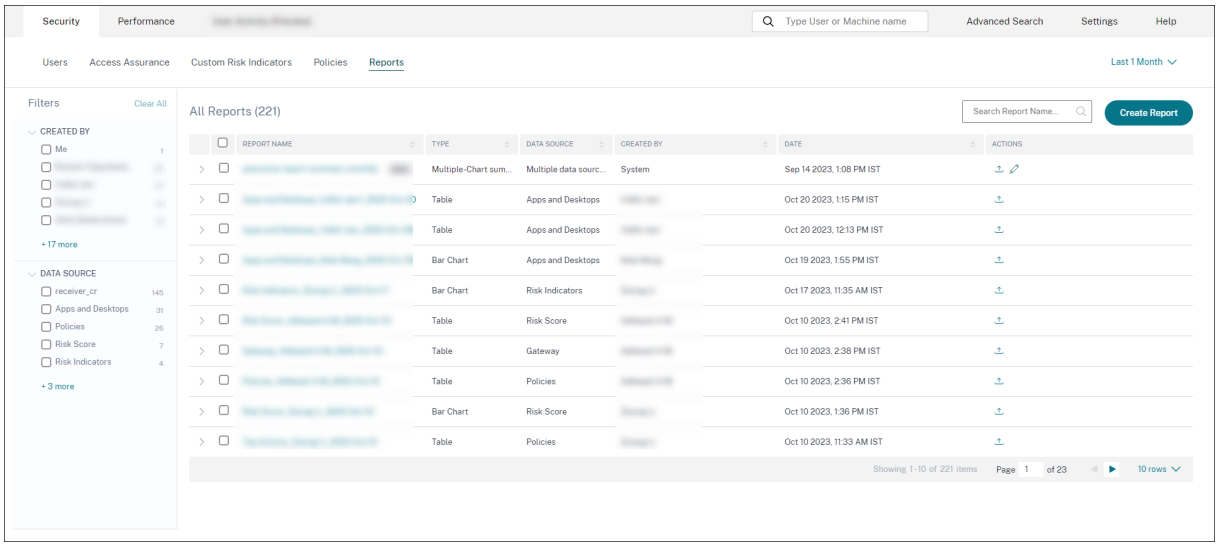
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Datenquelle	Feld	Beschreibung
	Benutzername	Der Benutzername oder die Domäne\ Benutzername, der für die Anmeldung verwendet wird.
	Risiko-Score-Kategorie	Basierend auf der Risikobewertung kann ein riskanter Benutzer in eine der folgenden Kategorien fallen: hohes Risiko, mittleres Risiko und niedriges Risiko.

Berichte

In dieser Ansicht können Sie die folgenden Aktionen für Berichte ausführen:

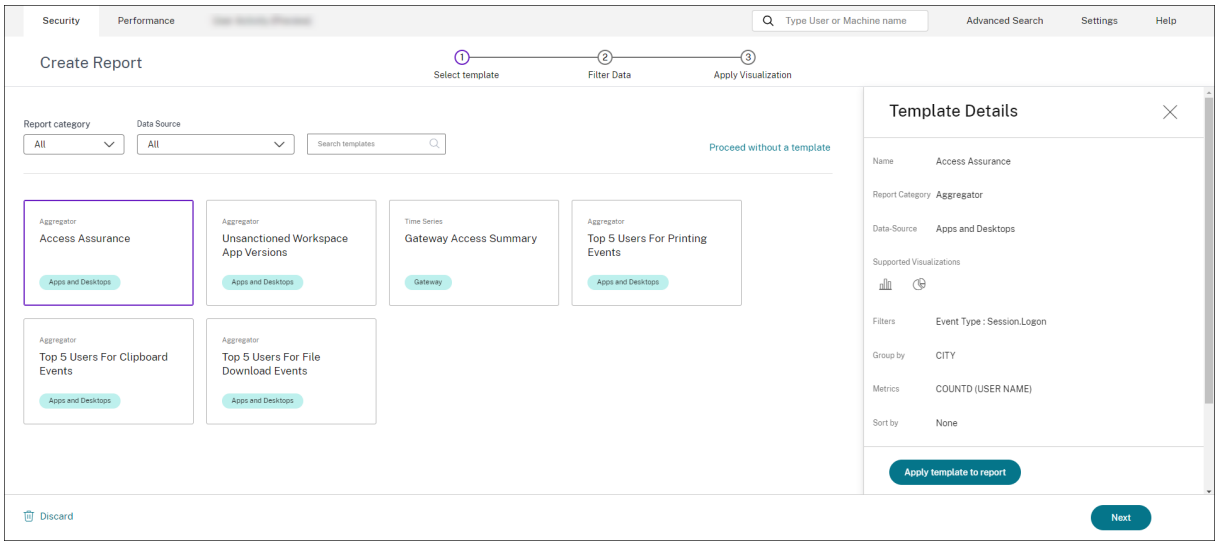
- Klicken Sie auf **Bericht erstellen**, um einen benutzerdefinierten Bericht zu erstellen.
- Erweitern Sie eine Zeile, um die Vorschau eines vorhandenen benutzerdefinierten Berichts zu sehen.
- Klicken Sie auf den Berichtsnamen, um die detaillierte Berichtsvisualisierung zu sehen.
- Klicken Sie auf das Exportsymbol, um einen vorhandenen benutzerdefinierten Bericht im PDF-Format zu exportieren.
- Klicken Sie auf das Bearbeitungssymbol, um die von Ihnen erstellten Berichte zu bearbeiten.
- Klicken Sie auf das Löschsymbol, um die von Ihnen erstellten Berichte zu löschen.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Erstellen Sie einen benutzerdefinierten Bericht

Um einen benutzerdefinierten Bericht zu erstellen, klicken Sie auf **Berichte erstellen**. Auf der Seite **Bericht erstellen** können Sie wählen, ob Sie einen benutzerdefinierten Bericht mit oder ohne Vorlagen erstellen möchten.

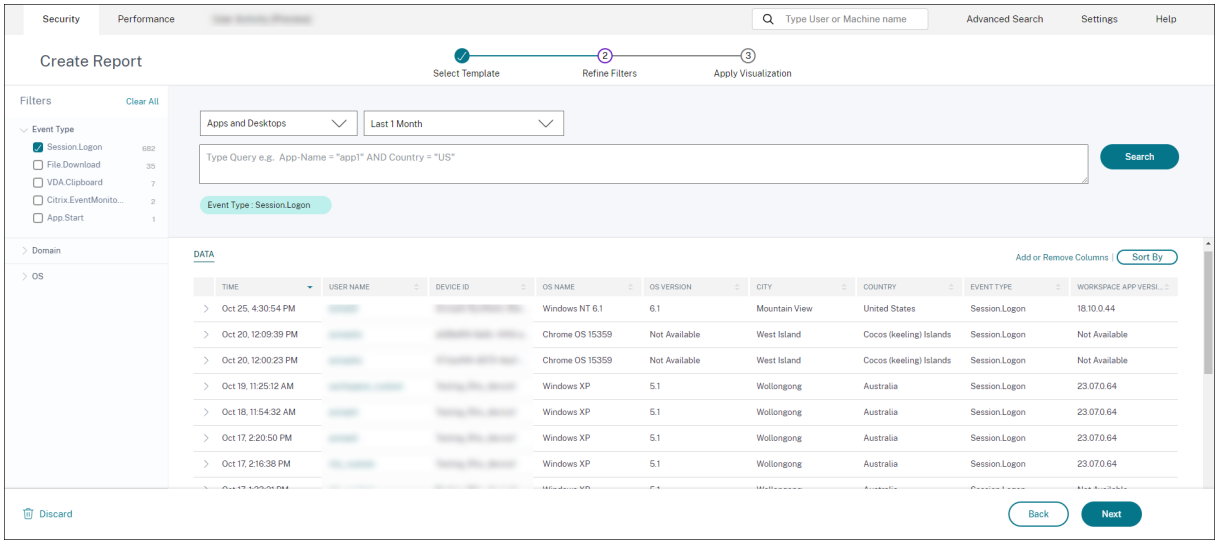


Erstellen eines benutzerdefinierten Berichts mit Vorlagen

So erstellen Sie einen benutzerdefinierten Bericht mit einer Vorlage:

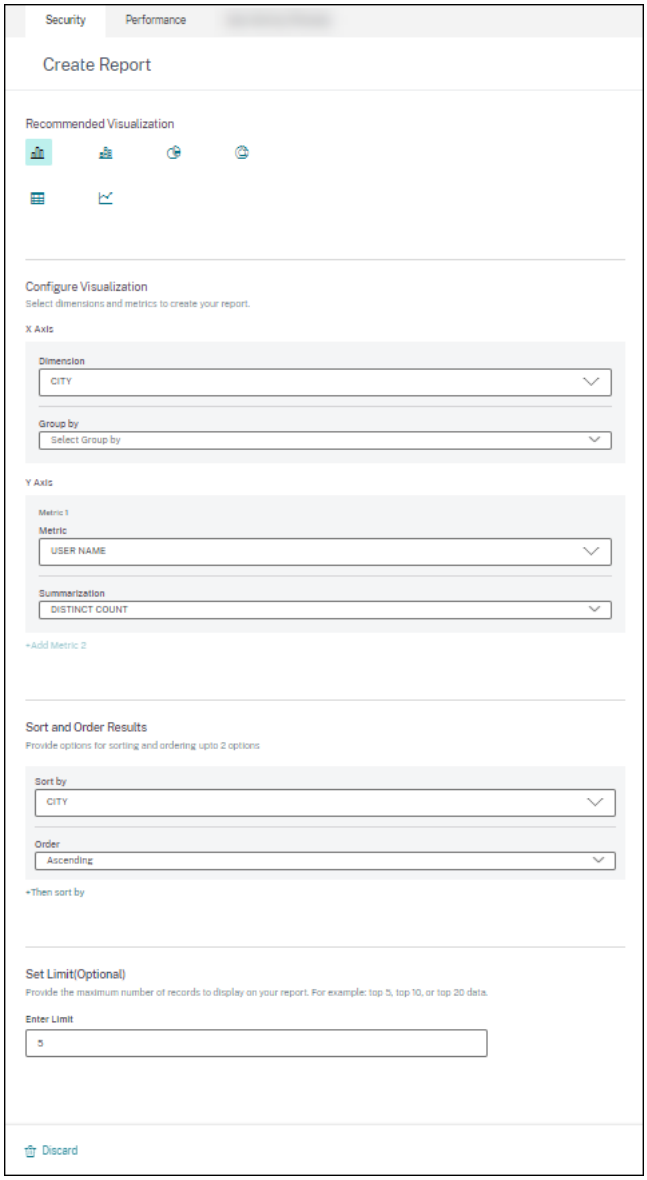
1. **Wählen Sie eine Vorlage**aus: Sobald Sie auf eine Vorlage geklickt haben, werden die Vorlagendetails auf der rechten Seite aufgeführt. Klicken Sie auf **Vorlage auf Bericht anwenden**, damit der Bericht die ausgewählte Vorlage verwenden kann.
2. **Filter verfeinern**: Auf der Seite **Filter verfeinern** werden die Filter angezeigt, die für die von Ihnen ausgewählte Vorlage vordefiniert waren. Nehmen Sie die erforderlichen Änderungen vor und klicken Sie dann auf **Weiter**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



1. **Visualisierung anwenden**: Wählen Sie eine der verfügbaren Visualisierungen für die Anzeige des Berichts aus.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



- **Balkendiagramm**: Stellt Daten mit vertikalen rechteckigen Balken dar, deren Höhe proportional zu den Werten ist. Wird für den Vergleich von Ereignissen verwendet.
- **Gestapeltes Säulendiagramm**: Stellt Daten in Form von übereinander gestapelten Balken dar. Wird verwendet, um die Gesamtsumme der Daten über mehrere Unterkategorien hinweg zu visualisieren.
- **Kreisdiagramm**: Stellt Daten in Form eines Kreises dar. Wird verwendet, um die relative Größe der Daten oder Prozentsätze zu visualisieren.
- **Ringdiagramm**: Stellt Daten in Form eines Ringes dar. Wird verwendet, um die relative Größe der Daten oder Prozentsätze zu visualisieren. - **Tabelle**: Präsentiert Daten in Form einer Tabelle. Wird verwendet, um so viele Dimensionen wie nötig zu visualisieren.
- **Liniendiagramm**: Stellt Daten mit Punkten dar, die durch gerade Liniensegmente miteinander verbunden sind. Wird verwendet, um Datentrends über einen bestimmten Zeitraum zu visual-

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

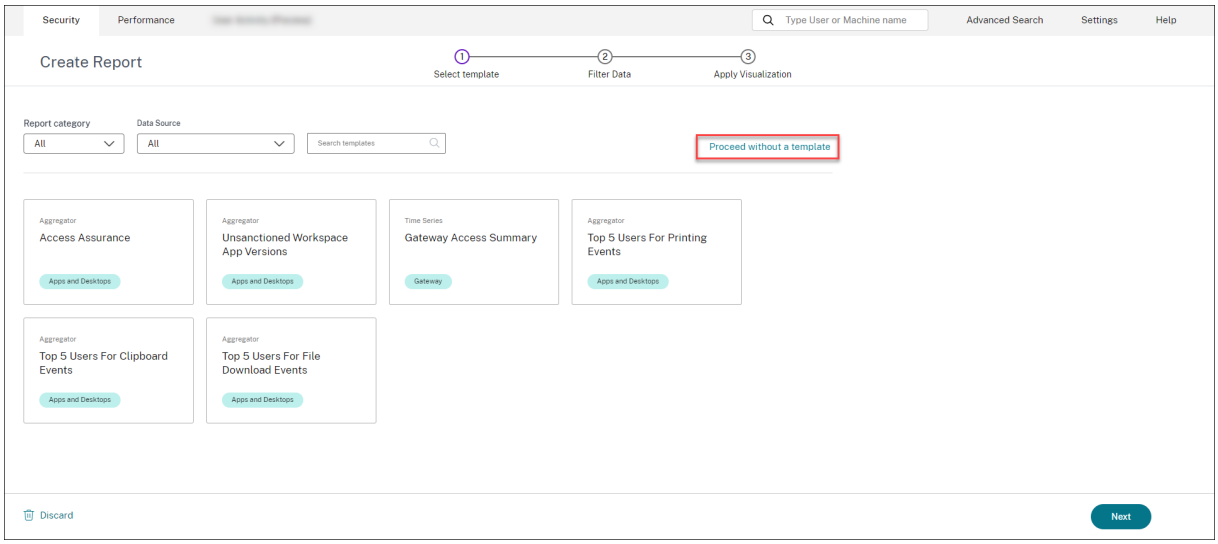
isieren.

1. Konfigurieren Sie nun die Visualisierung mit den folgenden Parametern:

    - Abmessung für die X-Achse
    - Metriken, die auf der Y-Achse dargestellt werden sollen
    - Zusammenfassung oder Aggregationen, wie Durchschnitt oder Anzahl, die auf die Metrik angewendet werden sollen
    - Optionen zum Sortieren und Ordnen
    - Eine optionale Grenze für die maximale Anzahl von Datensätzen, die im Bericht angezeigt werden sollen.

Erstellen eines benutzerdefinierten Berichts ohne Vorlagen

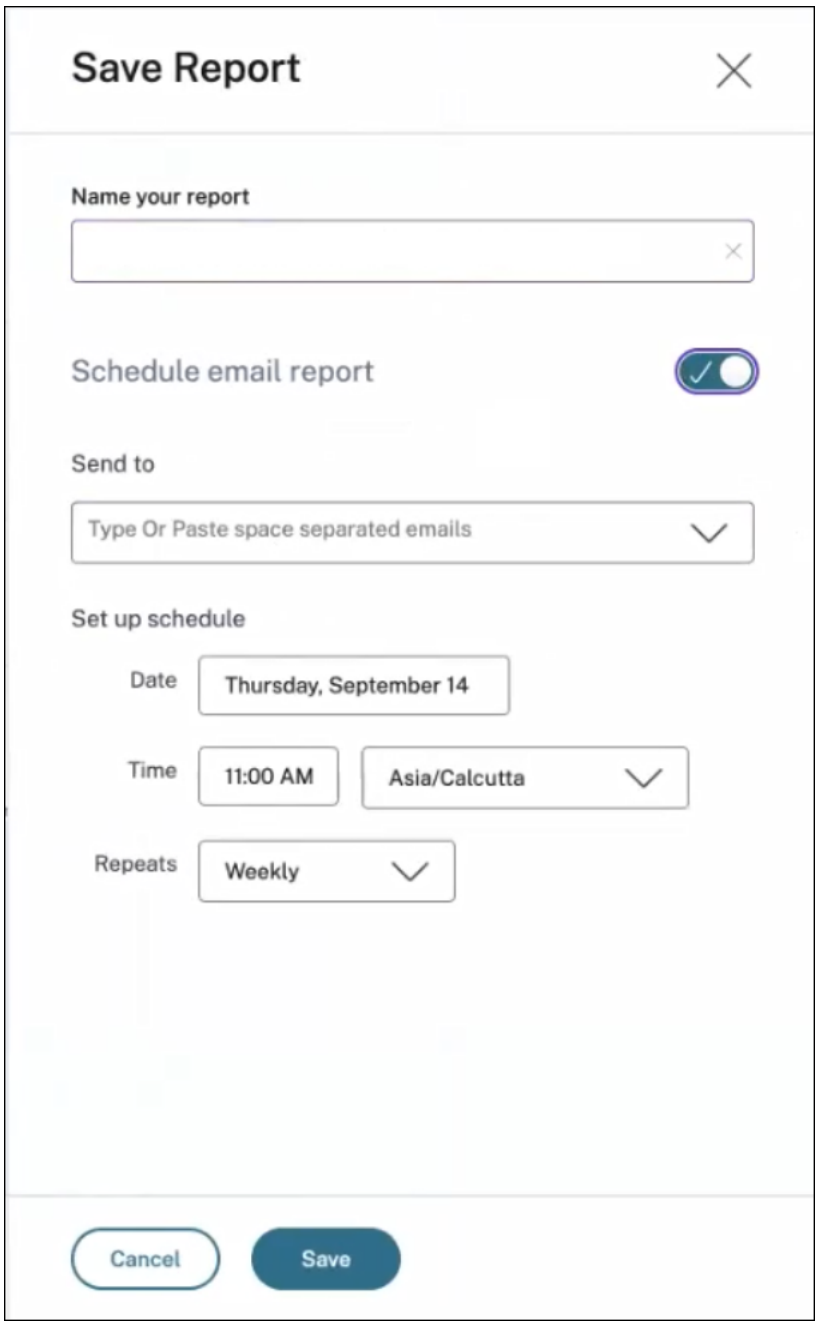
Sie können auch einen benutzerdefinierten Bericht ohne vordefinierte Vorlage erstellen. Klicken Sie auf **Benutzerdefinierten Bericht ohne Vorlage erstellen**. Wählen Sie eine Datenquelle aus der Dropdownliste aus. Folgen Sie den Schritten, um die Filter zu definieren, die Visualisierung anzuwenden, den Bericht zu speichern und zu planen.



Bericht speichern

1. Um den Bericht zu speichern, klicken Sie auf **Speichern**. Geben Sie einen Titel für Ihren Bericht an.
2. Sie können planen, den Bericht an die angegebenen E-Mail-IDs und Verteilerlisten an einem bestimmten Datum und zu einer bestimmten Uhrzeit oder nach einem wiederkehrenden Zeitplan per E-Mail zu senden.

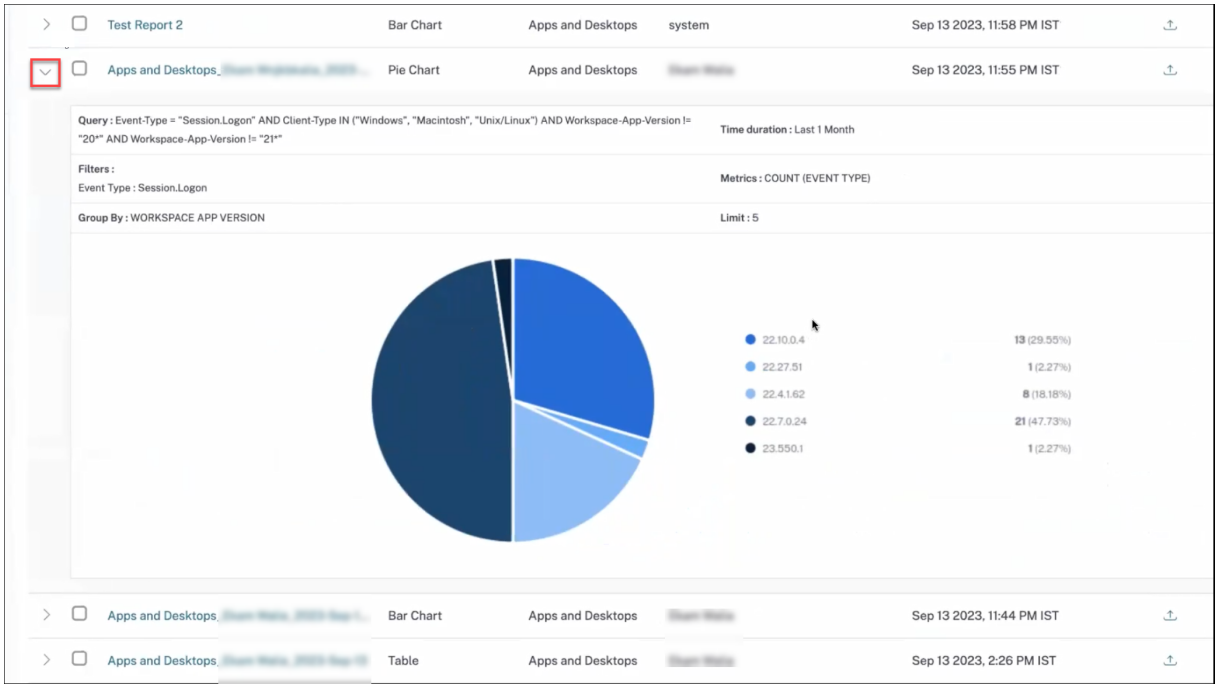
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Einen Bericht ansehen

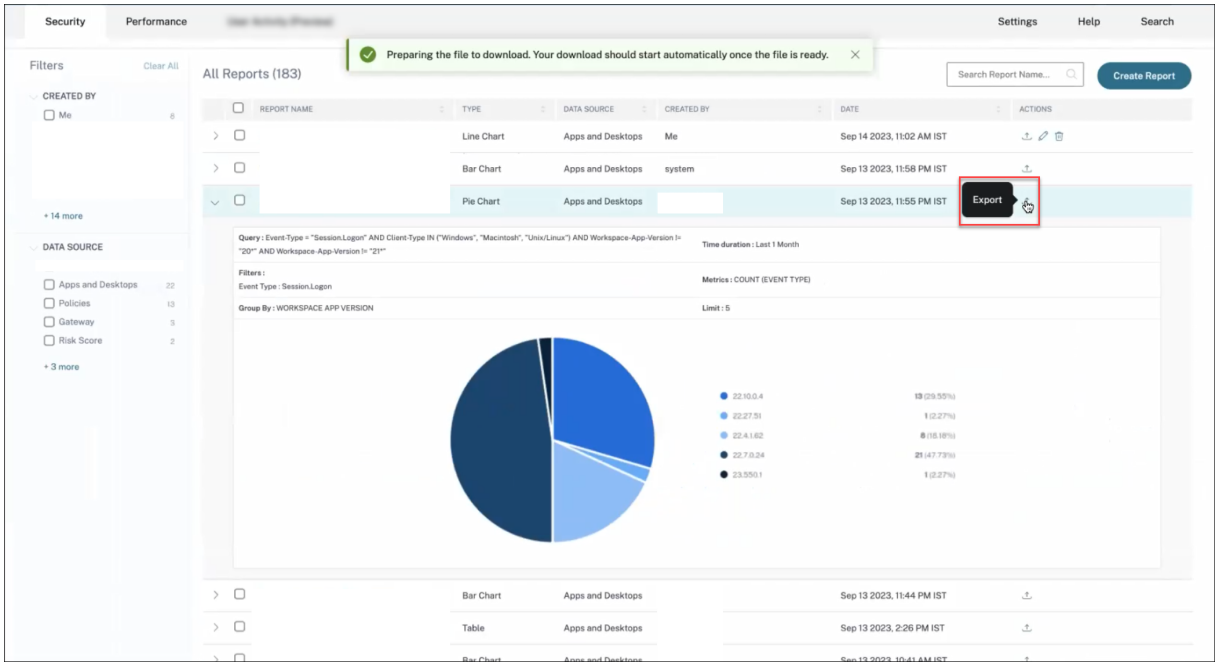
1. Nachdem Sie einen Bericht erstellt und gespeichert haben, können Sie den Bericht auf der Seite **Berichte** anzeigen. Sie können einen gespeicherten Bericht auch ändern oder löschen.
2. Klicken Sie auf die Dropdownschaltfläche, um eine Vorschau des Berichts anzuzeigen.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Exportieren eines Berichts

Klicken Sie auf das Exportsymbol, um den Bericht zu exportieren.

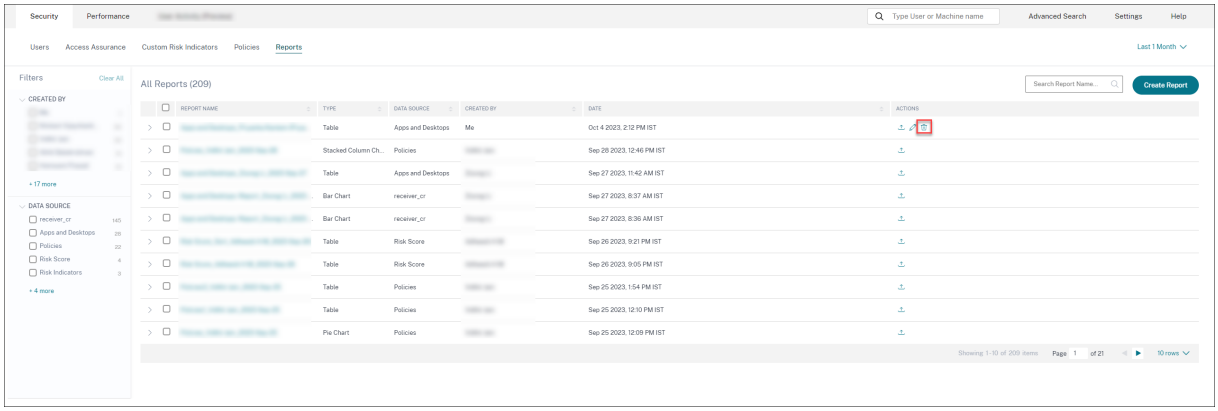


Einen Bericht löschen

Klicken Sie auf das Löschsymbol, um den Bericht zu löschen.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

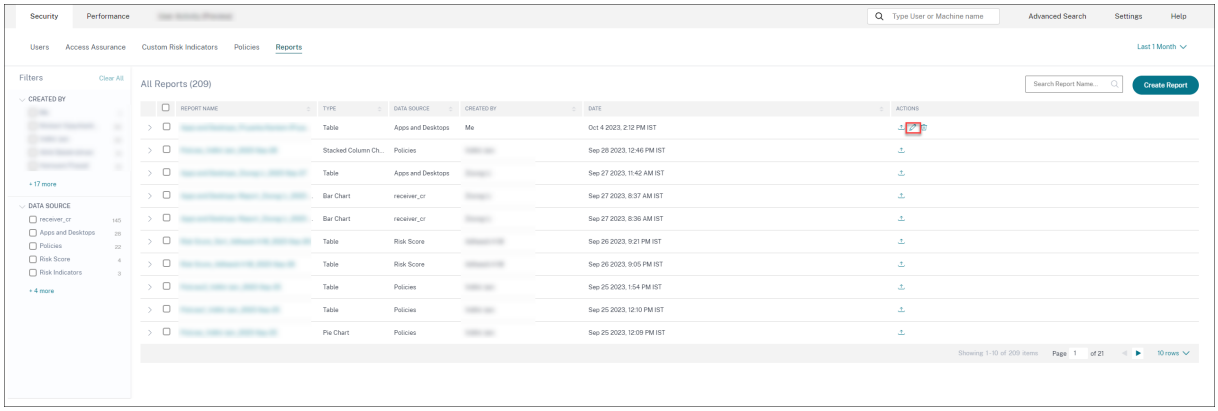
> Hinweis:
>
> Nur der Benutzer, der den Bericht erstellt hat, kann ihn löschen.



Einen Bericht bearbeiten

Klicken Sie auf das Bearbeitungssymbol, um den Bericht zu bearbeiten.

> Hinweis:
>
> Nur der Benutzer, der den Bericht erstellt hat, kann ihn bearbeiten.



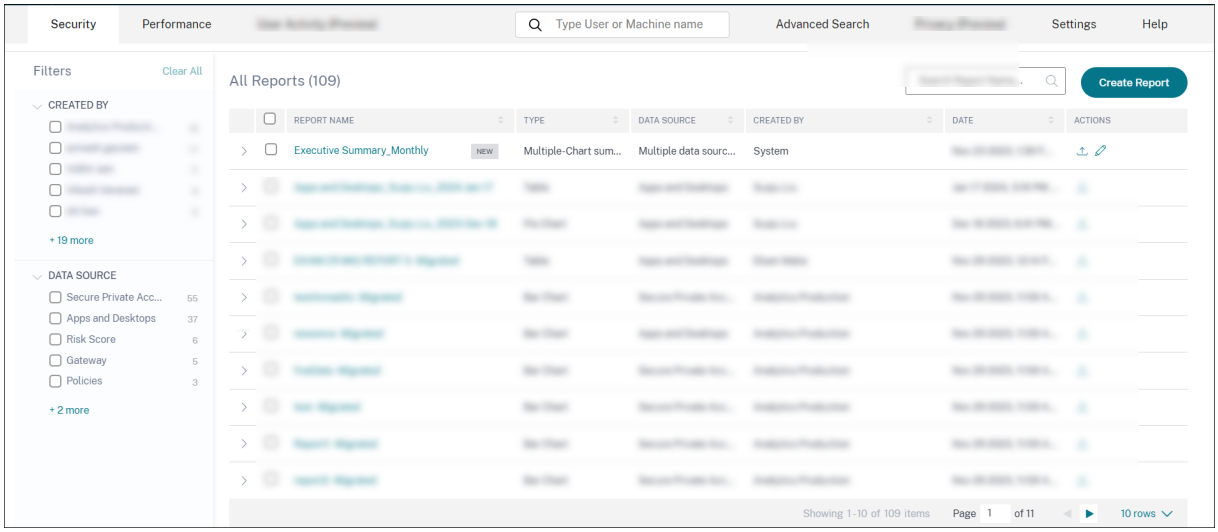
Zusammenfassender Bericht

Sie können einen automatisierten Export per E-Mail planen, der ein PDF eines vorab erstellten Zusammenfassungsberichts enthält. Der Executive Summary Report ist eine Sammlung von Berichten, in denen die Sicherheitslage Ihres Unternehmens für den ausgewählten Zeitraum auf einen Blick für das von Ihnen gewählte Publikum dargestellt wird.

Sie können den Bericht für Daten für die folgenden Zeiträume erstellen:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Letzte 1 Stunde
- Letzte 12 Stunden
- Letzter Tag
- Letzte 1 Woche
- Letzter Monat



Welche Berichte enthält er?

Der zusammenfassende Bericht enthält die folgenden Berichte:

- **Verteilung des Benutzerrisikos**: Die Verteilung von Profilen mit hohem, mittlerem und niedrigem Risiko auf der Grundlage ihrer höchsten berechneten Risikobewertung im ausgewählten Zeitraum.
- Benutzer mit dem höchsten Risiko: Die riskantesten Benutzer unter allen Benutzern, sortiert nach den höchsten Risikowerten für den ausgewählten Zeitraum.
- **Risikoereignisse nach Kategorien**: Die umfassende Übersicht über die Arten von Risikopositionen und kritischen Risiken, die anhand von Risikokategorien bereitgestellt werden, die sofortige Maßnahmen erfordern. Die Risikoindikatoren sind in die folgenden Kategorien unterteilt:
  - Kompromittierte Benutzer
  - Kompromittierte Endpunkte
  - Exfiltration von Daten
  - Insider-Bedrohungen
- **Risikoindikatoren**: Die ausgelösten Risikoindikatoren für die Benutzer für den ausgewählten Zeitraum.
- **Aktionen**: Die auf die Risikoindikatoren angewendeten Aktionen, die für die Benutzer für den ausgewählten Zeitraum ausgelöst wurden.

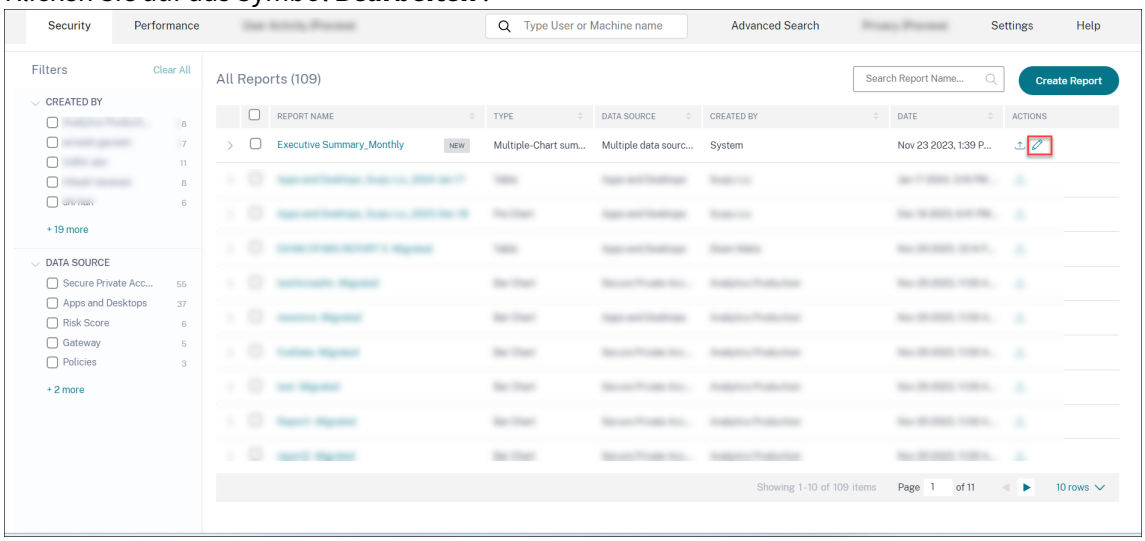
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Wichtigste Richtlinien**: Die fünf wichtigsten Richtlinien, die im ausgewählten Zeitraum am häufigsten ausgelöst wurden.
- **Top-Aktionen**: Die fünf wichtigsten Aktionen, die im ausgewählten Zeitraum am häufigsten ausgelöst wurden.
- **Risikoindikatoren nach Schweregrad**: Standard- und benutzerdefinierte Risikoindikatoren, die von den Benutzern ausgelöst wurden, sortiert nach Schweregrad.
- **Risikoindikatoren nach Gesamtereignissen**: Standard- und benutzerdefinierte Risikoindikatoren, die von den Benutzern ausgelöst wurden, sortiert nach den Ereignissen.

Einen zusammenfassenden Bericht bearbeiten

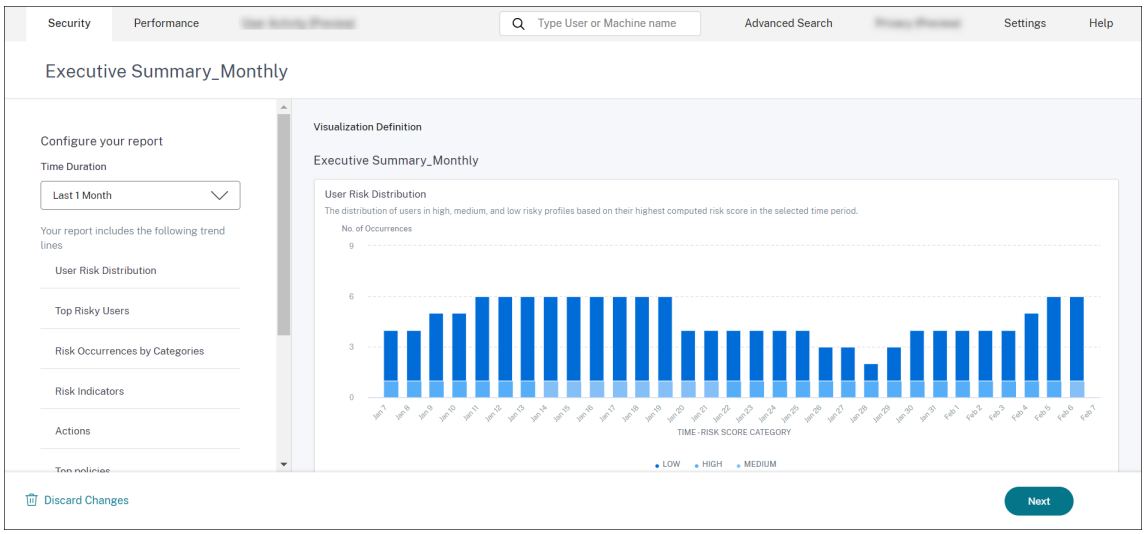
Gehen Sie wie folgt vor, um einen zusammenfassenden Bericht zu bearbeiten:

1. Klicken Sie auf das Symbol **Bearbeiten** .



2. Wählen Sie im Bereich **Bericht konfigurieren** die Zeitdauer aus, für die Sie die Daten anzeigen möchten.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



3. Klicken Sie auf **Weiter**. Der Bereich **Bericht speichern** wird angezeigt.

> **Hinweis:**
>
> Um die Änderungen zu verwerfen, klicken Sie auf **Änderungen verwerfen**.

4. Geben Sie im Bereich **Bericht speichern** die folgenden Details ein:

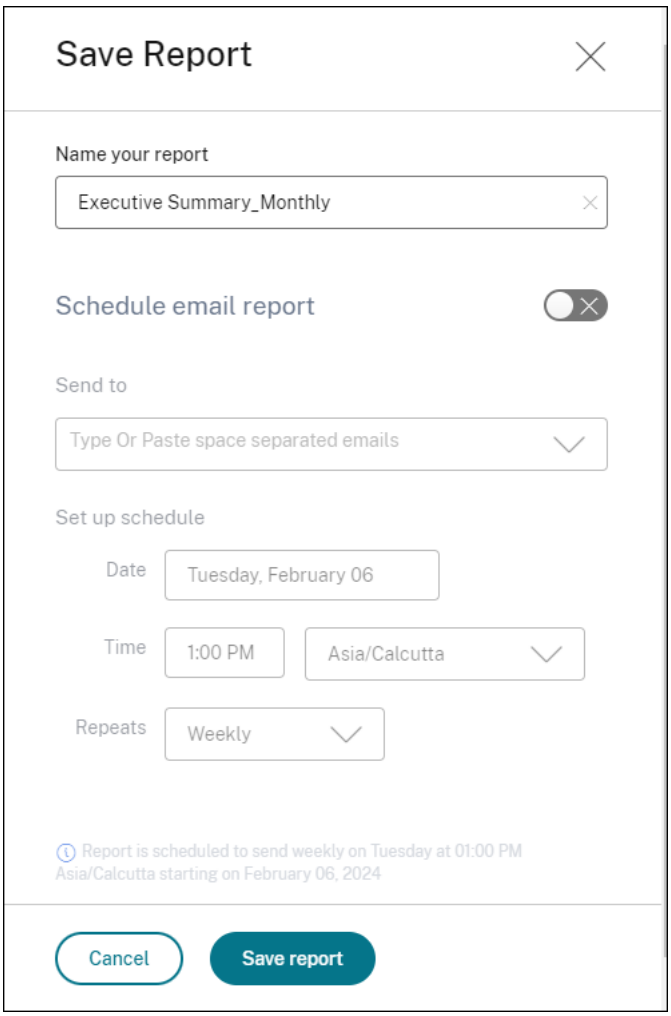
   a) **Benennen Sie Ihren Bericht**: Name des zusammenfassenden Berichts.

   b) **E-Mail-Bericht planen**: Aktivieren Sie diese Option, um den Bericht zu planen. Der Schalter ist standardmäßig ausgeschaltet.

   c) **Senden an**: Wählen Sie eine Verteilerliste aus dem Dropdownmenü aus. Sie können auch eine Kombination aus Verteilerlisten und einzelnen E-Mail-Adressen hinzufügen. Informationen zum Erstellen einer benutzerdefinierten Verteilerliste finden Sie unter E-Mail-Einstellungen für Administratoren.

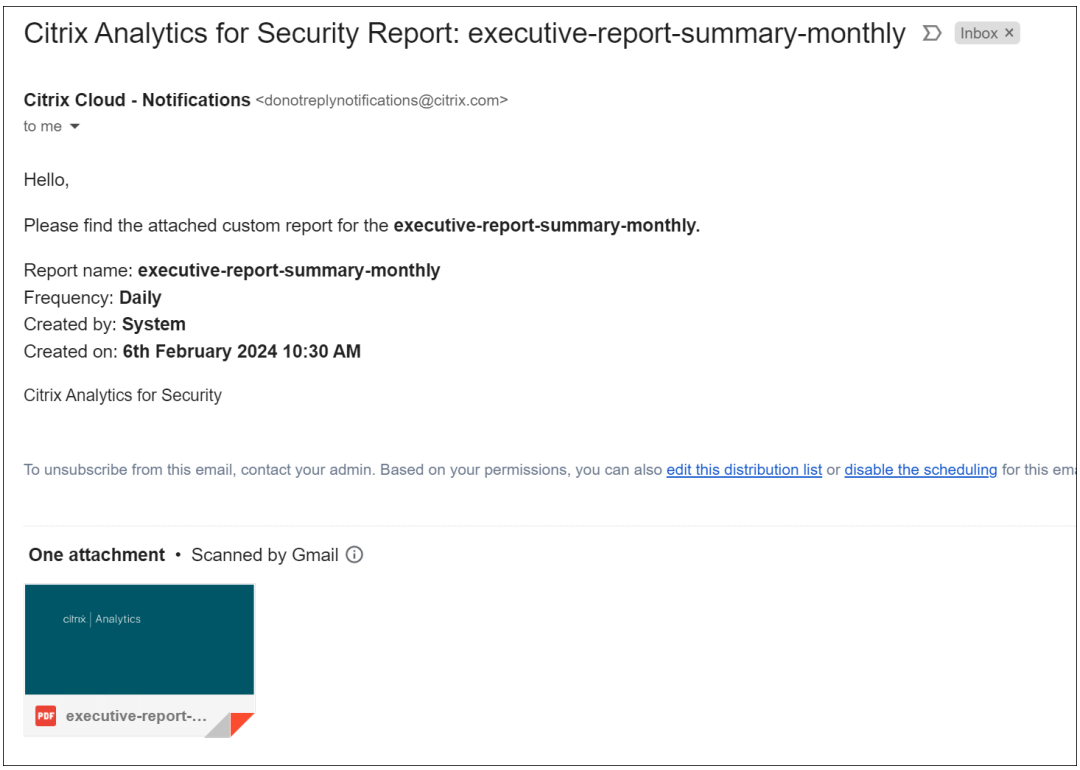
   d) **Zeitplan einrichten**: Wählen Sie den gewünschten Zeitpunkt aus, zu dem der Bericht zum ersten Mal an die ausgewählte Zielgruppe gesendet wird, sowie die Uhrzeit, zu der er wiederholt wird.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

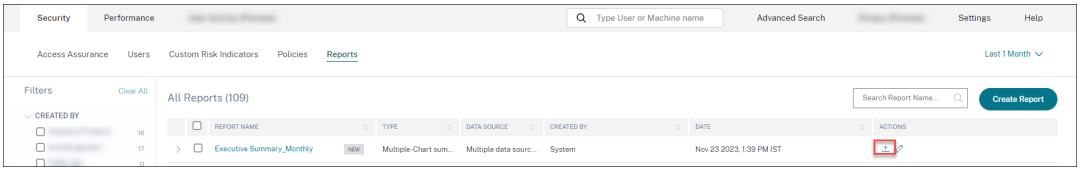


e) Klicken Sie auf **Bericht speichern**. Der Bericht wird dann als E-Mail an die aufgeführten Empfänger gesendet.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

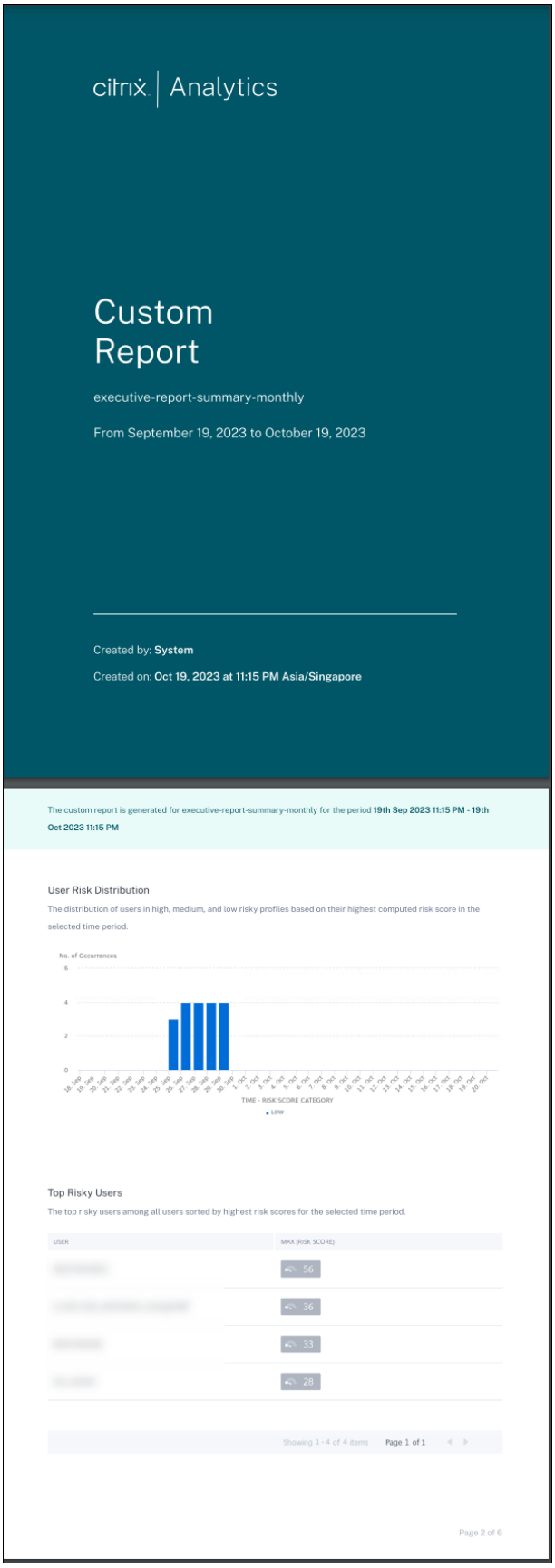


Alternativ können Sie den Geschäftsbericht über das **Exportsymbol** als PDF exportieren.



Der folgende Screenshot zeigt eine Beispiel-PDF-Ausgabe:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Self-Service-Suche

December 12, 2023

Was ist Self-Service-Suche?

Mit der Self-Service-Suchfunktion können Sie Benutzerereignisse suchen und filtern, die von Ihren Datenquellen empfangen wurden. Sie können die zugrunde liegenden Benutzerereignisse und ihre Attribute untersuchen. Diese Ereignisse helfen Ihnen, Datenprobleme zu identifizieren und zu beheben. Auf der Suchseite werden verschiedene Facetten (Dimensionen) und Metriken für eine Datenquelle angezeigt. Sie können Ihre Suchanfrage definieren und Filter anwenden, um die Ereignisse anzuzeigen, die Ihren definierten Kriterien entsprechen. Standardmäßig zeigt die Self-Service-Suchseite Benutzerereignisse für den letzten Tag an.

Derzeit ist die Self-Service-Suchfunktion für die folgenden Datenquellen verfügbar:

- Authentication
- Gateway
- Secure Browser
- Secure Private Access
- Apps und Desktops
- Leistungsfähige Benutzer, Maschinen und Sitzungen

Sie können auch eine Self-Service-Suche nach Ereignissen durchführen, die Ihren definierten Richtlinien entsprechen. Weitere Informationen finden Sie unter Self-Service-Suche nach Richtlinien.

So greifen Sie auf die Selbstbedienungssuche zu

Mit den folgenden Optionen können Sie auf die Self-Service-Suche zugreifen:

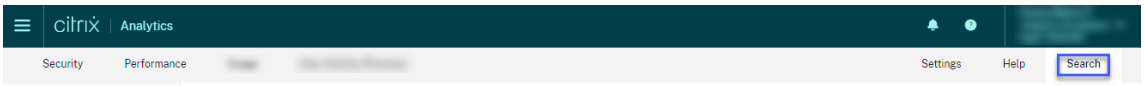
- **Obere Leiste**: Klicken Sie in der oberen Leiste auf **Suchen**, um alle Benutzerereignisse für die ausgewählte Datenquelle anzuzeigen.
- **Risikozeitleiste auf einer Benutzerprofilseite**: Klicken Sie auf **Ereignissuche**, um die Ereignisse für den jeweiligen Benutzer anzuzeigen.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

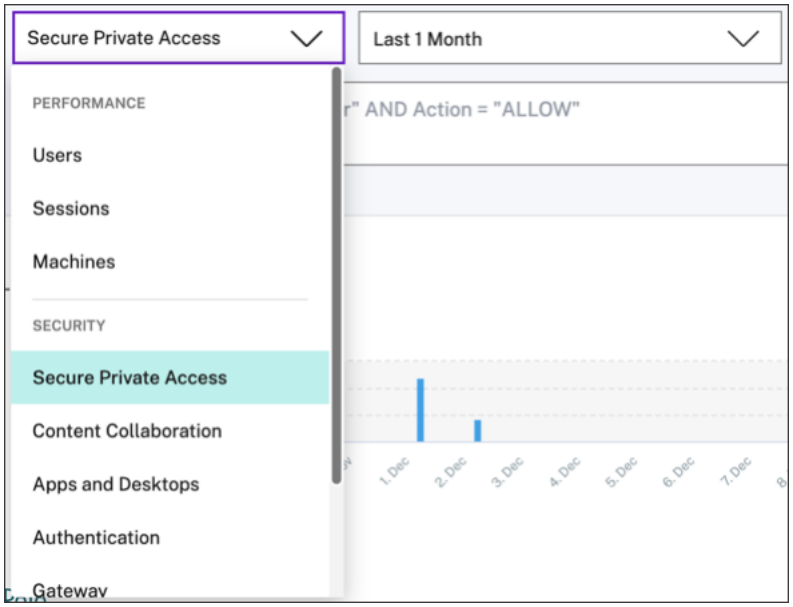
Self-Service-Suche aus der oberen Leiste

Verwenden Sie diese Option, um von einer beliebigen Stelle in der Benutzeroberfläche aus zur Self-Service-Suchseite zu gelangen.

1. Klicken Sie auf **Suchen**, um die Self-Service-Seite anzuzeigen.



2. Wählen Sie die Datenquelle und den Zeitraum aus, um die entsprechenden Ereignisse anzuzeigen.

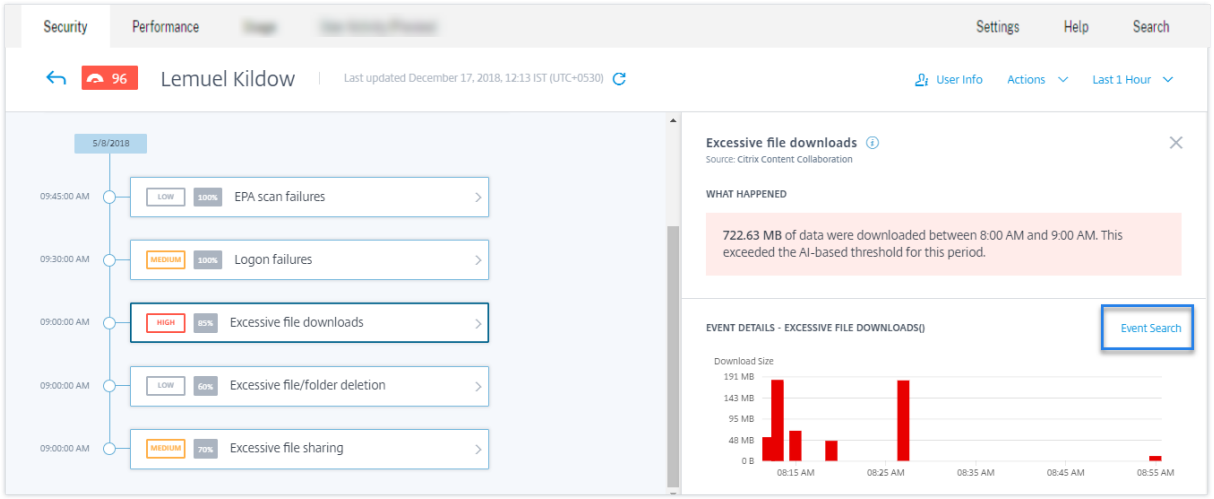


Self-Service-Suche aus der Risikozeitleiste des Benutzers

Verwenden Sie diese Option, wenn Sie die Benutzerereignisse anzeigen möchten, die mit einem Risikoindikator verknüpft sind.

Wenn Sie einen Risikoindikator aus der Zeitleiste eines Benutzers auswählen, wird im rechten Bereich der Risikoindikatorinformationen angezeigt. Klicken Sie auf **Ereignissuche**, um die Ereignisse zu untersuchen, die dem Benutzer und der Datenquelle zugeordnet sind (für die der Risikoindikator ausgelöst wird) auf der Self-Service-Suchseite.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Weitere Informationen zum Zeitplan für das Benutzerrisiko finden Sie unter Risikozeitleiste.

So verwenden Sie die Self-Service-Suche

Verwenden Sie die folgenden Funktionen auf der Self-Service-Suchseite:

- Facetten zum Filtern Ihrer Events.
- Suchfeld, um Ihre Abfrage einzugeben und Ereignisse zu filtern.
- Zeitauswahl zur Auswahl des Zeitraums.
- Timeline-Details zum Anzeigen der Ereignisdiagramme.
- Ereignisdaten zum Anzeigen der Ereignisse.
- Exportieren Sie ins CSV-Format, um Ihre Suchereignisse als CSV-Datei herunterzuladen.
- Exportieren Sie eine visuelle Zusammenfassung, um den visuellen Zusammenfassungsbericht Ihrer Suchanfrage herunterzuladen.
- Mehrspaltige Sortierung, um die Ereignisse nach mehreren Spalten zu sortieren.

Verwenden von Facetten zum Filtern von Ereignissen

Facetten sind die Zusammenfassung von Datenpunkten, die ein Ereignis darstellen. Facetten variieren je nach Datenquelle. Die Facetten für die Secure Private Access-Datenquelle sind beispielsweise Reputation, Aktionen, Standort und Kategoriegruppe. Während die Facetten für Apps und Desktops Ereignistyp, Domäne und Plattform sind.

Wählen Sie die Facetten aus, um Ihre Suchergebnisse zu filtern. Die ausgewählten Facetten werden als Chips angezeigt.

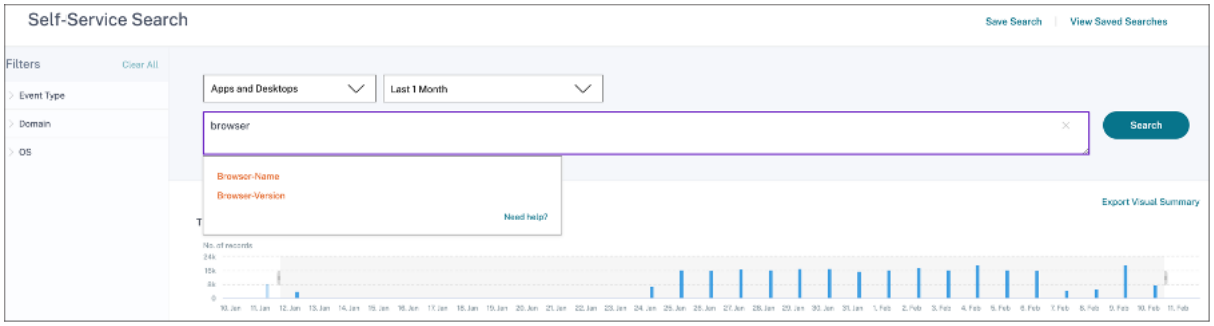
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Weitere Informationen zu den Facetten, die jeder Datenquelle entsprechen, finden Sie im Self-Service-Suchartikel für die Datenquelle, die weiter oben in diesem Artikel erwähnt wird.

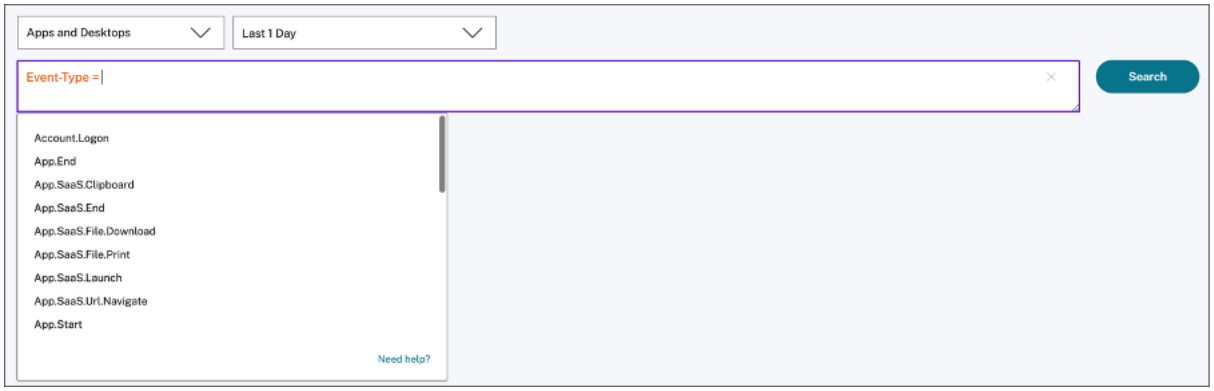
Verwenden Sie die Suchabfrage im Suchfeld, um Ereignisse zu filtern

Wenn Sie den Cursor in das Suchfeld setzen, zeigt das Suchfeld eine Liste von Dimensionen an, die auf den Benutzerereignissen basieren. Diese Dimensionen variieren je nach Datenquelle. Verwenden Sie die Dimensionen und die gültigen Operatoren, um Ihre Suchkriterien zu definieren und nach den erforderlichen Ereignissen zu suchen.

Bei der Self-Service-Suche nach Apps und Desktops erhalten Sie beispielsweise die folgenden Werte für die Dimension `Browser`. Verwenden Sie die Dimension, um Ihre Abfrage einzugeben, wählen Sie den Zeitraum aus, und klicken Sie dann auf **Suchen**.



Wenn Sie bestimmte Dimensionen wie `Event-Type` und `Clipboard-Operation` zusammen mit einem gültigen Operator auswählen, werden die Werte der Dimension automatisch angezeigt. Sie können einen Wert aus den vorgeschlagenen Optionen auswählen oder je nach Ihren Anforderungen einen neuen Wert eingeben.



Unterstützte Operatoren bei Suchanfragen Verwenden Sie die folgenden Operatoren in Ihren Suchanfragen, um Ihre Suchergebnisse zu verfeinern.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Betreiber	Beschreibung	Beispiel	Ausgabe
	Weisen Sie einer Suchdimension einen Wert zu.	Benutzername: John	Zeigt Ereignisse für den Benutzer John an.
=	Weisen Sie einer Suchdimension einen Wert zu.	Benutzername = John	Zeigt Ereignisse für den Benutzer John an.
~	Suchen Sie Ereignisse mit ähnlichen Werten.	Benutzername ~ test	Zeigt Ereignisse mit ähnlichen Benutzernamen an.
" "	Schließen Sie Werte getrennt durch Leerzeichen ein.	Benutzername = “John Smith”	Zeigt Ereignisse für den Benutzer John Smith an.
< >	Suchen Sie nach einem relationalen Wert.	Datenvolumen > 100	Zeigt Ereignisse an, bei denen das Datenvolumen größer als 100 GB ist.
AND	Suchereignisse, bei denen die angegebenen Bedingungen zutreffen.	Benutzername: John AND Datenvolumen > 100	Zeigt Ereignisse von Benutzer John an, bei denen das Datenvolumen größer als 100 GB ist.
! ~	Überprüft Ereignisse auf das von Ihnen angegebene übereinstimmende Muster. Dieser NOT LIKE Operator gibt die Ereignisse zurück, die das übereinstimmende Muster nirgendwo in der Ereigniszeichenfolge enthalten.	Benutzername! ~ John	Zeigt Ereignisse für die Benutzer an, außer John, John Smith oder solche Benutzer, die den übereinstimmenden Namen “John” enthalten.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Betreiber	Beschreibung	Beispiel	Ausgabe
! =	Prüft Ereignisse auf die genaue Zeichenfolge, die Sie angeben. Dieser NOT EQUAL-Operator gibt die Ereignisse zurück, die die genaue Zeichenfolge nicht irgendwo in der Ereigniszeichenfolge enthalten.	Country != USA	Zeigt Ereignisse für Länder mit Ausnahme der USA an.
*	Suchen Sie Ereignisse, die den angegebenen Strings entsprechen. Derzeit wird der Operator * nur mit den folgenden Operatoren : , = und ! = unterstützt. Bei den Suchergebnissen wird Groß-/Kleinschreibung beachtet	Benutzername = John*	Zeigt Ereignisse für alle Benutzernamen an, die mit John beginnen.
		Benutzername = *John*	Zeigt Ereignisse für alle Benutzernamen an, die John enthalten.
		Benutzername = *Smith	Zeigt Ereignisse für alle Benutzernamen an, die mit Smith enden.
		Benutzername: John*	Zeigt Ereignisse für alle Benutzernamen an, die mit John beginnen.
		Benutzername: *John*	Zeigt Ereignisse für alle Benutzernamen an, die John enthalten.
		Benutzername: *Smith	Zeigt Ereignisse für alle Benutzernamen an, die mit Smith enden.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Betreiber	Beschreibung	Beispiel	Ausgabe
		Benutzername! = John*	Zeigt Ereignisse für alle Benutzernamen an, die nicht mit John beginnen.
		Benutzername! = *Schmied	Zeigt Ereignisse für alle Benutzernamen an, die nicht mit Smith enden.
`IN`	Weisen Sie einer Suchdimension mehrere Werte zu, um die Ereignisse abzurufen, die sich auf einen oder mehrere Werte beziehen. **Hinweis**: Derzeit können Sie diesen Operator mit den folgenden Dimensionen von Apps und Desktops- `Device ID`, `Domain` `Event-Type`, und verwenden `User-Name`. Dieser Operator ist nur für die String-Werte anwendbar.	Benutzername IN (John, Kevin)	Finden aller Ereignisse im Zusammenhang mit John oder Kevin.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Betreiber	Beschreibung	Beispiel	Ausgabe
`NOT IN`	Weisen Sie einer Suchdimension mehrere Werte zu und suchen Sie die Ereignisse, die die angegebenen Werte nicht enthalten. **Hinweis**: Derzeit können Sie diesen Operator mit den folgenden Dimensionen von Apps und Desktops- `Device ID`, `Domain Event-Type`, und verwenden `User-Name`. Dieser Operator ist nur für die String-Werte anwendbar.	Benutzername NICHT IN (John, Kevin)	Finde die Events für alle Benutzer außer John und Kevin.
`IS EMPTY`	Sucht nach Nullwert oder leerem Wert für eine Dimension. Dieser Operator funktioniert nur für Dimensionen vom Typ Zeichenfolge wie `App-NameBrowser`, und `Country`. Es funktioniert nicht für Dimensionen vom Typ Nicht-Zeichenfolge (Zahl) wie `Upload-File-SizeDownload-File-Size`, und `Client-IP`.	Land IST LEER	Finden Sie Ereignisse, bei denen der Ländername nicht verfügbar oder leer ist (nicht angegeben).

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Betreiber	Beschreibung	Beispiel	Ausgabe
`IS NOT EMPTY`	Überprüft, ob kein Nullwert oder ein bestimmter Wert für eine Dimension vorhanden ist. Dieser Operator funktioniert nur für Dimensionen vom Typ Zeichenfolge wie `App-NameBrowser`, und `Country`. Es funktioniert nicht für Dimensionen vom Typ Nicht-Zeichenfolge (Zahl) wie `Upload-File-SizeDownload-File-Size`, und `Client-IP`.	Land IST NICHT LEER	Finden von Ereignissen, bei denen der Ländername verfügbar oder angegeben ist.
`OR`	Sucht nach Werten, bei denen eine oder beide Bedingungen zutreffen.	(User-Name = `John*` OR User-Name = `*Smith`) AND Event-Type = “Session.Logon”	Zeigt `Session.Logon`-Ereignisse für alle Benutzernamen an, die mit John beginnen oder mit Smith enden.

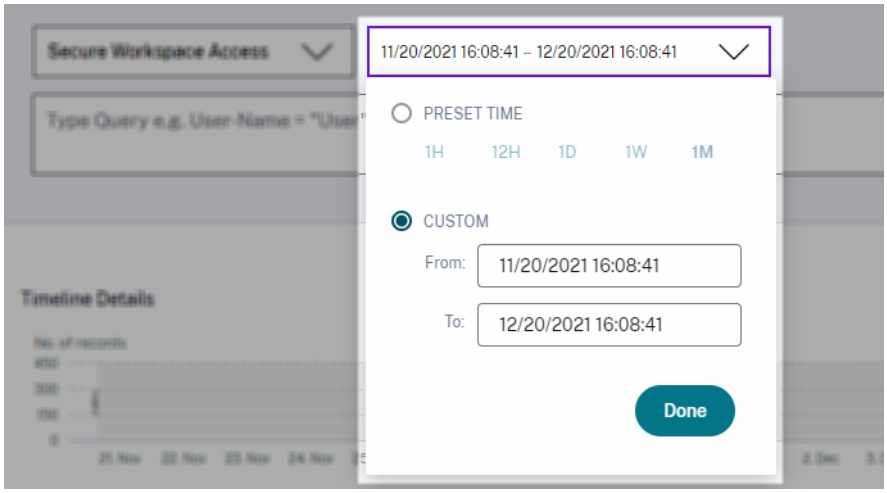
> **Hinweis**
>
> Verwenden Sie für den Operator NOT **EQUAL** beim Eingeben der Werte für die Dimensionen in Ihrer Abfrage die genauen Werte, die auf der Self-Service-Suchseite für eine Datenquelle verfügbar sind. Bei den Dimensionswerten wird die Groß-/Kleinschreibung

Weitere Informationen zum Angeben Ihrer Suchanfrage für die Datenquelle finden Sie im Self-Service-Suchartikel für die oben in diesem Artikel erwähnte Datenquelle.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Wählen Sie die Zeit, um das Ereignis anzuzeigen

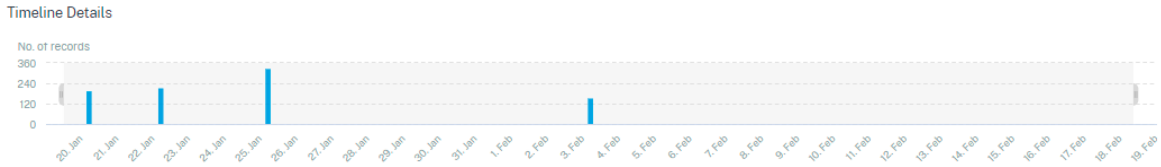
Wählen Sie eine voreingestellte Zeit aus oder geben Sie einen benutzerdefinierten Zeitraum ein und klicken Sie auf **Suchen**, um die Ereignisse anzuzeigen.



Zeigen Sie die Details der Zeitleiste an

Die Zeitleiste bietet eine grafische Darstellung von Benutzerereignissen für den ausgewählten Zeitraum. Bewegen Sie die Auswahlbalken, um den Zeitraum auszuwählen und die Ereignisse anzuzeigen, die dem ausgewählten Zeitraum entsprechen.

Die Abbildung zeigt Timeline-Details für Zugriffsdaten.

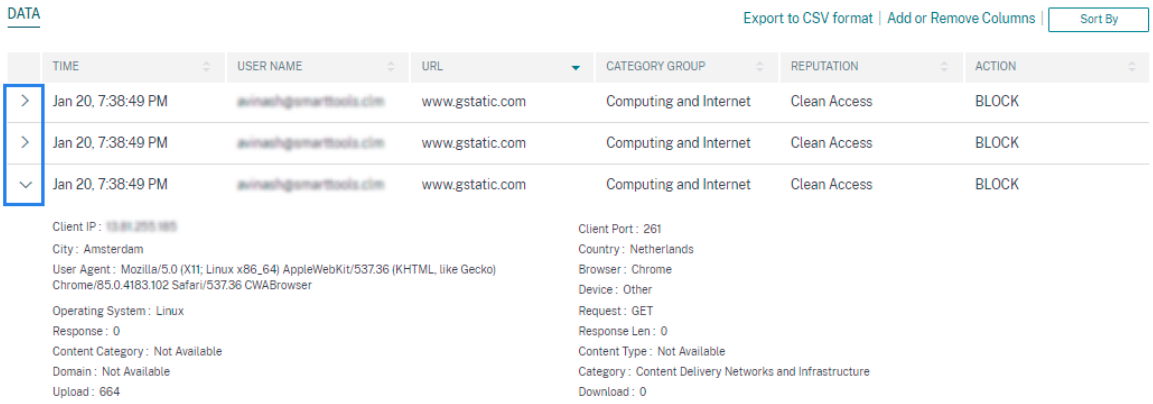


Ereignisse anzeigen

Sie können die detaillierten Informationen zum Benutzerereignis anzeigen. Klicken Sie in der Tabelle **DATEN** auf den Pfeil für jede Spalte, um die Details des Benutzerereignisses anzuzeigen.

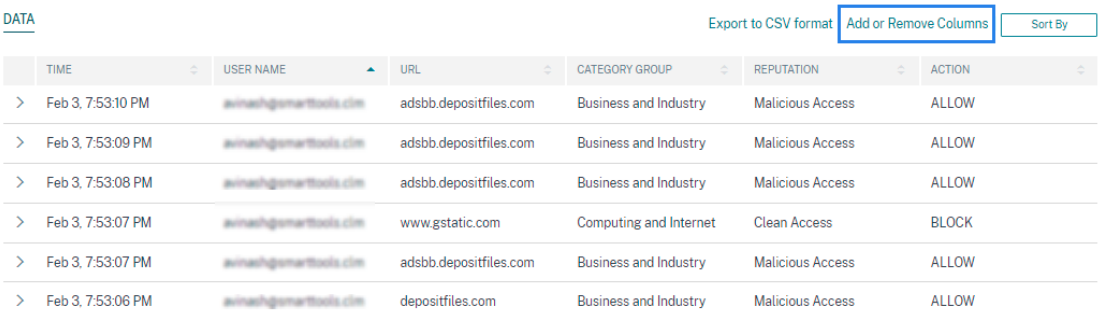
Die Abbildung zeigt die Details zu den Zugriffsdaten des Benutzers.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



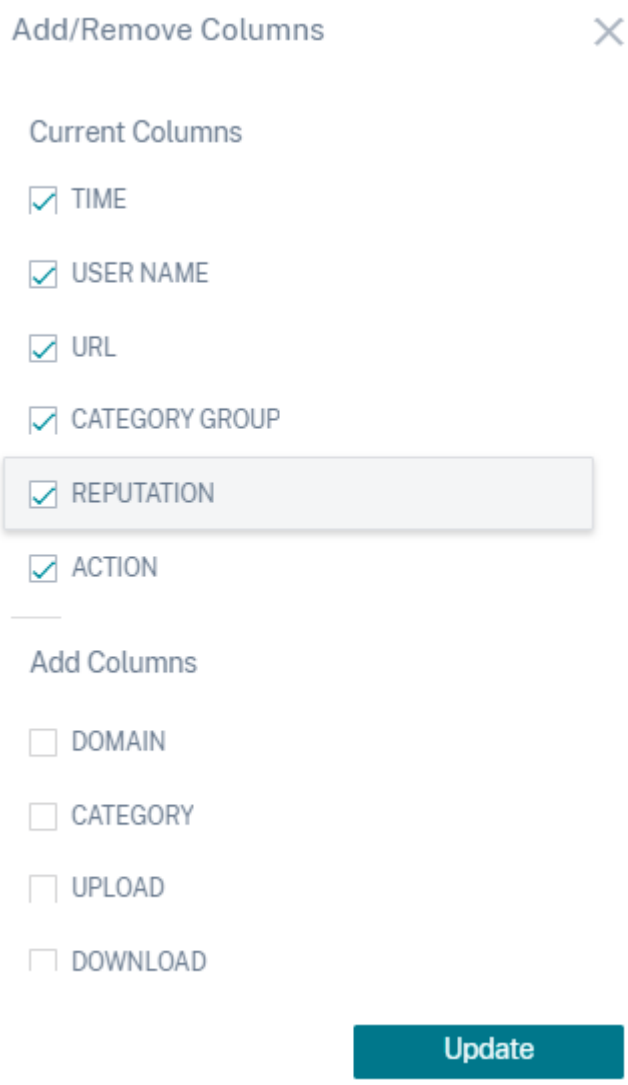
Spalten hinzufügen oder entfernen Sie können der Ereignistabelle entweder Spalten hinzufügen oder daraus entfernen, um die entsprechenden Datenpunkte anzuzeigen oder auszublenden. Führen Sie folgende Schritte aus:

1. Klicken Sie auf **Spalten hinzufügen oder entfernen**.



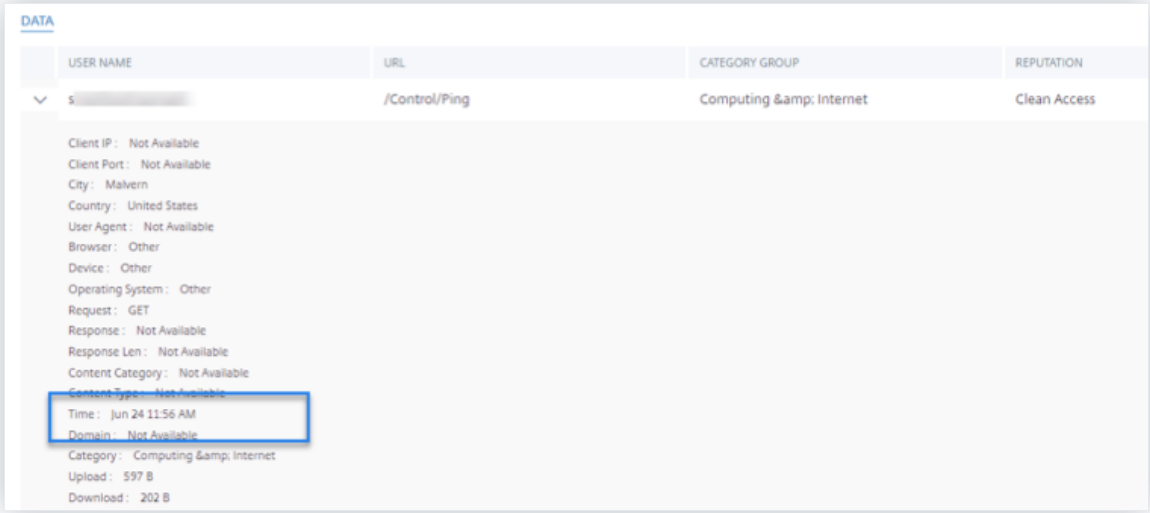
2. Markieren oder heben Sie die Auswahl der Datenelemente in der Liste auf und klicken Sie dann auf **Aktualisieren**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



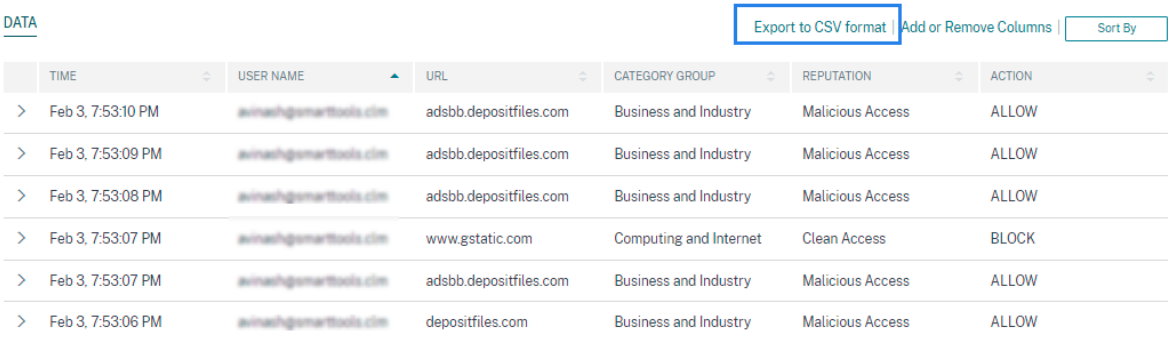
Wenn Sie einen Datenpunkt aus der Liste abwählen, wird die entsprechende Spalte aus der Ereignistabelle entfernt. Sie können diesen Datenpunkt jedoch anzeigen, indem Sie die Ereigniszeile für einen Benutzer erweitern. Wenn Sie beispielsweise den **TIME-Datenpunkt** aus der Liste abwählen, wird die Spalte **TIME** aus der Ereignistabelle entfernt. Um den Zeitdatensatz anzuzeigen, erweitern Sie die Ereigniszeile für einen Benutzer.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Exportieren Sie die Ereignisse in eine CSV-Datei

Exportieren Sie die Suchergebnisse in eine CSV-Datei und speichern Sie sie als Referenz. Klicken Sie auf In **CSV-Format** exportieren, um die Ereignisse zu exportieren und die generierte CSV-Datei herunterzuladen. Mit der Funktion In **CSV-Format exportieren** können Sie 100.000 Zeilen exportieren.



Visuelle Zusammenfassung exportieren

Sie können den visuellen Zusammenfassungsbericht Ihrer Suchanfrage herunterladen und eine Kopie mit anderen Benutzern, Administratoren oder Ihrem Führungsteam teilen.

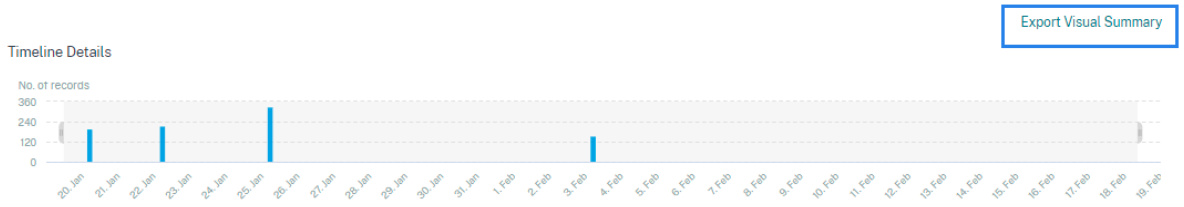
Klicken Sie auf **Visual Summary exportieren**, um den visuellen Zusammenfassungsbericht als PDF herunterzuladen. Der Bericht enthält die folgenden Informationen:

- Die Suchanfrage, die Sie für die Ereignisse für den ausgewählten Zeitraum angegeben haben.
- Die Facetten (Filter), die Sie für den ausgewählten Zeitraum auf die Ereignisse angewendet haben.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Die visuelle Zusammenfassung wie die Zeitleistendiagramme, Balkendiagramme oder Diagramme der Suchereignisse für den ausgewählten Zeitraum.

Für eine Datenquelle können Sie den visuellen Zusammenfassungsbericht nur herunterladen, wenn die Daten in visuellen Formaten wie Balkendiagrammen und Zeitleistendetails angezeigt werden. Andernfalls ist diese Option nicht verfügbar. Sie können beispielsweise den visuellen zusammenfassenden Bericht der Datenquellen wie Apps und Desktops, Sessions herunterladen, in dem Sie Daten als Zeitachsendetails und Balkendiagramme sehen. Für Datenquellen wie Benutzer und Maschinen sehen Sie Daten nur im Tabellenformat. Daher können Sie keinen visuellen Zusammenfassungsbericht herunterladen.

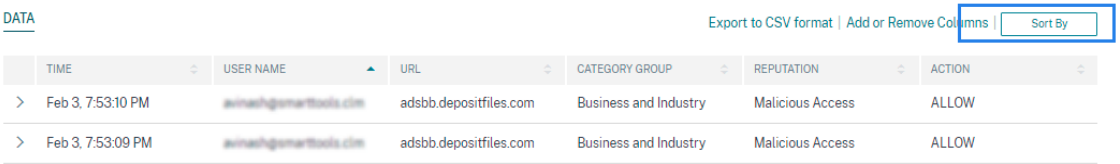


Mehrspaltige Sortierung

Die Sortierung hilft bei der Organisation Ihrer Daten und bietet eine bessere Sichtbarkeit. Auf der Self-Service-Suchseite können Sie die Benutzerereignisse nach einer oder mehreren Spalten sortieren. Die Spalten repräsentieren die Werte verschiedener Datenelemente wie Benutzername, Datum und Uhrzeit und URL. Diese Datenelemente variieren basierend auf den ausgewählten Datenquellen.

Gehen Sie wie folgt vor, um eine mehrspaltige Sortierung durchzuführen:

1. Klicken Sie auf **Sortieren nach**.



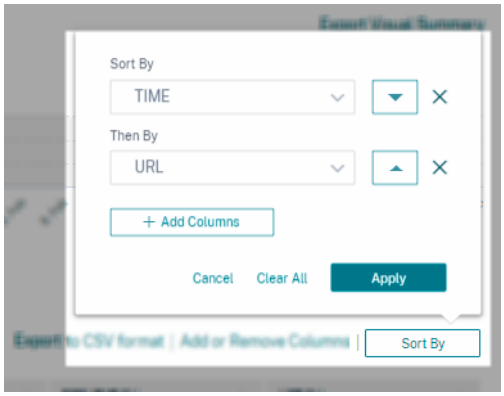
2. Wählen Sie eine Spalte aus der Liste **Sortieren nach** aus.
3. Wählen Sie die Sortierreihenfolge - aufsteigend (Pfeil nach oben) oder absteigend (Pfeil nach unten), um die Ereignisse in der Spalte zu sortieren.
4. Klicken Sie auf **+ Spalten hinzufügen**.
5. Wählen Sie eine weitere Spalte aus der Liste **Dann vorbei** aus.
6. Wählen Sie die Sortierreihenfolge aus - aufsteigend (Pfeil nach oben) oder absteigend (Abwärtsfehler), um die Ereignisse in der Spalte zu sortieren.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Hinweis**
>
> Sie können bis zu sechs Spalten hinzufügen, um die Sortierung durchzuführen.

7. Klicken Sie auf **Anwenden**.
8. Wenn Sie die vorherigen Einstellungen nicht anwenden möchten, klicken Sie auf **Abbrechen**. Um die Werte der ausgewählten Spalten zu entfernen, klicken Sie auf **Alle löschen**.

Das folgende Beispiel zeigt eine mehrspaltige Sortierung der Secure Private Access-Ereignisse. Die Ereignisse werden nach Zeit (in der neuesten bis ältesten Reihenfolge) und dann nach URL (in alphabetischer Reihenfolge) sortiert.



Alternativ können Sie mit der **Umschalttaste** eine mehrspaltige Sortierung durchführen. Drücken Sie die **Umschalttaste** und klicken Sie auf die Spaltenüberschriften, um die Benutzerereignisse zu sortieren.

So speichern Sie die Self-Service-Suche

Als Administrator können Sie eine Self-Service-Abfrage speichern. Diese Funktion spart Zeit und Mühe beim Umschreiben der Abfrage, die Sie häufig für die Analyse oder Fehlerbehebung verwenden. Die folgenden Optionen werden mit der Abfrage gespeichert:

- Angewandte Suchfilter
- Ausgewählte Datenquelle und Dauer

Gehen Sie wie folgt vor, um eine Selbstbedienungsabfrage zu speichern:

1. Wählen Sie die erforderliche Datenquelle und Dauer aus.
2. Geben Sie eine Abfrage in die Suchleiste ein.
3. Wenden Sie die erforderlichen Filter an.
4. Klicken Sie auf **Suche speichern**.
5. Geben Sie den Namen an, um die benutzerdefinierte Abfrage zu speichern.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Hinweis Stellen Sie**
>
> sicher, dass der Abfragename eindeutig ist. Andernfalls wird die Abfrage nicht gespeichert.

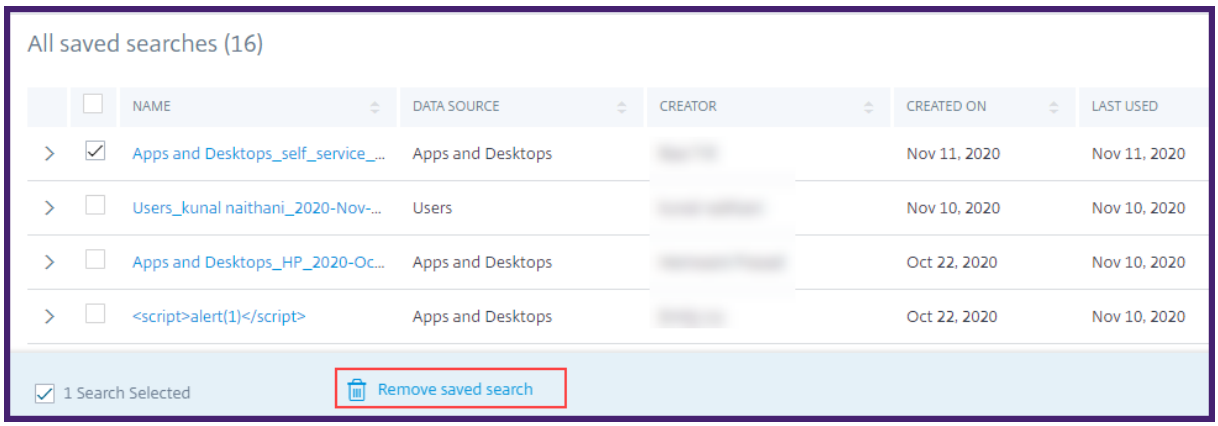
6. Aktivieren Sie die Schaltfläche **E-Mail-Bericht planen**, wenn Sie regelmäßig eine Kopie des Suchanfrageberichts an sich und andere Benutzer senden möchten. Weitere Informationen finden Sie unter Planen einer E-Mail für eine Suchanfrage.
7. Klicken Sie auf **Speichern**.

So zeigen Sie die gespeicherten Suchanfragenan:

1. **Klicken Sie auf Gespeicherte Suchen**
2. Klicken Sie auf den Namen der Suchanfrage.

So entfernen Sie eine gespeicherte Suche:

1. **Klicken Sie auf Gespeicherte Suchen**
2. Wählen Sie die Suchabfrage aus, die Sie gespeichert haben.
3. Klicke auf **Gespeicherte Suche entfernen**.



So ändern Sie eine gespeicherte Suche:

1. **Klicken Sie auf Gespeicherte Suchen**
2. Klicken Sie auf den Namen der Suchabfrage, die Sie gespeichert haben.
3. Ändern Sie die Suchanfrage oder die Facettenauswahl basierend auf Ihren Anforderungen.
4. Klicken Sie auf **Suche aktualisieren > Speichern**, um zu aktualisieren, und speichern Sie die geänderte Suche unter demselben Suchanfragenamen.
5. Wenn Sie die geänderte Suche unter einem neuen Namen speichern möchten, klicken Sie auf den Abwärtspfeil und dann auf **Als neue Suche speichern > Speichern unter**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Wenn Sie die Suche durch einen neuen Namen ersetzen, wird die Suche als neuer Eintrag gespeichert. Wenn Sie den vorhandenen Suchnamen beim Ersetzen beibehalten, setzen die geänderten Suchdaten die vorhandenen Suchdaten außer Kraft.

> **Hinweis**
>
> - Nur ein Abfrage-Besitzer kann seine gespeicherten Suchanfragen ändern oder entfernen.
> - Sie können die gespeicherte Adresse des Suchlinks kopieren, um sie mit einem anderen Benutzer zu teilen.

Planen Sie eine E-Mail für eine Suchanfrage

Sie können in regelmäßigen Abständen eine Kopie des Suchanfrageberichts an sich und andere Benutzer senden, indem Sie einen Zeitplan für die E-Mail-Zustellung einrichten.

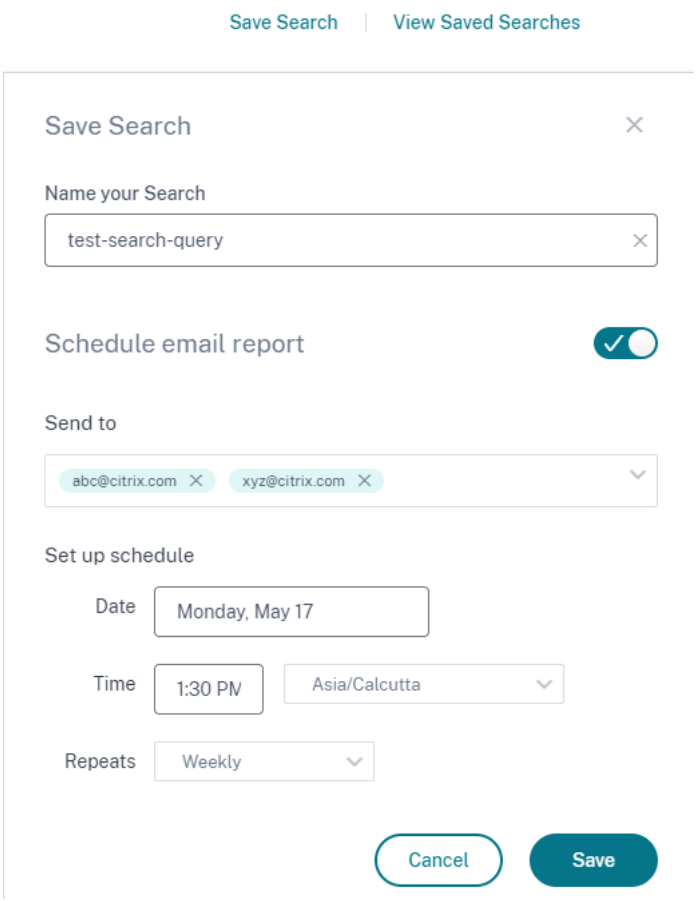
Diese Option ist nur verfügbar, wenn Ihr Suchanfragebericht Daten in visuellen Formaten wie Balkendiagrammen und Zeitachsendetails enthält. Andernfalls können Sie keine E-Mail-Zustellung planen. Sie können beispielsweise eine E-Mail für Datenquellen wie Apps und Desktops, Sessions planen, in der Sie Daten als Zeitachsendetails und Balkendiagramme sehen. Für Datenquellen wie Benutzer und Maschinen sehen Sie Daten nur im Tabellenformat. Daher können Sie keine E-Mail planen.

Planen Sie eine E-Mail beim Speichern einer Suchanfrage

Richten Sie beim Speichern einer Suchanfrage einen Zeitplan für die E-Mail-Zustellung wie folgt ein:

1. Aktivieren Sie im Dialogfeld **Suche speichern** die Schaltfläche **E-Mail-Bericht planen** .

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



2. Geben Sie die E-Mail-Adressen der Empfänger ein oder fügen Sie sie ein.

> **Hinweis**
>
> E-Mail-Gruppen werden nicht unterstützt.

3. Legen Sie Datum und Uhrzeit für die E-Mail-Zustellung fest.
4. Wählen Sie die Lieferfrequenz aus - täglich, wöchentlich oder monatlich.
5. Klicken Sie auf **Speichern**.

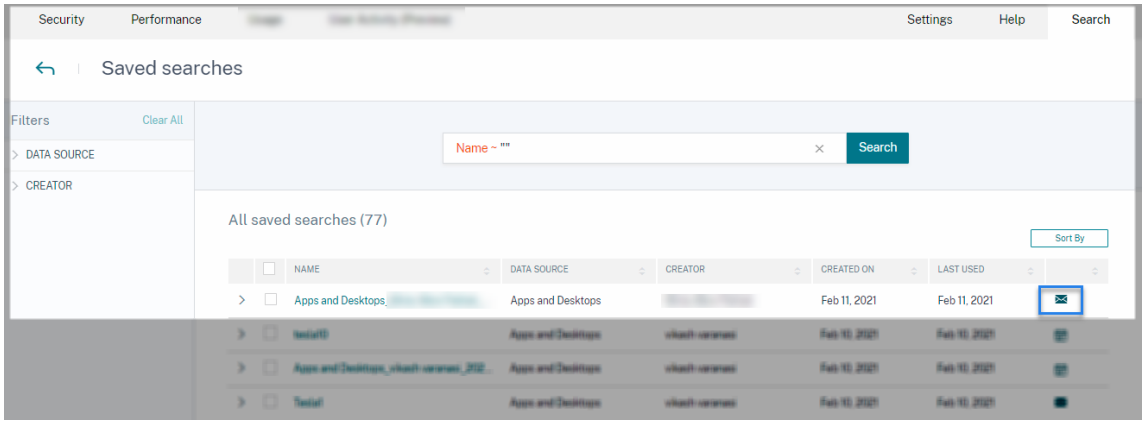
Planen Sie eine E-Mail für eine bereits gespeicherte Suchanfrage

Wenn Sie einen E-Mail-Lieferplan für eine Suchanfrage einrichten möchten, die Sie zuvor gespeichert haben, gehen Sie wie folgt vor:

1. **Klicken Sie auf Gespeicherte Suchen**
2. Gehen Sie zu der Suchanfrage, die Sie erstellt haben. Klicken Sie auf das Symbol **Diese Abfrage per E-Mail senden** .

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Hinweis**
>
> Nur ein Abfragebesitzer kann die E-Mail-Zustellung seiner gespeicherten Suchanfrage planen.



3. Aktivieren Sie die Schaltfläche **E-Mail-Bericht planen** .
4. Geben Sie die E-Mail-Adressen der Empfänger ein oder fügen Sie sie ein.

> **Hinweis**
>
> E-Mail-Gruppen werden nicht unterstützt.

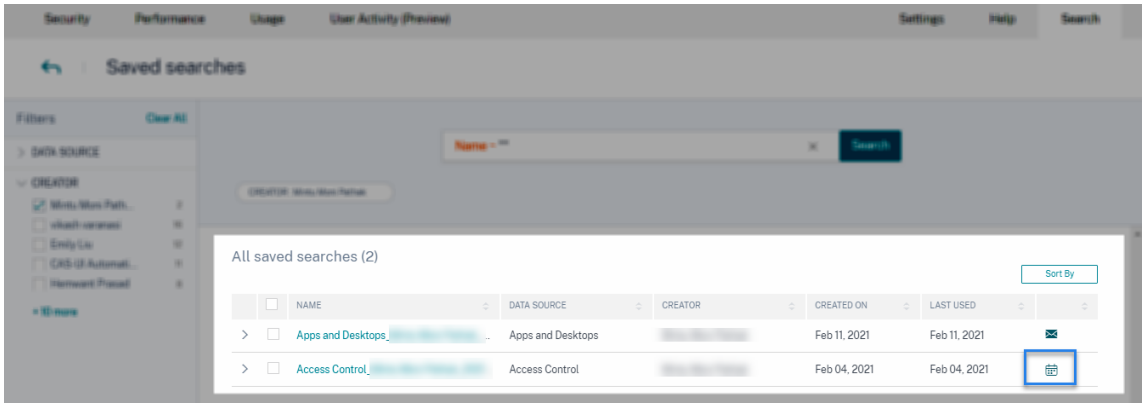
5. Legen Sie Datum und Uhrzeit für die E-Mail-Zustellung fest.
6. Wählen Sie die Lieferfrequenz aus - täglich, wöchentlich oder monatlich.
7. Klicken Sie auf **Speichern**.

Stoppen Sie einen E-Mail-Lieferplan für eine Suchanfrage

1. **Klicken Sie auf Gespeicherte Suchen**
2. Gehen Sie zu der Suchanfrage, die Sie erstellt haben. Klicken Sie auf das Symbol **E-Mail-Lieferplan anzeigen** .

> **Hinweis**
>
> Nur ein Abfragebesitzer kann den E-Mail-Zeitplan seiner gespeicherten Suchanfrage stoppen.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



3. Deaktivieren Sie die Schaltfläche **E-Mail-Bericht planen** .
4. Klicken Sie auf **Speichern**.

Inhalt per E-Mail

Die Empfänger erhalten von "Citrix Cloud - Benachrichtigungen donotreplynotifications@citrix.com" eine E-Mail über den Suchanfragebericht. Der Bericht ist als PDF-Dokument beigefügt. Die E-Mail wird in einem regelmäßigen Intervall gesendet, das von Ihnen in den Einstellungen für **E-Mail-Bericht planen** definiert wurde.

Der Suchanfragebericht enthält die folgenden Informationen:

- Die Suchanfrage, die Sie für die Ereignisse für den ausgewählten Zeitraum angegeben haben.
- Die Facetten (Filter), die Sie auf die Ereignisse angewendet haben.
- Die visuelle Zusammenfassung wie die Zeitleistendiagramme, Balkendiagramme oder Graphen der Suchereignisse.

Berechtigungen für Administratoren mit Vollzugriff und Nur-Lese-Zugriff

- Wenn Sie ein Citrix Cloud-Administrator mit vollem Zugriff sind, können Sie alle auf der **Suchseite** verfügbaren Funktionen nutzen.
- Wenn Sie ein Citrix Cloud-Administrator mit schreibgeschütztem Zugriff sind, können Sie nur die folgenden Aktivitäten auf der **Suchseite** ausführen:
  - Zeigen Sie die Suchergebnisse an, indem Sie eine Datenquelle und den Zeitraum auswählen.
  - Geben Sie eine Suchabfrage ein und sehen Sie sich die Suchergebnisse an.
  - Zeigen Sie die gespeicherten Suchergebnisse anderer Administratoren an.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Exportieren Sie die visuelle Zusammenfassung und laden Sie die Suchergebnisse als CSV-Datei herunter.

Informationen zu den Administratorrollen finden Sie unter Verwalten von Administratorrollen für Citrix Analytics.

Self-Service-Suche nach Authentifizierung

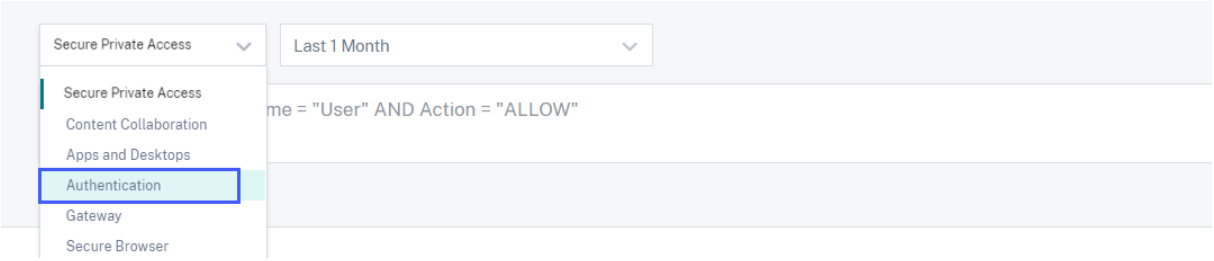
September 24, 2021

Verwenden Sie die Self-Service-Suche, um Einblicke in die Benutzerauthentifizierungsdetails der Citrix Cloud-Benutzer in Ihrem Unternehmen zu erhalten. Citrix Analytics for Security empfängt die Benutzerauthentifizierungsereignisse vom Identitäts- und Zugriffsverwaltungsdienst von Citrix Cloud. Authentifizierungsereignisse wie Benutzeranmeldung, Benutzerabmeldung und Client-Update werden auf der Self-Service-Suchseite angezeigt.

Weitere Informationen zu den Suchfunktionen finden Sie unter **Self-Service-Suche**.

Wählen Sie die Datenquelle für die Authentifizierung

Um die Authentifizierungsereignisse anzuzeigen, wählen Sie **Authentifizierung** aus der Liste aus. Standardmäßig zeigt die Self-Service-Seite die Ereignisse für den letzten Tag an. Sie können auch den Zeitraum auswählen, für den Sie die Ereignisse anzeigen möchten.

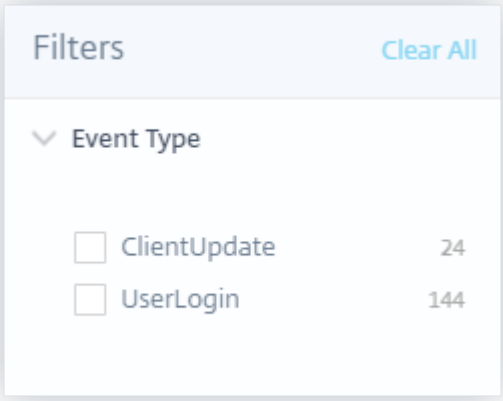


Wählen Sie die Facetten aus, um Ereignisse zu filtern

Verwenden Sie den folgenden Filter für die Authentifizierungsereignisse:

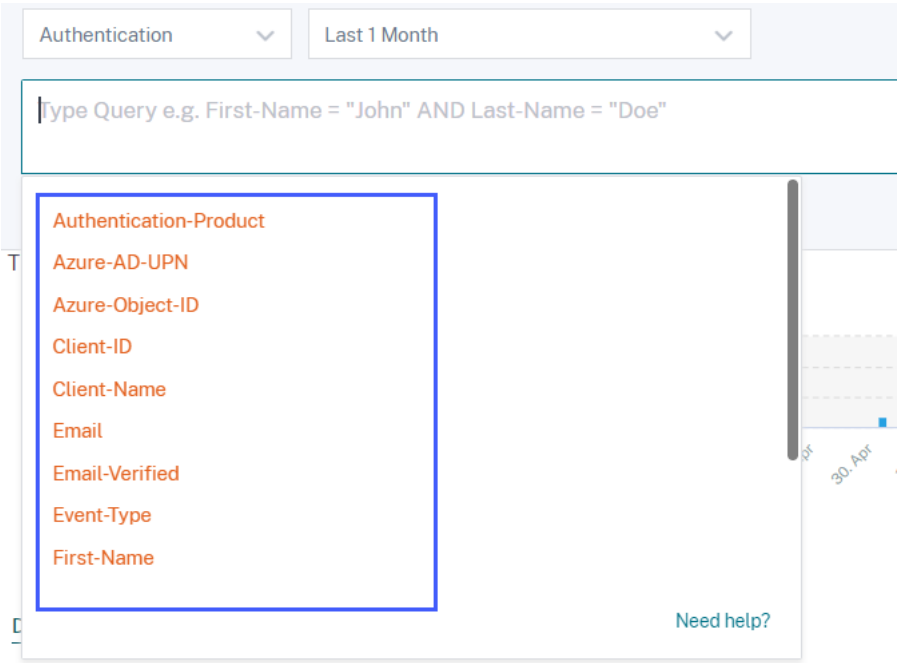
- **Ereignisart**- Suchen Sie Ereignisse basierend auf den Benutzerereignistypen wie Benutzeranmeldung, Benutzerabmeldung und Client-Update.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Angeben der Suchabfrage zum Filtern von Ereignissen

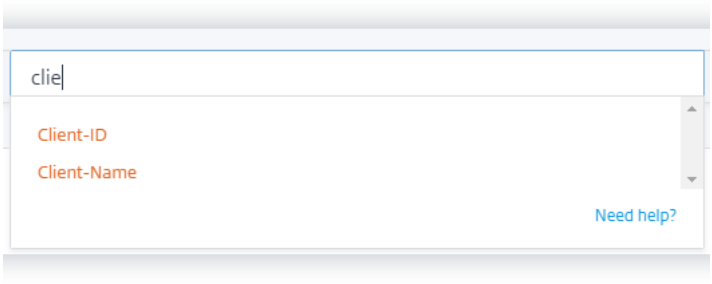
Platzieren Sie den Cursor in das Suchfeld, um die Liste der Dimensionen für die Authentifizierungsereignisse anzuzeigen. Verwenden Sie die Dimensionen und die Operatoren, um Ihre Abfrage anzugeben und nach den erforderlichen Ereignissen zu suchen.



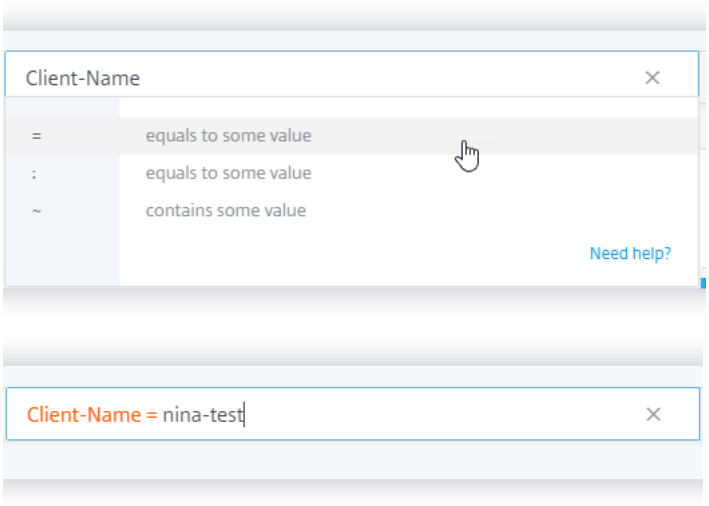
Beispielsweise möchten Sie die Authentifizierungsereignisse für einen Client “Nina-Test”mit verifiziertem E-Mail-Status anzeigen.

1. Geben Sie “Client”in das Suchfeld ein, um die zugehörigen Dimensionen abzurufen.

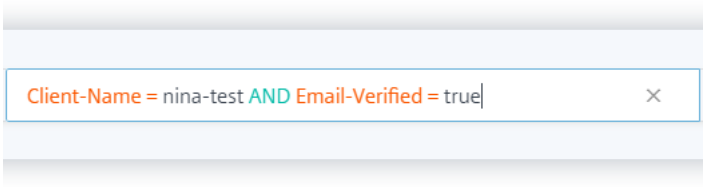
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



2. Wählen Sie **Client-Name** und geben Sie dann den Wert “nina-Test”mit dem Gleichheitsoperator an.



3. Wählen Sie den Operator **UND** und wählen Sie dann die Dimension “**E-Mail verifiziert** “aus. Weisen Sie **Email-Verified** mit dem Gleichheitsoperator den Wert “true”zu. Der Wert “true” zeigt an, dass die E-Mail des Benutzers verifiziert wurde.



4. Wählen Sie den Zeitraum aus, und klicken Sie auf **Suchen**, um die Ereignisse in der Tabelle **DATA** anzuzeigen.

Self-Service-Suche nach Gateway

September 24, 2021

Verwenden Sie die Self-Service-Suchfunktion, um Einblicke in die Benutzerereignisse zu erhalten,

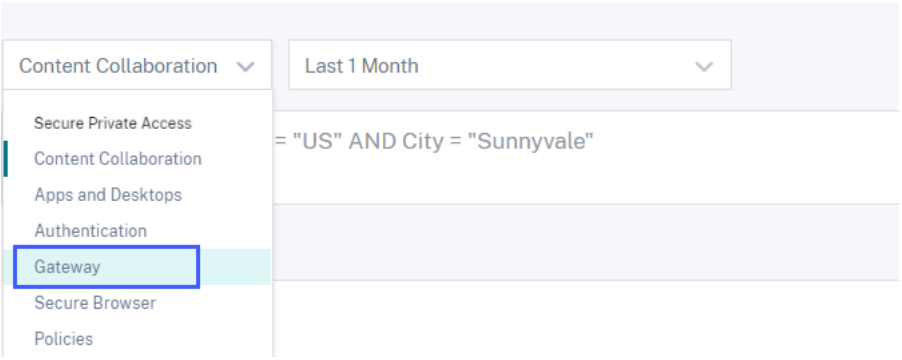
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

die von der Citrix Gateway-Datenquelle Wenn Benutzer über Citrix Gateway auf ihre Netzwerkressourcen wie Dateiserver, Anwendungen und Websites zugreifen, werden Ereignisse für jede Benutzerverbindung generiert. Einige Beispiele für Benutzerereignisse sind wie Authentifizierungsphase, Autorisierungstyp und VPN-Sitzungscode. Citrix Analytics for Security empfängt diese Ereignisse und zeigt sie auf der Self-Service-Suchseite an. Sie können die Benutzer und ihre Zugriffsdetails anzeigen.

Weitere Informationen zu den Suchfunktionen finden Sie unter **Self-Service-Suche**.

Wählen Sie die Gateway-Datenquelle

Um die Gateway-Ereignisse anzuzeigen, wählen Sie **Gateway** aus der Liste aus. Standardmäßig zeigt die Self-Service-Seite die Ereignisse für den letzten Tag an. Sie können auch den Zeitraum auswählen, für den Sie die Ereignisse anzeigen möchten.

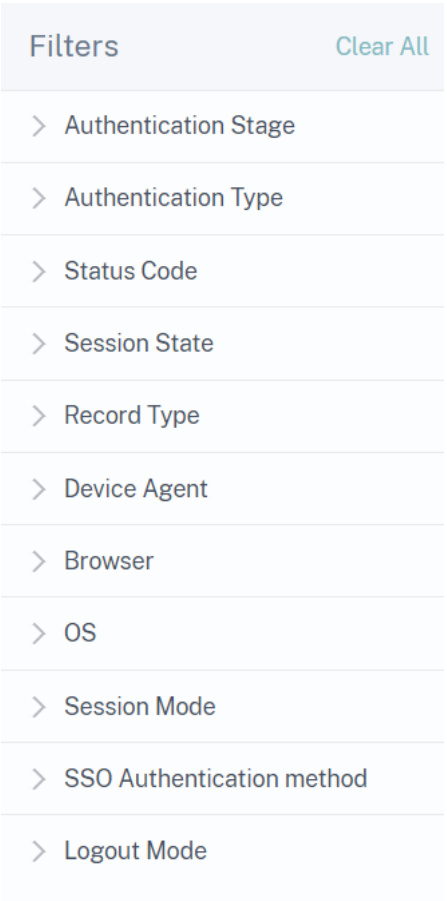


> **Hinweis**
>
> Alternativ können Sie über das Dashboard **Sicherheit** > **Benutzer** > **Zugriffsübersicht auf die Seite Self-Service-Suche nach Gateway zugreifen** . In erfolgreichen Anmeldeszenarien können Sie über den Statuscode auf die Daten zugreifen. Weitere Informationen finden Sie im Dashboard "Zugriffsübersicht".

Verwenden Sie die Facetten, um Ereignisse zu filtern

Die Facetten werden basierend auf den Ereignissen kategorisiert, die von Ihrer Datenquelle empfangen wurden. Verwenden Sie die folgenden Facetten, um Ihre Events zu filtern:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



- **Authentifizierungsphase**- Suchen Sie nach Ereignissen basierend auf verschiedenen Phasen der Clientauthentifizierung, z. B. primär, sekundär und tertiär.
- **Authentifizierungstyp**- Suchen Sie Ereignisse basierend auf den Clientauthentifizierungstypen wie Local, RADIUS, LDAP, TACACS, Clientzertifikatauthentifizierung einschließlich Smartcard-Authentifizierung.
- **Device Agent**- Suchen Sie Ereignisse basierend auf den Client-Geräten wie iPhone, iPad, Windows Mobile.
- **Record Type**- Suchen Sie Ereignisse basierend auf den Arten von VPN-Datensätzen. Folgende VPN-Datensatztypen stehen zur Verfügung:

Datensatztyp	Beschreibung
VPN_AI	Filtert Benutzerereignisse im Zusammenhang mit Authentifizierung.
VPN_IF	Filtert Benutzerereignisse im Zusammenhang mit ICA-Datei.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

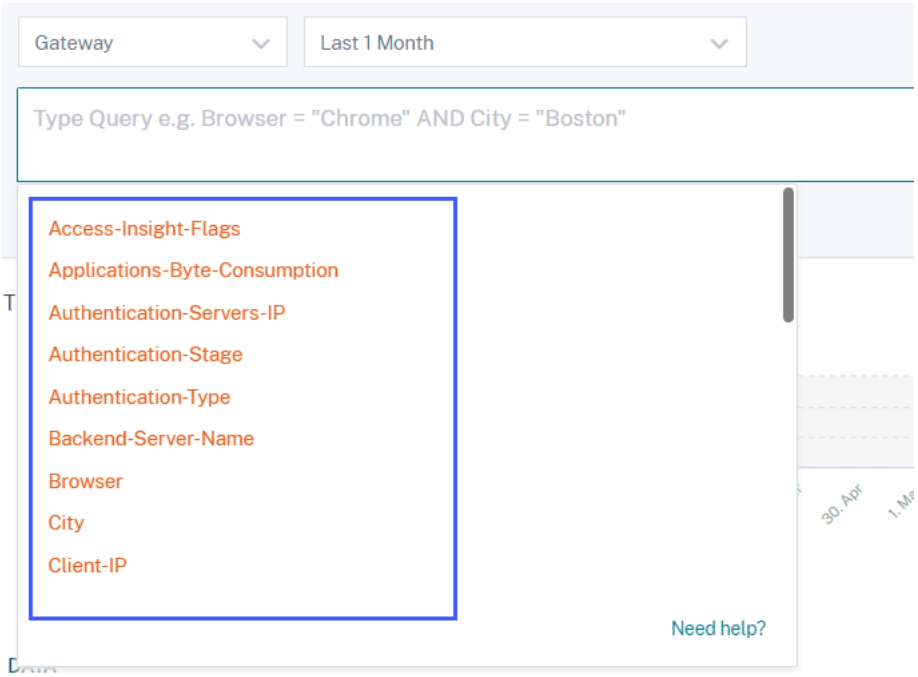
Datensatztyp	Beschreibung
VPN_ST	Filtert Benutzerereignisse im Zusammenhang mit der Sitzungsabmeldung.

- **Browser**- Suche Ereignisse basierend auf den Browsern wie Internet Explorer, Chrome, Firefox, Safari.
- **OS**- Suche nach Ereignissen basierend auf den Client-Betriebssystemen wie Windows, Mac, Linux, Android, iOS.
- **Statuscode**- Suchen Sie Ereignisse basierend auf den VPN-Statuscodes wie SSL-Umleitungsantwort, Autorisierungsfehler, einmaliges Anmelden fehlgeschlagen.
- **Sitzungsstatus**- Suchen Sie Ereignisse basierend auf den VPN-Sitzungsstatus wie Clientstatus, Autorisierungsstatus, SSO-Status, Aktualisierung der Anwendungsbandbreite.
- **Sitzungsmodus**- Suchen Sie Ereignisse basierend auf den VPN-Sitzungsmodi wie Full Tunnel, ICA-Proxy, Clientless.
- **SSO-Authentifizierungsmethode**- Suche nach Ereignissen basierend auf verschiedenen Methoden der Single-Sign-On-Authentifizierung wie Basic, Digest, NTLM, Kerberos, AG basic, formularbasiertes SSO.
- **Abmeldemodus**- Sucht Ereignisse basierend auf den VPN-Abmeldemodi wie interne Fehlerabmeldung, Sitzungstimeout-Abmeldung, vom Benutzer initiierte Abmeldung, Administratorsitzung.

Angeben der Suchabfrage zum Filtern von Ereignissen

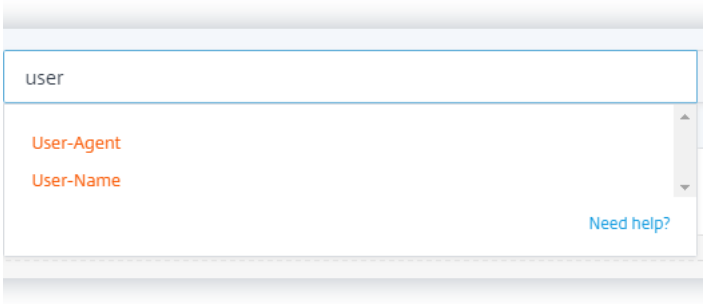
Platzieren Sie den Cursor in das Suchfeld, um die Liste der Dimensionen für die Gateway-Ereignisse anzuzeigen. Verwenden Sie die Dimensionen und die Operatoren, um Ihre Abfrage anzugeben und nach den erforderlichen Ereignissen zu suchen.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

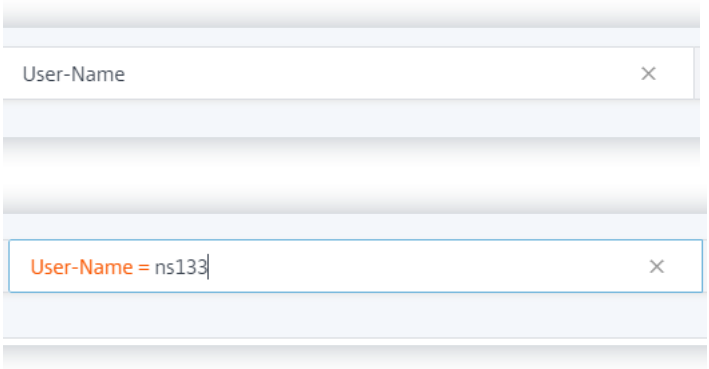


Sie möchten beispielsweise die Ereignisse für einen Benutzer “ns133”anzeigen, bei dem der VPN-Statuscode “erfolgreiche Anmeldung”lautet.

1. Geben Sie “Benutzer”in das Suchfeld ein, um die zugehörige Dimension auszuwählen.

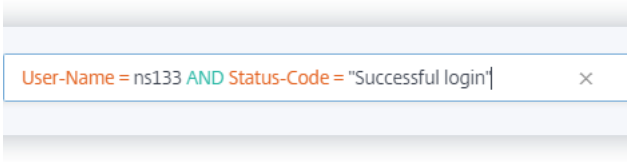


2. Wählen Sie **Benutzername** aus und geben Sie den Wert “ns133”mit dem Gleichheitsoperator ein.

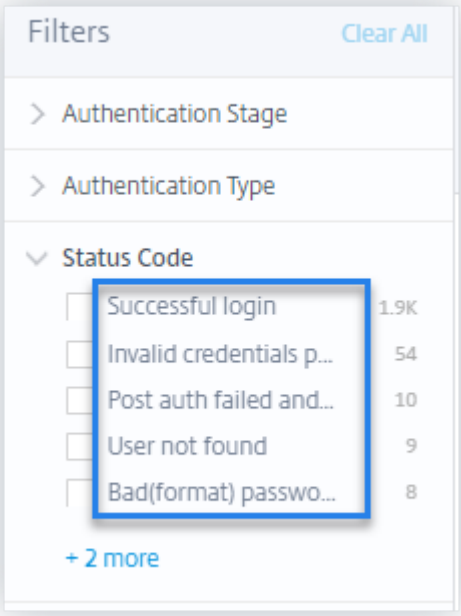


© 1999–2024 Cloud Software Group, Inc. All rights reserved.

3. Wählen Sie den Operator **UND** und wählen Sie dann die Dimension **Statuscode** aus. Geben Sie die Zeichenfolge “Erfolgreiche Anmeldung”für **den Statuscode** mit dem Gleichheitsoperator ein.



Um die möglichen Zeichenfolgenwerte für **Statuscode**zu identifizieren, erweitern Sie die Filterliste **Statuscode** und verwenden Sie den Filternamen als Zeichenfolge in Ihrer Suchanfrage.



4. Wählen Sie den Zeitraum aus, und klicken Sie auf **Suchen**, um die Ereignisse in der Tabelle **DATA** anzuzeigen.

Unterstützte Werte für Ihre Suchanfrage

Geben Sie die folgenden Werte für die Dimensionen ein, um Ihre Suchanfrage zu definieren.

Access-Insight-Flaggen

Zeigt die VPN-Sitzungsstatus an. Geben Sie einen der folgenden Flag-Werte ein:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Status der VPN-Sitzung	Flag-Wert
Vor-Authentifizierung	2
Letzter oder letzter Status der nFactor (Multi-Faktor) -Authentifizierung	1
Authentifizierung posten	4

> **Hinweis**
>
> Dieses Flag gilt nur für die vorhergehenden VPN-Sitzungsstatus für die Authentifizierungsereignisse. Für alle anderen Ereignisse ist der Flag-Wert Null.

Anwendungen-Byte-Verbrauch

Geben Sie für die `Applications-Byte-Consumption` Dimension den folgenden Wert ein:

Wert	Typ	Beschreibung
Beispiele: `40`, `100`	Zahl	Daten (in Byte), die von der Anwendung verbraucht werden, die Sie verwenden.

Authentifizierungs-Server-IP

Geben Sie für die `Authentication-Servers-IP` Dimension den folgenden Wert ein:

Wert	Typ	Beschreibung
Beispiel:`10.xxx.xx.xx`	Zeichenfolge	IP-Adresse des Authentifizierungsservers.

Authentifizierungs-Phase

Geben Sie für die `Authentication-Stage` Dimension den folgenden Wert ein:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Wert	Typ	Beschreibung
`PrimarySecondary`, oder `Tertiary`	Zeichenfolge	Verschiedene Phasen der Clientauthentifizierung.

Authentifizierung-Typ

Geben Sie für die `Authentication-Type` Dimension den folgenden Wert ein:

Wert	Typ	Beschreibung
`LDAP`,`SAML`, `Local`, `Radius`, `TACACS`, `SAMLIDP`, oder `OTP`.	Zeichenfolge	Authentifizieren Sie Ihre Benutzer mit einer der verfügbaren Methoden.

Backend-Server-Name

Geben Sie für die `Backend-Server-Name` Dimension den folgenden Wert ein:

Wert	Typ	Beschreibung
Beispiel:`10.xxx.xxx.xx`	Zeichenfolge	IP-Adresse des Back-End-Servers.

Browser

Geben Sie für die `Browser` Dimension den folgenden Wert ein:

Wert	Typ	Beschreibung
`PN Agent`, `Edge`, `Firefox`, `Chrome`, oder `Safari`.	Zeichenfolge	Verwendeter Browser.

Ort

Geben Sie für die `City` Dimension den folgenden Wert ein:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Wert	Typ	Beschreibung
Beispiele: `Boston`, `Beijing`	Zeichenfolge	Stadt, von wo aus sich der Benutzer angemeldet hat.

Client-IP

Geben Sie für die `Client-IP` Dimension den folgenden Wert ein:

Wert	Typ	Beschreibung
Beispiel:`10.xxx.xxx.xx`	Zeichenfolge	IP-Adresse des Benutzergeräts.

Client-IP-Typ

Geben Sie für die `Client-IP-Type` Dimension den folgenden Wert ein:

Wert	Typ	Beschreibung
öffentlich, privat	Zeichenfolge	Gibt an, ob die IP-Adresse des Benutzers öffentlich oder privat ist.

> **Hinweis**
>
> Bei den Werten wird Groß-/Kleinschreibung beachtet Geben Sie die Werte in Kleinbuchstaben ein.

Client-Port

Geben Sie für die `Client-Port` Dimension den folgenden Wert ein:

Wert	Typ	Beschreibung
Beispiel:`45334`	Zahl	Portnummer des Benutzergeräts.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Land

Geben Sie für die `Country` Dimension den folgenden Wert ein:

Wert	Typ	Beschreibung
Beispiele: `United States`, `India`	Zeichenfolge	Land, aus dem sich der Benutzer angemeldet hat.

> **Hinweis**
>
> Schließen Sie den Wert in “”ein, wenn der Wert Leerzeichen enthält. **Beispiel**: Land = “Vereinigt Staaten”.

Event-Typ

Geben Sie für die `Event-Type` Dimension den folgenden Wert ein:

Wert	Typ	Beschreibung
Authentifizierung, ICA-Datei, Sitzungsabmeldung	Zeichenfolge	Art der Benutzerereignisse.

Gateway-FQDN

Geben Sie für die `Gateway-FQDN` Dimension den folgenden Wert ein:

Wert	Typ	Beschreibung
Beispiel:`Gateway-test`	Zeichenfolge	Domainname Ihres Citrix Gateway.

Gateway-IP

Geben Sie für die `Gateway-IP` Dimension den folgenden Wert ein:

Wert	Typ	Beschreibung
Beispiel:`10.xxx.xxx.xx`	Zeichenfolge	IP-Adresse Ihres Citrix Gateway.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Gateway-Port

Geben Sie für die `Gateway-Port` Dimension den folgenden Wert ein:

Wert	Typ	Beschreibung
Beispiel:`443`	Zeichenfolge	Portnummer Ihres Citrix Gateway.

Abmelde-Modus

Geben Sie für die `Logout-Mode` Dimension den folgenden Wert ein:

Wert	Typ	Beschreibung
`"Internal error"`, `"Inactive time out"`, `"User initiated logout"`, oder `"Administrator killed session"`.	Zeichenfolge	Grund für das Timeout oder die Beendigung der VPN-Sitzung.

> **Hinweis**
>
> Schließen Sie den Wert in “”ein, wenn der Wert Leerzeichen enthält. **Beispiel**: Logout-Modus = `"Internal error"`.

NetScaler-IP

Geben Sie für die `NetScaler-IP` Dimension den folgenden Wert ein:

Wert	Typ	Beschreibung
Beispiel:`10.xxx.xx.xx`	Zeichenfolge	IP-Adresse Ihrer Citrix ADC Appliance.

Betriebssystem

Geben Sie für die `OS` Dimension den folgenden Wert ein:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Wert	Typ	Beschreibung
Beispiele: `MAC_OS`, `WINDOWS`	Zeichenfolge	Betriebssystem des Benutzergeräts.

Datensatztyp

Geben Sie für die `Record Type` Dimension den folgenden Wert ein:

Wert	Typ	Beschreibung
`VPN_AI`	Zeichenfolge	Zeigt Benutzerereignisse im Zusammenhang mit Authentifizierung an.
`VPN_IF`	Zeichenfolge	Zeigt Benutzerereignisse im Zusammenhang mit ICA-Datei an.
`VPN_ST`	Zeichenfolge	Zeigt Benutzerereignisse im Zusammenhang mit der Sitzungsabmeldung an.

SSO-Authentifizierungsmethode

Geben Sie für die `SSO-Authentication-Method` Dimension den folgenden Wert ein:

Wert	Typ	Beschreibung
`NSAUTH_BEARER`, `NSAUTH_FORM`, `NSAUTH_CITRIXAGBASIC`, `NSAUTH_NEGOTIATE`, `NSAUTH_NTLM`, oder `NSAUTH_BASIC`.	Zeichenfolge	Verschiedene Methoden der Single Sign-On-Authentifizierung.

Server-IP

Geben Sie für die `Server-IP` Dimension den folgenden Wert ein:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Wert	Typ	Beschreibung
Beispiel:`10.xx.xxx.xx`	Zeichenfolge	IP-Adresse des Back-End-Servers.

Server-Port

Geben Sie für die `Server-Port` Dimension den folgenden Wert ein:

Wert	Typ	Beschreibung
Beispiel:`47054`	Zahl	Portnummer des Back-End-Servers.

Sitzungs-Status

Geben Sie für die `Session-State` Dimension den folgenden Wert ein:

Wert	Typ	Beschreibung
`"Set Client State"`, `"Authorization State"`, `"SSO State"`, und `"Application Bandwidth Update"`	Zeichenfolge	Der Status der VPN-Sitzung.

> **Hinweis**
>
> Schließen Sie den Wert in “”ein, wenn der Wert Leerzeichen enthält. **Beispiel**: Session-State = `"Set Client State"`.

Status-Code

Geben Sie für die `Status-Code` Dimension den folgenden Wert ein:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Wert	Typ	Beschreibung
`"Successful login"`, `"Invalid credentials passed"`, `"Post auth failed and connection quarantined"`, `"Login not permitted"`, `"Maximum login failures reached"`	Zeichenfolge	Der VPN-Statuscode.

> **Hinweis**
>
> Schließen Sie den Wert in “”ein, wenn der Wert Leerzeichen enthält. **Beispiel**: Session-Code = `"Successful login"`.

Benutzer-Agent

Geben Sie für die `User-Agent` Dimension den folgenden Wert ein:

Wert	Typ	Beschreibung
`IPHONEIPAD`, oder `WINPHONE`	Zeichenfolge	Der Agent oder das Gerät, mit dem auf das VPN zugegriffen wurde.

VPN-Session-ID

Geben Sie für die `VPN-Session-ID` Dimension den folgenden Wert ein:

Wert	Typ	Beschreibung
`c2c290c61dfe4e07247bde1e21463d12`	Zeichenfolge	Sitzungs-ID, die vom Server für die VPN-Sitzung eines Benutzers zugewiesen wurde.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

VPN-Sitzungsmodus

Geben Sie für die `VPN-Session-Mode` Dimension den folgenden Wert ein:

Wert	Typ	Beschreibung
`"Full Tunnel""ICA Proxy"`, oder `Clientless`	Zeichenfolge	Verschiedene Modi der VPN-Sitzung eines Benutzers.

> **Hinweis**
>
> Schließen Sie den Wert in “”ein, wenn der Wert Leerzeichen enthält. **Beispiel**: Session-Code = `"Full Tunnel"`.

Self-Service-Suche für Richtlinien

May 4, 2022

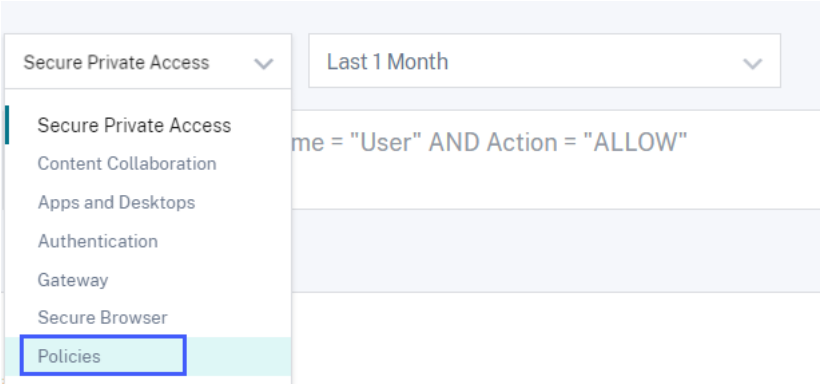
Citrix Analytics for Security ermöglicht es Ihnen, Richtlinien zu erstellen und Aktionen für ungewöhnliche oder verdächtige Ereignisse auf Benutzerkonten anzuwenden. Wenn die Benutzerereignisse Ihren definierten Richtlinien entsprechen, werden die Aktionen automatisch auf die Benutzerkonten angewendet, um die Bedrohung zu isolieren und das Auftreten zukünftiger anomaler Ereignisse zu verhindern. Mithilfe der Self-Service-Suche können Sie die Benutzerereignisse anzeigen, die Ihren definierten Richtlinien entsprechen, und die auf diese anomalen Ereignisse angewendeten Aktionen anzeigen.

Weitere Informationen zu den Suchfunktionen finden Sie unter **Self-Service-Suche**.

Wählen Sie den Datensatz Richtlinien

Um die Ereignisse im Zusammenhang mit den definierten Richtlinien anzuzeigen, wählen Sie **Richtlinien** aus der Liste aus. Standardmäßig zeigt die Self-Service-Seite die Ereignisse für den letzten Tag an. Sie können auch den Zeitraum auswählen, für den Sie die Ereignisse anzeigen möchten.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

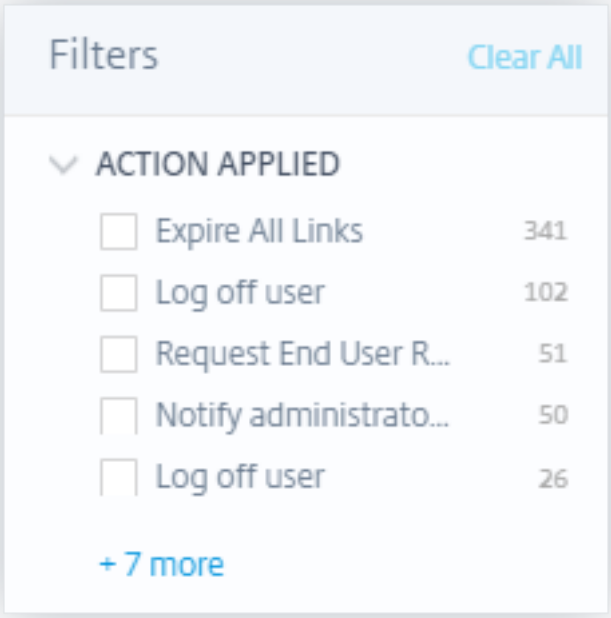


Hinweis

Sie können auch über das Dashboard **Sicherheit** > **Benutzer** > Richtlinien **und Aktionen auf die Seite Self-Service-Suche nach Richtlinien** zugreifen. Wählen Sie eine Richtlinie im Dashboard aus, um die Benutzerereignisse im Zusammenhang mit der Richtlinie anzuzeigen. Weitere Informationen finden Sie im Dashboard Richtlinien und Aktionen .

Wählen Sie die Facetten aus, um Ereignisse zu filtern

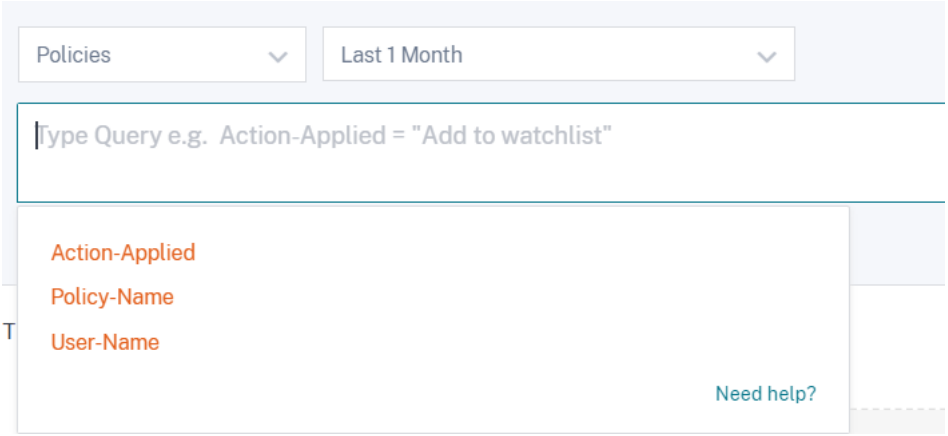
Die Facettenliste zeigt die angewendeten Aktionen für die Benutzerereignisse an. Wählen Sie die angewendeten Aktionen aus der Facettenliste aus und zeigen Sie die Ereignisse basierend auf den angewendeten Aktionen an. Weitere Informationen zu den Aktionen, die Sie beim Konfigurieren von Richtlinien anwenden können, finden Sie unter Was sind Aktionen?



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

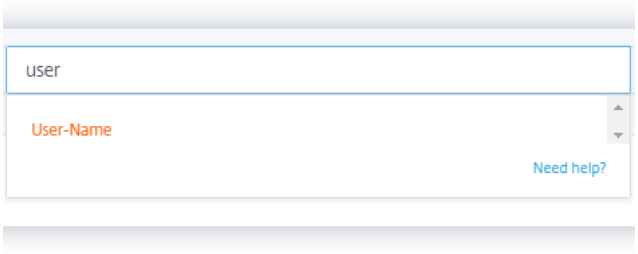
Angeben der Suchabfrage zum Filtern von Ereignissen

Platzieren Sie den Cursor in das Suchfeld, um die Liste der Dimensionen für die Ereignisse im Zusammenhang mit Richtlinien anzuzeigen. Verwenden Sie die Dimensionen und die Operatoren, um Ihre Abfrage anzugeben und nach den erforderlichen Ereignissen zu suchen.

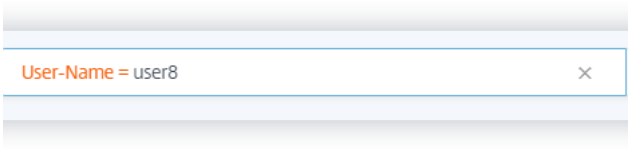


Sie möchten beispielsweise die anomalen Ereignisse eines Benutzers “user8”anzeigen, bei dem die für diese Ereignisse angewendete Aktion “Benutzer deaktivieren”lautet.

1. Geben Sie “Benutzer”in das Suchfeld ein, um die zugehörigen Dimensionen abzurufen.



2. Wählen Sie **Benutzername** und geben Sie den Wert “user8”mit dem Gleichheitsoperator ein.

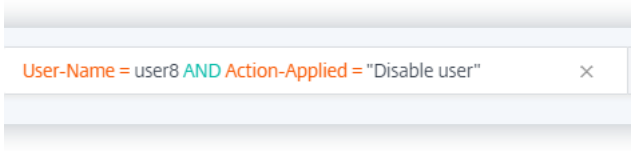


3. Wählen Sie den Operator **UND** und wählen Sie dann die Dimension **Aktion Angewendet** aus. Geben Sie die Zeichenfolge “Benutzer deaktivieren”für **Aktion unter Verwendung des** Gleichheits-Operators ein.

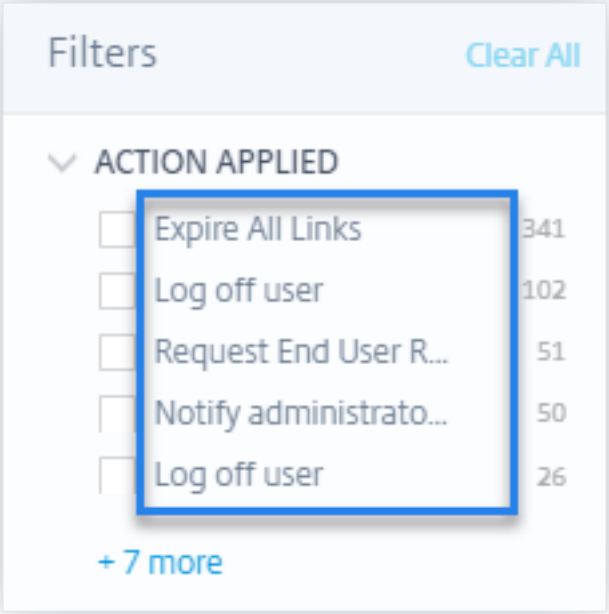
> **Hinweis**
>
> Wenn der Zeichenfolgenwert zwei oder mehr Wörter enthält, muss er mit dem Operator

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> eingeschlossen werden “” <!--NeedCopy-->. Zum Beispiel “Disable user” <!--NeedCopy-->“Session Recording beenden”.



Um die möglichen Zeichenfolgenwerte für **Action-Applied**zu identifizieren, erweitern Sie die Facettenliste und verwenden Sie den Filternamen als Zeichenfolge in Ihrer Suchanfrage.



4. Wählen Sie den Zeitraum aus, und klicken Sie auf **Suchen**, um die Ereignisse in der Tabelle **DATA** anzuzeigen.

Self-Service-Suche für Remote-Browserisolierung (Secure Browser)

December 12, 2023

Verwenden Sie die Self-Service-Suche, um Einblicke in die Browsersitzungen der Citrix Workspace-Benutzer zu erhalten, die den Citrix Remote Browser Isolation Service verwenden. Citrix Remote Browser Isolation ist ein Cloud-Dienst, der ein sicheres Surfen im Internet bietet, ohne die Sicherheit Ihres Unternehmensnetzwerks zu gefährden. Wenn Benutzer mithilfe der Remote Browser

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Isolation auf Webanwendungen zugreifen, werden für jede Benutzerverbindung Ereignisse wie Sitzungsverbindung, Sitzungsstart, veröffentlichte Anwendungen und gelöschte Anwendungen generiert. Citrix Analytics for Security empfängt diese Ereignisse und zeigt sie auf der Self-Service-Seite an. Sie können die Benutzer und ihre Browsersitzungen verfolgen.

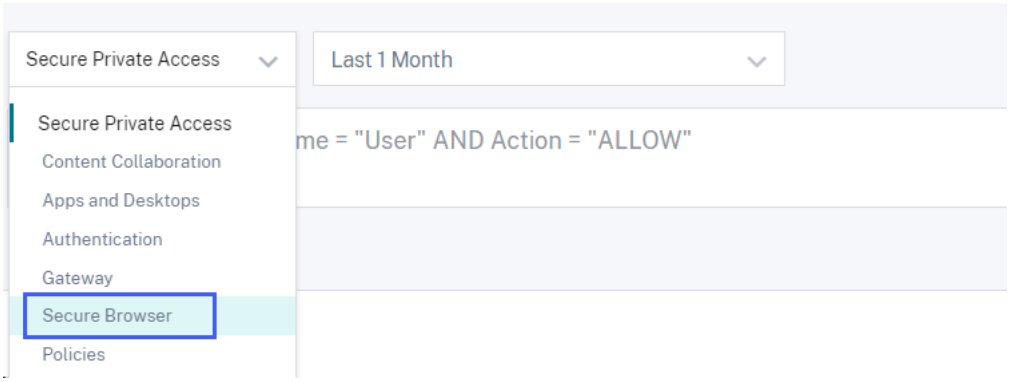
Weitere Informationen zu den Suchfunktionen finden Sie unter **Self-Service-Suche**.

Voraussetzung

Um Ereignisse aus einer Remote-Browser-Isolation zu empfangen, aktivieren Sie die **Hostnamen-Nachverfolgung** in der Remote-Browser-Isolation, um Hostnamen für die Benutzersitzungen zu protokollieren. Diese Informationen werden an Citrix Analytics for Security gesendet. Weitere Informationen finden Sie unter Veröffentlichte Remote-Browser-Isolationen verwalten.

Remote Browser Isolation-Datenquelle auswählen

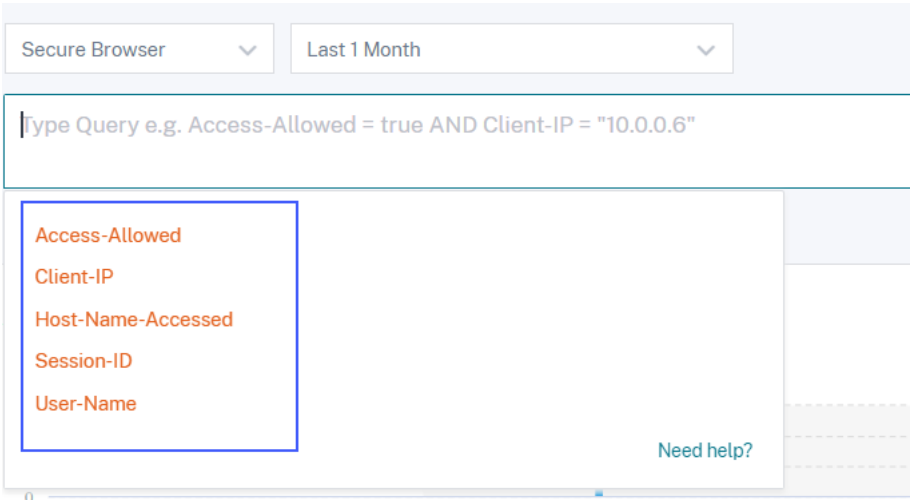
Um die Remote Browser Isolation-Ereignisse anzuzeigen, wählen Sie **Remote Browser Isolation** aus der Liste aus. Standardmäßig zeigt die Self-Service-Seite die Ereignisse für den letzten Tag an. Sie können auch den Zeitraum auswählen, für den Sie die Ereignisse anzeigen möchten.



Angeben der Suchabfrage zum Filtern von Ereignissen

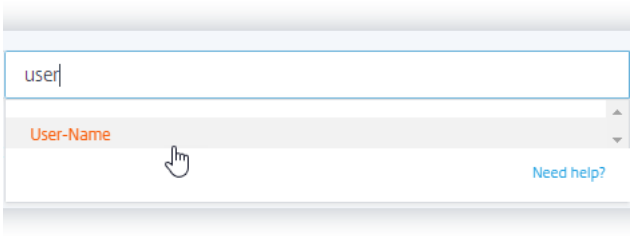
Platzieren Sie den Cursor in das Suchfeld, um die Liste der Dimensionen für die Remote Browser Isolation Events anzuzeigen. Verwenden Sie die Dimensionen und die Operatoren, um Ihre Abfrage anzugeben und nach den erforderlichen Ereignissen zu suchen.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

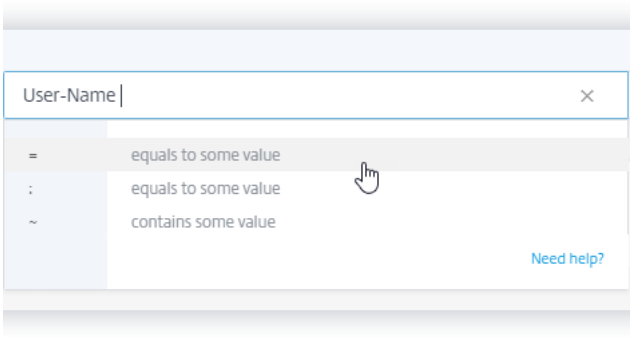


Sie möchten beispielsweise die Browser-Ereignisdetails für einen Benutzer "aa"anzeigen, der berechtigt ist, auf verschiedene Hostdienste wie google.com, amazon.com zuzugreifen.

1. Geben Sie "Benutzer"in das Suchfeld ein, um die zugehörigen Dimensionen anzuzeigen.



2. Klicken Sie auf **Benutzername** und geben Sie den Wert "aa"mit dem Gleichheitsoperator ein.



3. Wählen Sie den Operator **UND** die **Dimension Zugriff ermöglichen** aus. Weisen Sie **Allow-Access** mithilfe des Gleichheitsoperator den Wert "true"zu. Der "true"-Wert gibt an, dass der Benutzer auf die Hostdienste zugreifen kann.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

4. Wählen Sie den Zeitraum aus, und klicken Sie auf **Suchen**, um die Ereignisse in der Tabelle **DATA** anzuzeigen.

Details zu Benutzerereignis anzeigen

Sie können die folgenden Daten anzeigen, die Sie vom Remote Browser Isolation Service erhalten haben:

- **Uhrzeit**- Datum und Uhrzeit, wann das Benutzerereignis eingetreten ist.
- **Benutzername**—Der Benutzer, der das Ereignis initiiert hat.
- **Sitzungs-ID**—Die eindeutige Nummer, die der Benutzersitzung zugewiesen wurde.
- **Client-IP**—IP-Adresse des Benutzergeräts.
- **Hostname**—Der Hostdienst, auf den der Benutzer über das Netzwerk zugreifen kann.
- **Zugriff zulassen**- Dem Benutzer wird der Zugriff auf den Hostdienst gewährt oder verweigert.

Self-Service-Suche für Secure Private Access

April 12, 2024

Verwenden Sie die Self-Service-Suche, um Einblicke in die Zugriffsereignisse der Citrix Cloud-Benutzer in Ihrem Unternehmen zu erhalten. Beispiele für Zugriffsereignisse sind URL-Kategorie, Inhaltskategorie, Browser und Geräte. Citrix Analytics for Security empfängt diese Ereignisse vom Secure Private Access-Dienst und zeigt sie bei der Self-Service-Suche an. Sie können die Benutzer und ihre Zugriffsdetails verfolgen.

Weitere Informationen zu den Suchfunktionen finden Sie unter **Self-Service-Suche**.

> **Hinweis**
>
> Die folgenden Funktionen von Citrix Analytics for Security sind beeinträchtigt, da die kategorienbasierte Webfilterung durch Secure Private Access nicht mehr unterstützt wird:
>
> 1. Datenfelder wie Kategorie-Gruppe, Kategorie und Reputation von URLs sind im Citrix Analytics for Security Dashboard nicht mehr verfügbar.
> 2. Der Indikator für riskante Website-Zugriffe, der auf denselben Daten basiert, ist ebenfalls veraltet und wird für Kunden nicht ausgelöst.
> 3. Alle vorhandenen benutzerdefinierten Risikoindikatoren, die die Datenfelder (Kategorie-

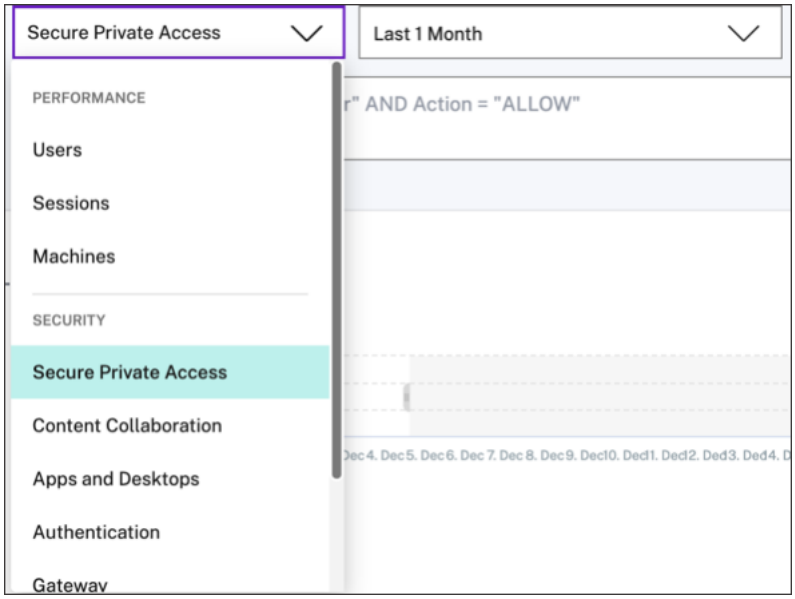
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> Gruppe, Kategorie und Reputation von URLs) und die zugehörigen Richtlinien verwenden, werden nicht mehr ausgelöst.

Einzelheiten zur Einstellung von Secure Private Access finden Sie unter Veraltete Funktionen.

Wählen Sie die Secure Private Access-Datenquelle

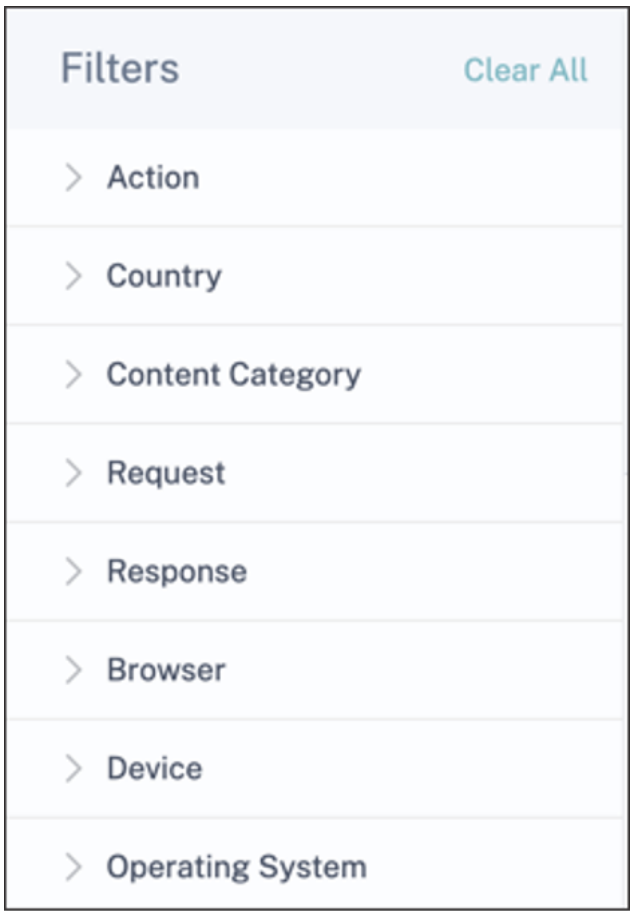
Um die Secure Private Access-Ereignisse anzuzeigen, wählen Sie **Secure Private Access** aus der Liste aus. Standardmäßig zeigt die Self-Service-Seite die Ereignisse für den letzten Tag an. Sie können auch den Zeitraum auswählen, für den Sie die Ereignisse anzeigen möchten.



Wählen Sie die Facetten aus, um Ereignisse zu filtern

Verwenden Sie die folgenden Facetten, die mit den Secure Private Access-Ereignissen verknüpft sind.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

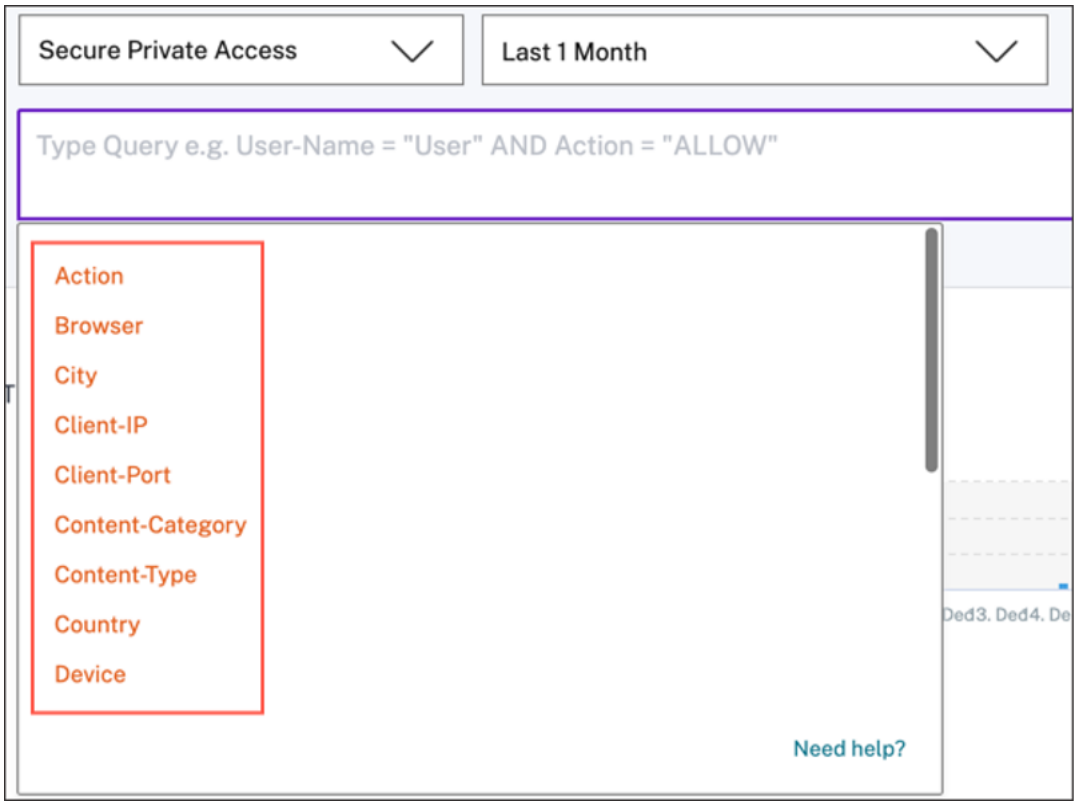


- **Aktion**- Suchen Sie nach Ereignissen basierend auf den Aktionen, die in den Anwendungen der Benutzer wie Zulassen, Blockieren und Umleiten ergriffen wurden.
- **Land**—Suchen Sie nach Ereignissen auf der Grundlage der Zugriffsorte der Benutzer.
- **Inhaltskategorie**- Suche nach Ereignissen basierend auf den Kategorien von Inhalten, auf die zugegriffen wird, wie Anwendung, Bild und Text.
- **Anfrage**- Suchen Sie Ereignisse basierend auf den HTTP-Methoden wie GET, POST, PUT, DELETE.
- **Response**- Suche nach Ereignissen basierend auf der HTTP-Antwort.
- **Browser**- Suchen Sie nach Ereignissen basierend auf den von den Benutzern verwendeten Browsern.
- **Gerät**- Suche nach Ereignissen basierend auf den verwendeten Geräten wie Android-Handys, iPhones, MacBook.
- **Betriebssystem**- Suchen Sie Ereignisse basierend auf den Betriebssystemen, die auf den Geräten installiert sind.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

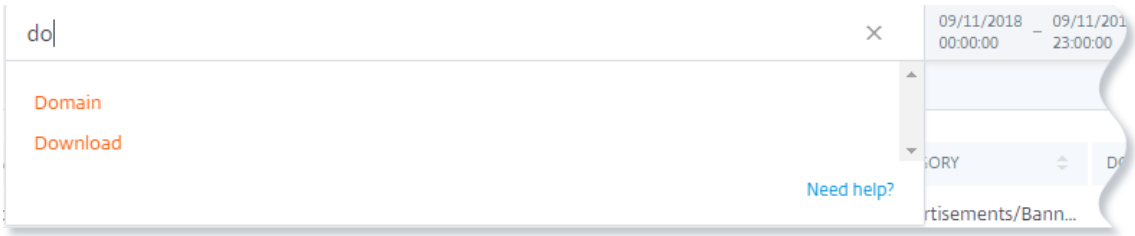
Angeben der Suchabfrage zum Filtern von Ereignissen

Platzieren Sie den Cursor in das Suchfeld, um die Liste der Dimensionen für die Secure Private Access-Ereignisse anzuzeigen. Verwenden Sie die Dimensionen und die Operatoren, um Ihre Abfrage anzugeben und nach den erforderlichen Ereignissen zu suchen.



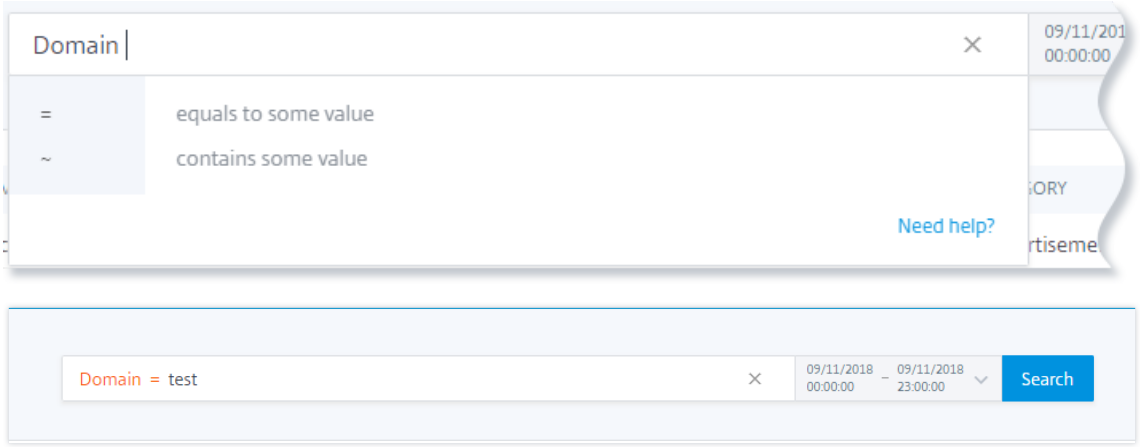
Beispielsweise möchten Sie die Testdomänen anzeigen, in denen das Daten-Download-Volume mehr als 2.000 Byte beträgt. Geben Sie Ihre Suchanfrage wie folgt an:

1. Geben Sie “do”in das Suchfeld ein, um die entsprechenden Vorschläge zu erhalten.

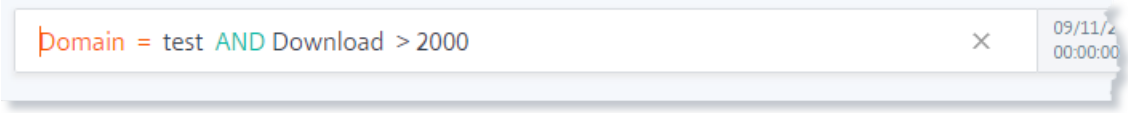


2. Klicken Sie auf **Domäne** und geben Sie dann den Wert “test”mit dem Gleichheitsoperator an.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



3. Verwenden Sie den Operator **UND** und wählen Sie dann die Dimension **Download** aus. Wählen Sie den Operator **>** und geben Sie das Download-Volume in Byte ein.



4. Wählen Sie den Zeitraum aus, und klicken Sie auf **Suchen**, um die Ereignisse in der Tabelle **DATA** anzuzeigen.

Self-Service-Suche für Apps und Desktops

February 9, 2024

Verwenden Sie die Self-Service-Suche, um Einblicke in die Benutzerereignisse zu erhalten, die von der Citrix Virtual Apps and Desktops Datenquelle und der Citrix DaaS-Datenquelle (ehemals Citrix Virtual Apps and Desktops Service) empfangen wurden. Wenn Benutzer virtuelle Apps oder virtuelle Desktops verwenden, werden Ereignisse generiert, die ihren Aktivitäten und Aktionen entsprechen. Beispiele für Benutzerereignisse sind Dateidownload, Kontoanmeldung und App-Start. Citrix Analytics for Security empfängt diese Benutzerereignisse und zeigt sie auf der Self-Service-Seite an. Sie können die Benutzer und ihre Aktivitäten verfolgen.

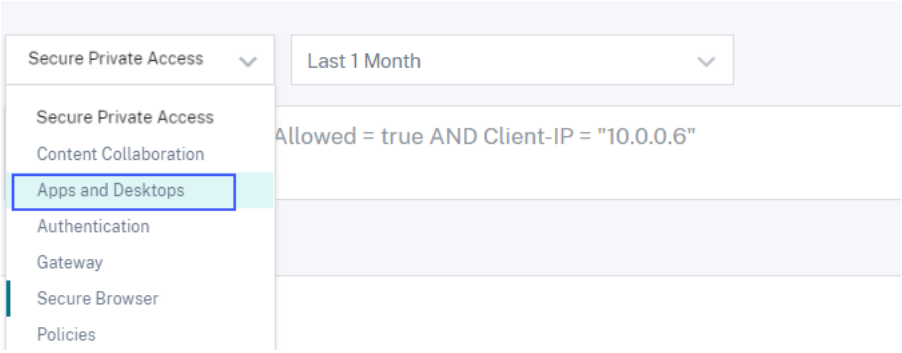
Weitere Informationen zu den Suchfunktionen finden Sie unter **Self-Service-Suche**.

Wählen Sie die Datenquelle Apps und Desktops aus

Um die Ereignisse von Citrix Virtual Apps and Desktops oder Citrix DaaS anzuzeigen, wählen Sie **Apps and Desktops** aus der Liste aus. Standardmäßig zeigt die Self-Service-Seite die Ereignisse für

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

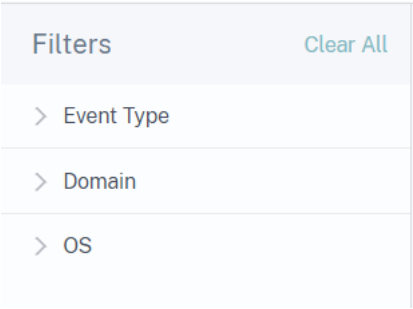
den letzten Tag an. Sie können auch den Zeitraum auswählen, für den Sie die Ereignisse anzeigen möchten.



Standardmäßig werden auf der Self-Service-Seite die Ereignisse des letzten Monats angezeigt. Die Seite bietet Ihnen auch mehrere Facetten und ein Suchfeld, um die erforderlichen Ereignisse zu filtern und sich auf sie zu konzentrieren.

Wählen Sie die Facetten aus, um Ereignisse zu filtern

Verwenden Sie die folgenden Facetten, die mit den Ereignissen Apps und Desktops verknüpft sind.

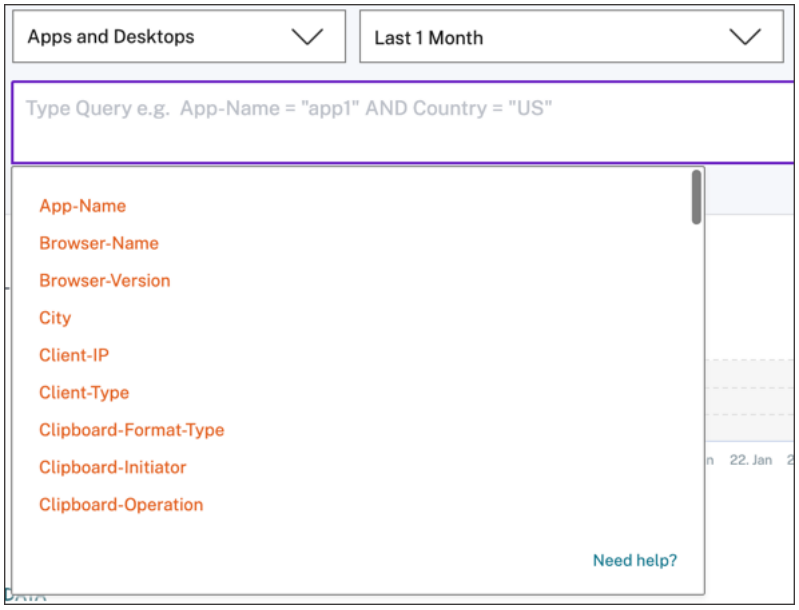


- **Ereignistyp**—Sucht anhand des Ereignistyps nach Ereignissen wie Kontoanmeldung, App-Ende und Sitzungsende.
- **Domain**- Suchen Sie Ereignisse basierend auf den Domänen wie citrate.net.
- **OS**- Suchen Sie nach Ereignissen basierend auf den Betriebssystemen wie Chrome, iOS und Windows, die auf dem Gerät des Benutzers verwendet werden. Wählen Sie den Namen und die Versionen des Betriebssystems aus, um die Ereignisse zu filtern. Weitere Informationen zu den Betriebssystemversionen finden Sie unter Unterstützte Werte für Ihre Suchanfrage.

Angeben der Suchabfrage zum Filtern von Ereignissen

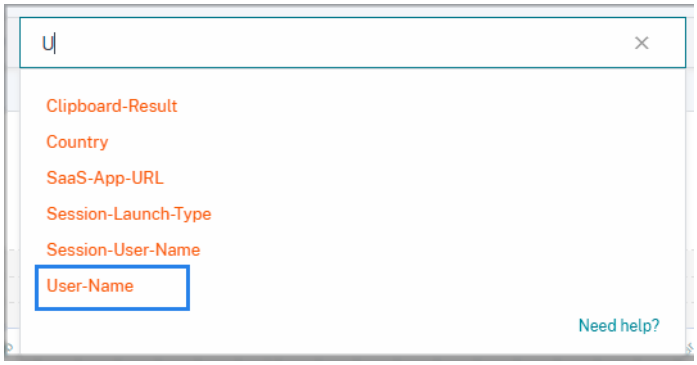
Platzieren Sie den Cursor in das Suchfeld, um die Liste der Dimensionen für die Apps- und Desktops-Ereignisse anzuzeigen. Verwenden Sie die Dimensionen und die Operatoren, um Ihre Abfrage anzugeben und nach den erforderlichen Ereignissen zu suchen.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

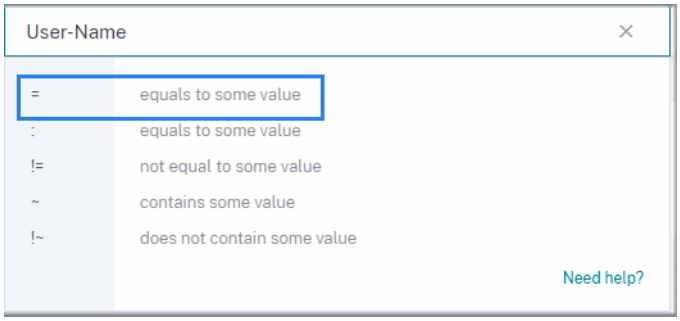


Sie möchten beispielsweise nach Ereignissen für den Benutzer "John Doe"suchen, der das Windows-Betriebssystem verwendet.

1. Geben Sie "U"in das Suchfeld ein, um die entsprechenden Vorschläge zu erhalten.



2. Klicken Sie auf **Benutzername** und geben Sie den Wert "John"mit dem Gleichheitsoperator ein.



3. Wählen Sie den Operator **UND** die Dimension des **Betriebssystemnamens** aus. Weisen Sie den Wert "Windows 7"mit dem Gleichheitsoperator zu.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
User-Name = "John" AND OS-Name = "Windows 7"
```

4. Wählen Sie den Zeitraum aus, und klicken Sie auf **Suchen**, um die Ereignisse basierend auf der Tabelle **DATA** anzuzeigen.

Ereignistypen und unterstützte Felder

Die folgenden Felder sind für alle Ereignistypen außer VDA.print verfügbar:

- Ort
- Client-IP
- Land
- Geräte-ID
- Betriebssystemname
- Betriebssystemversion
- Zusätzliche OS-Informationen
- Zeit
- Benutzername
- Version der Workspace App
- Status der Workspace-App

In der folgenden Tabelle werden die für die Apps and Desktops-Datenquelle verfügbaren Ereignistypen sowie die für jeden Ereignistyp spezifischen Felder beschrieben.

Wert	Beschreibung	Felder
`Account.Logon`	Wird ausgelöst, wenn Sie sich über die Citrix Workspace-App am Store anmelden. **Hinweis**: Account.Logon ist für den HTML5-Client nicht verfügbar.	Überprüfen Sie die allgemeinen Felder wie oben beschrieben.
`Session.Logon`	Wird ausgelöst, wenn Sie sich bei Ihrer virtuellen Sitzung anmelden.	App-Schutzrichtlinien, Domäne, Sitzungsstarttyp, Sitzungsservername, Sitzungsbenutzername

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Wert	Beschreibung	Felder
`Session.End`	Wird ausgelöst, wenn Sie Ihre virtuelle Sitzung beenden.	Domäne, Sitzungsstarttyp, Name des Sitzungsservers, Sitzungsbenutzername
`App.Start`	Wird ausgelöst, wenn Sie eine virtuelle App-Sitzung starten. **Hinweis**: Dieser Ereignistyp ist nicht anwendbar, wenn die Anwendung innerhalb der Desktop-Sitzung gestartet wird.	App-Name, Domäne, Sitzungsstarttyp, Sitzungsservername, Sitzungsbenutzername
`App.End`	Wird ausgelöst, wenn Sie eine virtuelle App-Sitzung beenden. **Hinweis**: Dieser Ereignistyp ist nicht anwendbar, wenn die Anwendung innerhalb der Desktop-Sitzung gestartet wird.	App-Name, Domäne, Sitzungsstarttyp, Sitzungsservername, Sitzungsbenutzername
`File.Download`	Wird ausgelöst, wenn ein Benutzer eine Datei von einer virtuellen Remote-Sitzung auf das Client-Gerät kopiert. Es wird nicht ausgelöst, wenn Dateiübertragungen innerhalb der virtuellen Sitzungen stattfinden. **Hinweis**: Dieser Ereignistyp wird nur gesendet, wenn der Server die Dateiumleitung zulässt (weitere Informationen finden Sie in den Einstellungen für die Dateiumleitung) und die **Dateizugriffseinstellung** im Client-Workspace auf **Lesen und**Schreiben gesetzt ist.	Domäne, Gerätetyp herunterladen, Name der Download-Datei, Download-Dateipfad, Download-Dateigröße, Name des Sitzungsservers, Sitzungsbenutzername

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Wert	Beschreibung	Felder
`Printing`	Wird ausgelöst, wenn Sie eine Datei mit der von der Citrix Workspace-App gestarteten Sitzung über einen Clientdrucker drucken. **Hinweis**: Bei der Citrix Workspace-App gibt es zwei technische Einschränkungen, die sich auf Druckereignisse auswirken. Erstens ist die Telemetrie des Namens des gedruckten Dokuments aufgrund eines bekannten Problems bei allen Plattformvarianten nicht im Druckvorgang enthalten. Zweitens ist die Telemetrie "Größe der gedruckten Datei" aufgrund einer anderen bekannten technischen Einschränkung nicht im Druckvorgang für Windows enthalten. Um diese Datensätze (Dateiname/Dateigröße) zu sammeln, verwenden Sie das VDA.print-Ereignis. Weitere Informationen finden Sie unter Aktivieren der Drucktelemetrie für Citrix DaaS.	Browsername, Browserversion, Domäne, Druckername, Druckdateiformat, Druckdateigröße, Name des Sitzungsservers, Sitzungsbenutzername
`AppProtection.ScreenCapture`	Wird ausgelöst, wenn ein Benutzer versucht, in einer geschützten Sitzung einen Screenshot aufzunehmen. **Hinweis**: Weitere Informationen finden Sie unter App-Schutz.	Geschützte App-Titel, Name des Bildschirmaufnahmetools, Pfad zum Bildschirmaufnahmetool

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Wert	Beschreibung	Felder
App.SaaS.Launch	Wird ausgelöst, wenn die Citrix Workspace-App eine SaaS-App im Citrix Enterprise Browser startet.	Browsername, Browserversion, SaaS-App-Name, SaaS-App-URL
App.SaaS.End	Wird ausgelöst, wenn die Citrix Workspace-App eine SaaS-App im Citrix Enterprise Browser schließt.	Browsername, Browserversion, SaaS-App-URL
App.SaaS.Clipboard	Wird ausgelöst, wenn ein Zwischenablagevorgang im Citrix Enterprise Browser ausgeführt wird.	Browsername, Browserversion, Formatgröße der Zwischenablagedetails, Formattyp der Zwischenablagedetails, Initiator der Zwischenablagedetails, Ergebnis der Zwischenablagedetails, Vorgang der Zwischenablage, SaaS-App-URL
App.SaaS.File.Download	Wird ausgelöst, wenn eine Datei im Citrix Enterprise Browser heruntergeladen wird.	Browsername, Browserversion, Download-Gerätetyp, Download-Dateipfad, Download-Dateigröße
App.SaaS.File.Print	Wird ausgelöst, wenn das Drucken im Citrix Enterprise Browser initiiert wird.	Browsername, Browserversion, Name der Druckdatei, Name der SaaS-App, SaaS-App-URL
App.SaaS.Url.Navigate	Wird ausgelöst, wenn der Citrix Enterprise Browser durch eine URL navigiert.	Browsername, Browserversion, SaaS-App-Name, SaaS-App-URL
Citrix.EventMonitor.AppStart	Wird ausgelöst, wenn eine Anwendung, die der App-Überwachungsliste des Sitzungsaufzeichnungsservers hinzugefügt wurde, innerhalb einer virtuellen Desktop-Sitzung gestartet wird.	App-Name

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Wert	Beschreibung	Felder
Citrix.EventMonitor.AppEnd	Wird ausgelöst, wenn eine Anwendung, die der App-Überwachungslistedes Sitzungsaufzeichnungsservers hinzugefügt wurde, innerhalb einer virtuellen Desktop-Sitzung gestoppt wird.	App-Name
Citrix.EventMonitor.Clipboard	Wird ausgelöst, wenn eine Aktion in der Zwischenablage innerhalb einer Sitzungsaufzeichnung ausgeführt wurde.	Typ des Zwischenablage-Datenformats, Prozessname, Fenstertitel
Citrix.EventMonitor.FileTransfer	Wird ausgelöst, wenn ein Benutzer eine Datei zwischen einer virtuellen Desktop-Sitzung und dem Computer des Benutzers überträgt.	Dateigröße, Betriebsrichtung (Host zu Client, Client zu Host), Quellpfad, Zielpfad
Citrix.EventMonitor.RegistryChange	Wird ausgelöst, wenn ein Registrierungsvorgang ausgeführt wird. Die möglichen Registrierungsvorgänge sind Erstellen, Löschen, Umbenennen, Wert festlegen und Wert löschen.	Registrierungsvorgang, Registrierungsname, Registrierungspfad, Prozess-ID, Prozessdateipfad
Citrix.EventMonitor.SessionEnd	Wird ausgelöst, wenn eine Sitzungsaufzeichnung endet.	Beschreibung
Citrix.EventMonitor.SessionLaunch	Wird ausgelöst, wenn eine Sitzungsaufzeichnung gestartet wurde.	Typ der Sitzungsaufzeichnung
Citrix.EventMonitor.TopMost	Wird ausgelöst, wenn sich das oberste Fenster ändert.	App-Name
Citrix.EventMonitor.IdleStart	Wird ausgelöst, wenn die Sitzung inaktiv wird.	Überprüfen Sie die allgemeinen Felder wie oben beschrieben.
Citrix.EventMonitor.IdleEnd	Wird ausgelöst, wenn die inaktive Sitzung endet.	Überprüfen Sie die allgemeinen Felder wie oben beschrieben.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Wert	Beschreibung	Felder
`Citrix.EventMonitor.WebBrowsing`	Wird ausgelöst, wenn der Benutzer innerhalb einer virtuellen Desktop-Sitzung mit Webseiten in Browsern interagiert.	App-Name, URL
`Citrix.EventMonitor.FileCreate`	Wird ausgelöst, wenn eine Datei oder ein Ordner in einer virtuellen Desktop-Sitzung im Pfad des überwachten Dateisystems erstellt wird.	Dateiname, Dateipfad, Dateigröße
`Citrix.EventMonitor.FileRename`	Wird ausgelöst, wenn eine Datei oder ein Ordner in einer virtuellen Desktop-Sitzung im Pfad des überwachten Dateisystems umbenannt wird.	Überprüfen Sie die allgemeinen Felder wie oben beschrieben.
`Citrix.EventMonitor.FileMove`	Wird ausgelöst, wenn eine Datei oder ein Ordner aus dem Pfad des überwachten Dateisystems in einer virtuellen Desktop-Sitzung oder zwischen Sitzungshosts (VDAs) und Clientgeräten verschoben wird.	Überprüfen Sie die allgemeinen Felder wie oben beschrieben.
`Citrix.EventMonitor.FileDelete`	Wird ausgelöst, wenn eine Datei oder ein Ordner im Pfad des überwachten Dateisystems in einer virtuellen Desktop-Sitzung gelöscht wird.	Dateiname, Dateipfad, Dateigröße
`Citrix.EventMonitor.CDMUSBDriveAttach`	Wird ausgelöst, wenn ein USB-Massenspeichergerät, dem Client Drive Mapping (CDM) zugeordnet ist, in einen Client gesteckt wird, von dem aus die virtuelle Apps- und Desktop-Sitzung verbunden ist.	Überprüfen Sie die allgemeinen Felder wie oben beschrieben.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Wert	Beschreibung	Felder
`Citrix.EventMonitor.GenericUSBDriveAttach`	Wird ausgelöst, wenn ein vom Typ Generic umgeleitetes USB-Massenspeichergerät in einen Client gesteckt wird, von dem aus die virtuelle Apps- und Desktop-Sitzung verbunden ist.	Überprüfen Sie die allgemeinen Felder wie oben beschrieben.
`Citrix.EventMonitor.RDPConnection`	Wird ausgelöst, wenn ein Benutzer eine Remote-Desktop-Verbindung innerhalb einer VDA-Maschine herstellt.	Ziel-IP, Prozess-ID
`Citrix.EventMonitor.UserAccountModification`	Wird für alle Arten von Benutzerkontooperationen ausgelöst, d. h. Kontoerstellung, Aktivierung, Deaktivierung, Löschung, Namensänderungen und Kennwortänderung.	Beschreibung, Zielbenutzername
`VDA.Print`	Wird ausgelöst, wenn ein Druckauftrag in Apps und Desktops initiiert wird. **Hinweis**: Dieses Ereignis gilt nur für Citrix DaaS-Datenquellen. Weitere Informationen finden Sie unter Aktivieren der Drucktelemetrie für Citrix DaaS.	Benutzername des Dokuments, Computername, Druckdateiname, Größe der Druckdatei, Druckername, Uhrzeit, Gesamtzahl der gedruckten Kopien, Gesamtzahl der gedruckten Seiten
`VDA.Clipboard`	Wird ausgelöst, wenn ein Zwischenablagevorgang in Apps and Desktops ausgeführt wird. **Hinweis**: Dieses Ereignis gilt nur für Citrix DaaS-Datenquellen. Weitere Informationen finden Sie unter Telemetrie in der Zwischenablage für Citrix DaaS aktivieren.	Typ des Zwischenablage-Formats, Zwischenablage-Operation, Zwischenablage-Operationsrichtung, Zulässiger Zwischenablage-Vorgang, Größe der Zwischenablage, Computername

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Hinweis**
>
> Für alle Sitzungsaufzeichnungsereignisse muss die Richtlinie zur Protokollierung ihrer Ereignisse auf dem Sitzungsaufzeichnungsserver aktiviert sein. Weitere Informationen finden Sie unter Erstellen einer benutzerdefinierten Ereigniserkennungsrichtlinie.

Unterstützte Werte für Ihre Suchanfrage

Geben Sie die folgenden Werte für die Dimensionen ein, um Ihre Suchanfrage zu definieren.

Feld	Wert	Typ	Beschreibung
App-Name	Anwendung oder Desktop-Sitzungen. Beispielanwendungssitzungen: Eine Sitzung ohne Farmnamen: #Cloud - Excel 2016 Und eine Sitzung mit dem Farmnamen: XA65PROD#Concur Beispiel für Desktopsitzungen: Eine Sitzung ohne Farmnamen: #SINXIAP0616 $S1-1 Und eine Sitzung mit dem Farmnamen: XA65PROD# SINXIAP0616 $S1 -1	Zeichenfolge	Name einer gestarteten Anwendung oder eines Desktops.
App-Protection-Policies	Beispiel:AntiScreenCaptureEnabled	Zeichenfolge	Aktive Anwendungsschutzrichtlinien für die Sitzung.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Feld	Wert	Typ	Beschreibung
Browser-Name	Beispiel: Google Chrome, Citrix Unternehmensbrowser, Microsoft Edge, FIREFOX, SAFARI	Zeichenfolge	Browsername
Browser-Version	Beispiel: 80.0.3987.122, 101.0.9999.0	Zeichenfolge	Browserversion
City	Beispiele: Santa Clara, Houston, Chicago	Zeichenfolge	Der Stadtname eines Benutzers.
Client-IP	Eine IP-Adresse. Beispiel: 10.10.10.10	Zeichenfolge	IP-Adresse des Benutzerendpunkts.
Client-Type	Android, Windows, Macintosh, Chrome, HTML5, Unix/Linux, iOS, Sitzungsaufzeichnung, Monitor	Zeichenfolge	Zeigt verschiedene Typen von Citrix Workspace-Apps an, die auf den Betriebssystemen oder der ursprünglichen Datenquelle basieren.
Clipboard-Format-Type	Beispiele: text, html, CF_UNICODETEXT	Zeichenfolge	Das in die Zwischenablage kopierte Datenformat.
Clipboard-Initiator	Beispiele: Tastatur, Kontextmenü, Javascript	Zeichenfolge	Gibt an, wie der Zwischenablagevorgang eingeleitet wurde. **Hinweis**: Wird nur von den SaaS-Anwendungen unterstützt.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Feld	Wert	Typ	Beschreibung
Clipboard-Operation	Kopieren, Ausschneiden, Einfügen oder Platzieren	Zeichenfolge	Gibt an, welche Zwischenablage ausgeführt wird. **Hinweis**: Die **Platzen-Operation** zeigt an, dass Daten in die Zwischenablage gelegt werden. Dies garantiert nicht, ob die Daten in der Zwischenablage vom Client eingefügt oder verwendet wurden. Dieser Vorgang wird nur für vda.Clipboard Event unterstützt.
Clipboard-Operation-Direction	Kunde zu Host, Host zu Kunde	Zeichenfolge	Gibt die Richtung des Vorgangs in der Zwischenablage an. **Hinweis**: Wird nur von Apps and Desktop (Citrix DaaS) Clipboard Operation unterstützt.
Clipboard-Operation-Permitted	Zulässig oder Abgelehnt	Zeichenfolge	Gibt an, ob der Vorgang in der Zwischenablage in Apps and Desktop Session zulässig ist. **Hinweis**: Wird nur von Apps and Desktop (Citrix DaaS) Clipboard Operation unterstützt.
Clipboard-Result	Erfolgreich oder blockiert	Zeichenfolge	Gibt das Ergebnis des Zwischenablagevorgangs an. **Hinweis**: Wird nur von den SaaS-Anwendungen unterstützt.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Feld	Wert	Typ	Beschreibung
Clipboard-Size	Beispiele: 10, 20	Zahl	Größe der Daten (in Byte), die derzeit in der Zwischenablage gespeichert sind.
Country	Beispiele: USA, Indien	Zeichenfolge	Der Ländername eines Benutzers.
Description	**Für Citrix.EventMonitor.UserAccountModification** **Ereignisse**: Ein Benutzerkonto wurde erstellt, ein Benutzerkonto wurde aktiviert, es wurde versucht, das Kennwort eines Kontos zurückzusetzen.	Zeichenfolge	Beschreibt den Änderungsstatus eines Benutzerkontos, z. B. das Konto wurde erstellt, gelöscht, umbenannt oder es wurde versucht, das Kennwort zurückzusetzen.
	Für Citrix.EventMonitor.SessionEnd **Ereignisse**: Unbekannt, Abmeldung, Rollover, Trigger und Incomplete		Beschreibt den Grund für das Ende der Sitzungsaufzeichnung.
Destination-IP	Beispiel: 10.60.110.xxx	Zeichenfolge	IP-Adresse des Remote-Desktops.
Destination-Path	Beispiel:\ H$\ Desktop\ Folder\ example.txt	Zeichenfolge	Der endgültige Pfad der Datei nach Abschluss der Übertragung.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Feld	Wert	Typ	Beschreibung
Device-ID	Beispiel: cb781185-18ad-4f45-b75f	Zeichenfolge	Geräte-ID, die für Lizenzierung, Client-Name oder Betriebssystem-Hardware-ID verwendet wird.
Domain	Beispiel: example.com	Struktur	Der Domänenname eines Servers, der eine Anfrage gesendet hat.
Download-Device-Type	Beispiele: USB, Festplatte, RemoteDrive, CD-ROM oder Browser-Downloads.	Zeichenfolge	Der Gerätetyp, auf den die Datei heruntergeladen oder übertragen wird.
Download-File-Format	Beispiel: txt, PDF, xlsx, docx	Zeichenfolge	Das Format der heruntergeladenen Datei.
Download-File-Name	Beispiel: example-file.txt	Zeichenfolge	Name der heruntergeladenen Datei.
Download-File-Path	Beispiel: C:\Users\admin\Desktop	Zeichenfolge	Der Pfad der heruntergeladenen Datei.
Download-File-Size	Beispiel: 8.05	Zahl	Die Größe der heruntergeladenen Datei in Kilobyte.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Feld	Wert	Typ	Beschreibung
Event-Type	Account.Logon, Session.Logon, Session.End, App.Start, App.End, File.Download, Printing, AppProtection.ScreenCapture, App.SaaS.Launch, App.SaaS.End, App.SaaS.Clipboard, App.SaaS.File.Download, App.SaaS.File.Print, App.SaaS.Url.Navigate, Citrix.EventMonitor.AppStart, Citrix.EventMonitor.AppEnd, Citrix.EventMonitor.TopMost, Citrix.EventMonitor.WebBrowsing, Citrix.EventMonitor.FileCreate, Citrix.EventMonitor.FileRename, Citrix.EventMonitor.FileMove, Citrix.EventMonitor.FileDelete, Citrix.EventMonitor.CDMUSBDriveAttach, Citrix.EventMonitor.GenericUSBDriveAttach, Citrix.EventMonitor.RDPConnection, Citrix.EventMonitor.UserAccountModification, VDA.Print, VDA.Clipboard, Citrix.EventMonitor.RegistryChange, Citrix.EventMonitor.SessionLaunch, Citrix.EventMonitor.SessionEnd,	Zeichenfolge	Weitere Informationen finden Sie unter Ereignistypen und unterstützte Felder.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Feld	Wert	Typ	Beschreibung
Jail-Broken	Ja oder Nein	Zeichenfolge	Zeigt an, ob das Gerät gerootet ist oder nicht. **Hinweis**: Fehlt diese Dimension, ist das Gerät nicht gerootet. Dieser Schlüssel gilt für die Citrix Workspace-App für iOS- und Android-Geräte.
Operation-Direction	Host-zu-Client/Client-zu-Host	Zeichenfolge	Gibt die Richtung der Dateiübertragung an.
OS-Extra-Info	Beispiel: 20G80, Service Pack 1, 19043	Zeichenfolge	Zeigt die zusätzlichen Informationen des Betriebssystems wie Build-Nummern, Service Packs und Patches an.
OS-Name	Beispiel: macOS 11, Windows 7, Android 8.1, Windows 10 Enterprise	Zeichenfolge	Gibt den Namen des Betriebssystems an.
OS-Version	Beispiel: 11.5.1, 14.7.1, 2009	Zeichenfolge	Gibt die Version des Betriebssystems an
Print-File-Format	Beispiele: PDF, PS, DOCX	Zeichenfolge	Format der gedruckten Datei.
Print-File-Name	Beispiel: example-file.pdf	Zeichenfolge	Name der gedruckten Datei.
Print-File-Size	Beispiele: 10, 20	Zeichenfolge	Größe der gedruckten Datei in Byte.
Printer-Name	Beispiel: testprinter-1	Zeichenfolge	Name des verwendeten Druckers.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Feld	Wert	Typ	Beschreibung
Process-ID	Beispiel: 11248	Zeichenfolge	Bezieht sich auf die Prozess-ID, die verwendet wird, um den spezifischen Prozess zu identifizieren, der zwei Aktionen ausführt: **Erstellen eines neuen Prozesses** und **Herstellen einer Remote-Desktop-Verbindung**. Die Prozess-ID ist derzeit nur dem Ereignis Citrix.EventMonitor.RDPConnection zugeordnet.
Protected-App-Titles	Beispiel: Admin Desktop —Citrix Workspace	Zeichenfolge	Name der Anwendung, die in der geschützten Sitzung ausgeführt wird.
Registry-Name	Name der geänderten Registrierung	Zeichenfolge	Der Name der Registrierung, die geändert wurde.
Registry-Operation	Umbenennen, Erstellen, Löschen, SetValue, DeleteValue	Zeichenfolge	Gibt an, welcher Registrierungsvorgang ausgeführt wurde.
Registry-Path	Pfad der geänderten Registrierung	Zeichenfolge	Der Pfad der Registrierung, die geändert wurde.
SaaS-App-Name	Beispiel: Workday	Zeichenfolge	Name der SaaS-Anwendung.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Feld	Wert	Typ	Beschreibung
SaaS-App-URL	Beispiel:https://xyz.com|String	Zeichenfolge	URL der SaaS-Anwendung oder Gateway/Proxy-URL. **Hinweis**: Die Gateway-/Proxy-URL wird im app.saas.Launch-Ereignis angezeigt, wenn die SaaS-Anwendung zum ersten Mal gestartet wird.
Screen-Capture-Tool-Name	Beispiel: ScreenShotTool.exe	Zeichenfolge	Name des Screenshot-Tools.
Screen-Capture-Tool-Path	Beispiel: c:\Program files (x86)\ ScreenContent Client	Zeichenfolge	Pfad des Screenshot-Tools.
Session-Launch-Type	Anwendung oder Desktop	Zeichenfolge	Gibt an, ob die gestartete Sitzung ein Anwendungs- oder Desktoptyp ist.
Session-Recording-Type	Traditionelle Aufzeichnung/Aufzeichnung nur für Veranstaltungen	Zeichenfolge	Gibt den Typ der gestarteten Sitzungsaufzeichnung an.
Session-Server-Name	Beispiele: Hosted Desktop, Cloud-VDA-1	Zeichenfolge	Name der Anwendung oder des Desktops, mit der verbunden ist, wie von einem Server empfangen.
Session-User-Name	Beispiele: Demo-Benutzer, Testbenutzer	Zeichenfolge	Vom Server empfangener Benutzername.
Source-Path	Beispiel: C:\Users\admin\Desktop\example.txt	Zeichenfolge	Der ursprüngliche Pfad der Datei vor der Übertragung.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Feld	Wert	Typ	Beschreibung
Target-User-Name	Beispiele: user01	Zeichenfolge	Derzeit wird der Target-User-Name nur für das Ereignis Citrix.EventMonitor.UserAccountModif verwendet, bei dem das Benutzerkonto geändert wurde.
Total-Copies-Printed	Beispiele: 1, 2	Zahl	Gesamtzahl der vom Benutzer gedruckten Exemplare.
Total-Pages-Printed	Beispiele: 1,2	Zahl	Gesamtzahl der vom Benutzer gedruckten Dokumentseiten.
User-Name	Benutzername oder Domäne\Benutzername	Zeichenfolge	Der Benutzername oder Domäne\Benutzername. Wird für StoreFront-Login verwendet. Wenn die StoreFront-Anmeldung nicht über die Citrix Workspace-App für HTML5 oder Chrome erfolgt, entspricht dieser Wert dem vom Server empfangenen Wert.
VDA-Name	Beispiel: TSVDA-19-01.xd.Local	Zeichenfolge	Gibt den Namen der VDA-Maschine an.
Window-Title	Beispiel: Administrator - 01 Befehlszeile	Zeichenfolge	Gibt den Titel des Fensters an, in dem der Zwischenablagevorgang ausgeführt wurde.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Feld	Wert	Typ	Beschreibung
Workspace-App-Version	Beispiel: 20.8.0.3 (2008)	Zeichenfolge	Die Citrix Workspace-App oder die Citrix Receiver-Version wurde auf dem Gerät des Benutzers installiert und zum Starten virtueller Remote-Apps und Desktop-Sitzungen verwendet.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Feld	Wert	Typ	Beschreibung
Workspace-App-Status	Unterstützt oder nicht unterstützt	Zeichenfolge	Gibt an, ob die installierte Version der Citrix Workspace-App oder von Citrix Receiver auf dem Gerät des Benutzers von Citrix Analytics for Security unterstützt wird oder nicht. Bewegen Sie den Mauszeiger über **Nicht unterstützt**, wenn die Workspace-App nicht unterstützt wird. Ein Popup-Fenster mit einem Link zur Liste der unterstützten Versionen wird angezeigt. Wenn sich eine Workspace-App-Version dem Status „Nicht unterstützt "nähert, wird auf der Self-Service-Suchseite ein Banner angezeigt, in dem die verfügbaren unterstützten Versionen aufgeführt sind, auf die Sie ein Upgrade einleiten können.

Benennungsformat des Betriebssystems

Citrix Analytics erhält die Betriebssystemdetails (OS) eines Benutzergeräts und übersetzt sie in Betriebssystemname, Betriebssystemversion und OS Extra Info.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Betriebssystemname** gibt den Namen des Betriebssystems an.
- Die **Betriebssystemversion** gibt die Release-ID oder die Release-Version des Betriebssystems an.
- **OS Extra Info** gibt die zusätzlichen Informationen des Betriebssystems wie Build-Nummern, Service Packs und Patches an.

Die folgende Tabelle enthält einige Beispiele für das Versionsnummerierungsformat von Betriebssystemen.

Betriebssystemname	Betriebssystemversion	Zusätzliche OS-Informationen
macOS 11	11.5.1	20G80
iOS 14	14.7.1	Nicht verfügbar
Windows 10 Enterprise	2009	19043
Windows 7	6.1	Service Pack 1
Android 8.1	8.1.0	Nicht verfügbar

> **Hinweise**
>
> - Um die Betriebssystemdetails für Mac Version 11.x oder höher abzurufen, ist die empfohlene Clientversion die Citrix Workspace-App für Mac 2108 oder höher.
> - Die Betriebssystemdetails für Windows 10 sind derzeit nicht verfügbar.

Problembehandlung bei Citrix Analytics für Sicherheit und Leistung

December 12, 2023

In diesem Abschnitt wird erläutert, wie Sie die folgenden Probleme beheben können, die bei der Verwendung von Citrix Analytics for Security auftreten können.

- Überprüfen Sie anonyme Benutzer als legitime Benutzer.
- Beheben Sie Probleme mit der Ereignisübertragung aus einer Datenquelle.
- Lösen Sie Virtual Apps and Desktops Desktop-Ereignisse, SaaS-Ereignisse aus und überprüfen Sie die Ereignisübertragung an Citrix Analytics for Security.
- DerSitzungsaufzeichnungsserver kann keine Verbindung herstellen.
- Konfigurationsprobleme mit dem Citrix Analytics-Add-On für Splunk

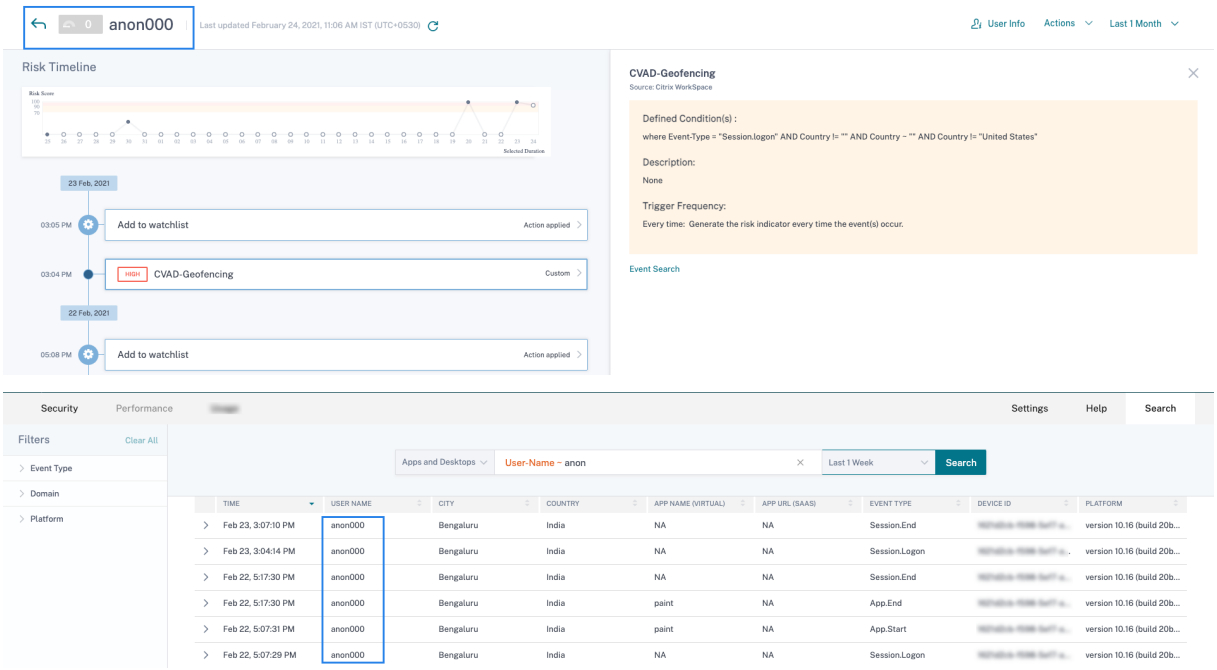
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Überprüfen Sie die anonymen Benutzer als legitime Benutzer

August 19, 2022

Als Administrator stellen Sie möglicherweise fest, dass einige Citrix Virtual Apps and Desktops -Benutzer und Citrix DaaS-Benutzer (früher Citrix Virtual Apps and Desktops Service) in Citrix Analytics for Security als anonym angezeigt werden. Diese Benutzer werden als erkannte Benutzer identifiziert. Ihre Benutzernamen erscheinen jedoch als anonXYZ (wobei "XYZ"eine dreistellige Zahl darstellt) auf den folgenden Seiten:

- Benutzer
- Zeitleiste des Nutzers
- Riskante Benutzer
- Self-Service-Suche nach der Datenquelle Apps und Desktops



Wenn Sie solche Benutzer sehen, möchten Sie möglicherweise Folgendes wissen:

- Wer sind diese Benutzer?
- Sind diese Benutzer legitim oder böswillig?
- Wie überprüfe ich sie?
- Welche Aktionen muss ich für diese Benutzer anwenden?

In den folgenden Szenarien sehen Sie anonyme Benutzer in Ihrer Citrix IT-Umgebung:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Wenn ein Benutzer eine veröffentlichte sichere Browser-App verwendet
- Wenn ein Benutzer einen nicht authentifizierten Store verwendet

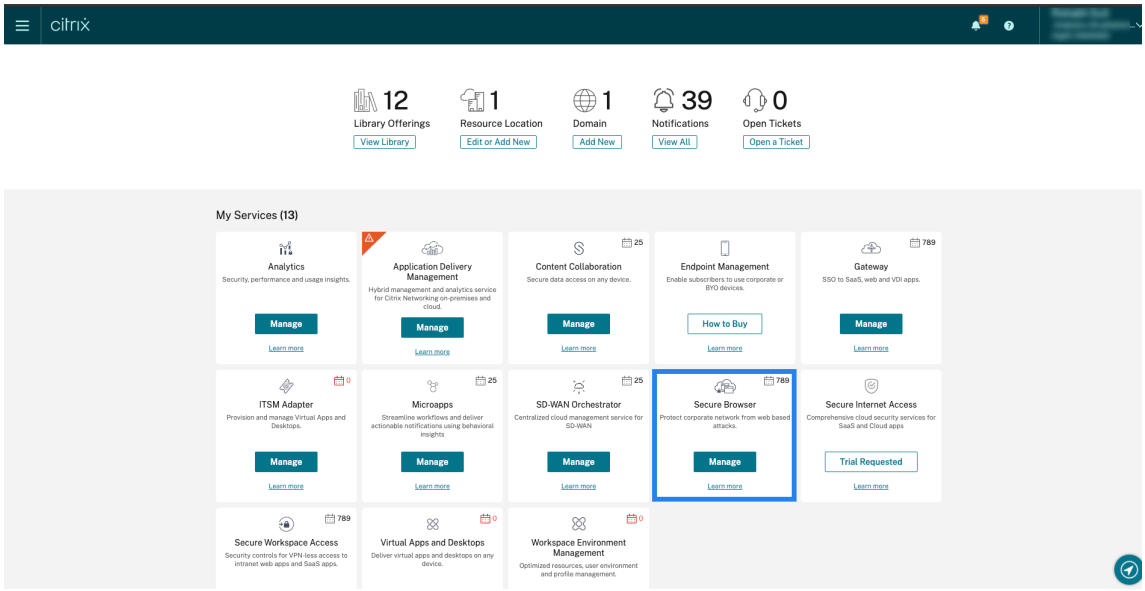
Benutzer verwendet veröffentlichte sichere Browser-Apps

Die sicheren Browser-Apps sind Web-Apps, die mit dem Citrix Secure Browser Service veröffentlicht werden. Diese Apps isolieren Ihre Webbrowser-Ereignisse und schützen Ihr Unternehmensnetzwerk vor browserbasierten Angriffen. Weitere Informationen finden Sie unter Secure Browser Service.

Die sicheren Browser-Apps verwenden die anonyme Sitzungsfunktion von Citrix DaaS.

So überprüfen Sie, ob Secure Browser in Ihrem Citrix Cloud-Konto konfiguriert ist:

1. Melden Sie sich bei Citrix Cloud an.
2. Klicken Sie auf der **Secure Browser**-Karte auf **Verwalten**.



3. Suchen Sie auf der Seite **Verwalten** nach veröffentlichten sicheren Browser-Apps.

Wenn ein Benutzer über Citrix Receiver für Websites über einen Webbrowser auf einen StoreFront-Store zugreift und die veröffentlichten sicheren Browser-Apps verwendet, ist die Identität des

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Benutzers ausgeblendet. Daher zeigt Citrix Analytics den Benutzer als anonym an.

Wenn ein Benutzer über eine Citrix Receiver- oder Citrix Workspace-App auf einen StoreFront-Store zugreift, die auf seinem Gerät installiert ist und die veröffentlichten sicheren Browser-Apps verwendet, zeigt Citrix Analytics den Benutzer als den im StoreFront angegebenen Benutzernamen an.

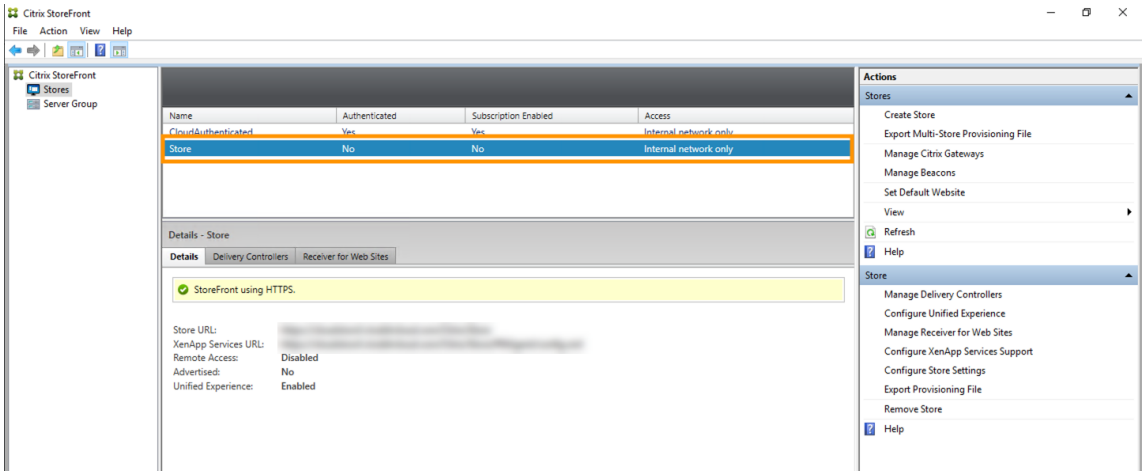
Sie können den Benutzer also als legitimen Benutzer Ihrer Organisation betrachten. Sie müssen keine Aktion anwenden, wenn dem Benutzer kein riskantes Verhalten zugeordnet ist.

Benutzer, der einen nicht authentifizierten Store verwendet

Der nicht authentifizierte Store ist eine Funktion von Citrix StoreFront und gilt für die Stores, die vom Kunden verwaltet werden. Diese Funktion unterstützt den Zugriff für nicht authentifizierte (anonyme) Benutzer.

So überprüfen Sie, ob Ihre Organisation über einen nicht authentifizierten Store verfügt:

1. Starten Sie Citrix Studio.
2. Klicken Sie auf **Stores**.
3. Überprüfen Sie für Ihre Geschäfte den Authentifizierungsstatus in der Spalte Authentifiziert.



Wenn ein Geschäft nicht authentifiziert ist und der Benutzer auf diesen nicht authentifizierten Speicher zugreift, bleibt die Benutzeridentität anonym. Daher zeigt Citrix Analytics den Benutzer als anonym an. Sie können diesen Benutzer als legitimen Benutzer Ihrer Organisation betrachten. Sie müssen keine Aktion anwenden, wenn dem Benutzer kein riskantes Verhalten zugeordnet ist.

Probleme mit der Ereignisübertragung aus einer Datenquelle beheben

April 12, 2024

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Dieser Abschnitt hilft Ihnen bei der Behebung von Datenübertragungsproblemen in Citrix Analytics for Security. Wenn eine Datenquelle Benutzerereignisse nicht korrekt überträgt, können Probleme wie die Nicht-Erkennung von Benutzern und Risikoindikatoren auftreten.

Checkliste

Sequenz	Schecks
1	Haben Sie die richtige Berechtigung, Security Analytics zu nutzen?
2	Wird die Datenquelle in Ihrer Heimatregion unterstützt?
3	Erfüllt Ihre Umgebung alle Systemanforderungen?
4	Sind alle entdeckten Datenquellen und die Datenverarbeitung in Analytics aktiviert?
5	Übertragen die Benutzeraktivitäten auf der Datenquelle Ereignisse genau an Analytics?
6	Werden die Ereignisse der virtuellen Apps und Desktops an Analytics übertragen?
7	Werden die Benutzerereignisse auf der Self-Service-Suchseite in Analytics angezeigt?
8	Werden die Benutzer von Analytics entdeckt?

Test 1 —Haben Sie die richtige Berechtigung, Security Analytics zu verwenden?

Citrix Analytics for Security ist ein abonnementbasiertes Angebot. Weitere Informationen finden Sie unter Erste Schritte.

Test 2- Wird die Datenquelle in Ihrer Heimatregion unterstützt?

Citrix Analytics for Security wird in den folgenden Home-Regionen unterstützt:

- Vereinigte Staaten (US)
- Europäische Union (EU)
- Asien-Pazifik Süd (APS)

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Je nach Standort Ihrer Organisation können Sie sich in einer der Heimatregionen bei Citrix Cloud einbinden.

Bestimmte Datenquellen werden jedoch nicht in allen Heimatregionen unterstützt. Die Datenquellen sind die Produkte, von denen Citrix Analytics for Security Benutzerereignisse empfängt.

Wenn Ihr Unternehmen in einer Heimatregion, in der eine Datenquelle nicht unterstützt wird, in Citrix Cloud integriert ist, erhalten Sie keine Benutzerereignisse von der Datenquelle.

Verwenden Sie die folgende Tabelle, um die Datenquellen und die Regionen anzuzeigen, in denen sie unterstützt werden.

Datenquelle	Unterstützt in der US-Region	Unterstützt in der EU-Region	In der APS-Region unterstützt
Citrix Endpoint Management	Ja	Ja	Ja
NetScaler Gateway (on-premises)	Ja	Ja	Ja
Citrix Identitätsanbieter	Ja	Ja	Ja
Citrix Secure Browser	Ja	Ja	Ja
Citrix Secure Private Access	Ja	Nein	Nein
Citrix DaaS (früher Citrix Virtual Apps and Desktops Service)	Ja	Ja	Ja
Citrix Virtual Apps and Desktops on-premises	Ja	Ja	Ja
Microsoft Active Directory	Ja	Ja	Ja
Microsoft Graph Security	Ja	Ja	Ja

Test 3- Erfüllt Ihre Umgebung alle Systemanforderungen?

Citrix Analytics kann einige Minuten benötigen, um die Benutzerereignisse aus den Datenquellen zu empfangen. Wenn auf den Sitekarten der Datenquelle keine Benutzerereignisse angezeigt werden, stellen Sie sicher, dass Ihre Umgebung die Voraussetzungen und Systemanforderungenerfüllt.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Voraussetzungen

1. Alle Ihre Citrix Cloud-Abonnements müssen aktiv sein. Stellen Sie auf der Citrix Cloud-Seite sicher, dass alle Citrix Cloud-Dienste aktiv sind.
2. Wenn Sie on-premises verwenden Citrix Virtual Apps and Desktops, müssen Sie Ihre Sites zu Citrix Workspace hinzufügen und die Site-Aggregation konfigurieren. Citrix Analytics erkennt automatisch die Sites, die Citrix Workspace hinzugefügt wurden. Weitere Informationen finden Sie unter Aggregieren on-premises virtueller Apps und Desktops in Arbeitsbereichen.
3. Wenn Sie eine StoreFront-Bereitstellung für Ihre Sites verwenden, konfigurieren Sie Ihre StoreFront-Server so, dass die Citrix Workspace-App Benutzerereignisse an Citrix Analytics senden kann. Stellen Sie sicher, dass die StoreFront-Version 1906 oder höher ist. Wenn Sie den StoreFront-Server nicht konfigurieren, empfängt Citrix Analytics keine Benutzerereignisse von on-premises Citrix Virtual Apps and Desktops. Informationen zum Konfigurieren der StoreFront-Bereitstellung finden Sie im Citrix Analytics Service Analytics-Dienstartikel in der StoreFront-Dokumentation.
4. Die Citrix Virtual Apps and Desktops-Benutzer und Citrix DaaS-Benutzer müssen die angegebene Version der Citrix Workspace-Apps oder Citrix Receiver auf ihren Endpunkten verwenden. Andernfalls erhält Analytics die Benutzerereignisse nicht von den Benutzerendpunkten. Die Liste der unterstützten Versionen der Citrix Workspace-App oder Citrix Receiver ist in Citrix Virtual Apps and Desktops und der Citrix DaaS-Datenquelleverfügbar.
5. Um die Benutzerereignisse aus einer veröffentlichten Secure Browser-Sitzung zu empfangen, aktivieren Sie die Einstellung **Hostname Tracking** im Secure Browser. Diese Einstellung ist standardmäßig deaktiviert. Weitere Informationen finden Sie unter Verwalten veröffentlichter sicherer Browser.
6. Integrieren Sie Ihre Datenquellen wie in den folgenden Artikeln erwähnt:
    - Citrix Endpoint Management-Datenquelle
    - Citrix Gateway-Datenquelle
    - Citrix Secure Private Access-Datenquelle
    - Citrix Virtual Apps and Desktops und Citrix DaaS-Datenquelle
    - Microsoft Active Directory-Integration
    - Integration von Microsoft Graph Security

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Test 4- Sind alle entdeckten Datenquellen und die Datenverarbeitung in Analytics aktiviert?

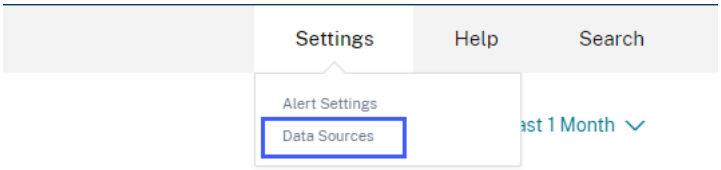
Stellen Sie sicher, dass alle Ihre Datenquellen erkannt werden und Sie die Datenverarbeitung für sie aktiviert haben. Wenn Sie die Datenverarbeitung für eine Datenquelle nicht aktivieren, werden die Benutzer, die die Datenquelle verwenden, nicht erkannt. Diese Situation könnte ein potenzielles Sicherheitsrisiko darstellen.

Durch die Aktivierung der Datenverarbeitung wird sichergestellt, dass Citrix Analytics Ihre Benutzerereignisse verarbeitet. Ereignisse werden nur an Citrix Analytics gesendet, wenn die Benutzer die Datenquelle aktiv verwenden.

> **Hinweis**
>
> Citrix Analytics zieht nicht aktiv Daten aus Ihrer Umgebung.

Gehen Sie wie folgt vor, um Ihre Datenquellen zu ermitteln und Analysen zu ermöglichen:

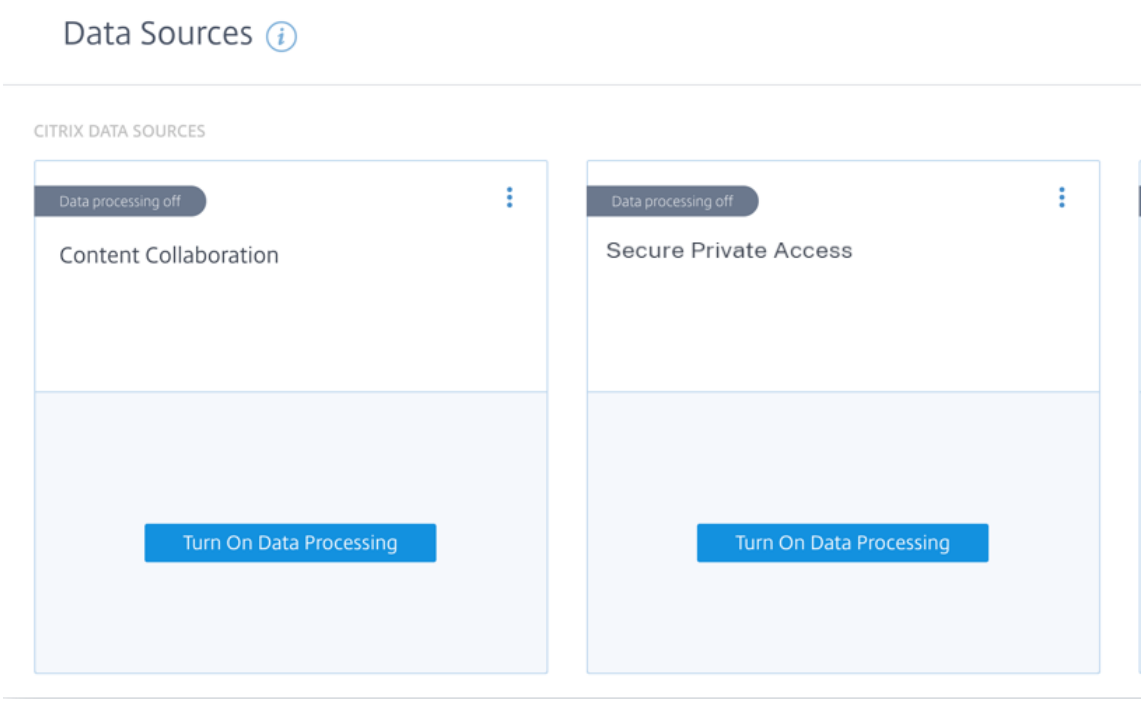
1. Klicken Sie auf **Einstellungen** > **Datenquellen** > **Sicherheit**, um die erkannten Datenquellen anzuzeigen. Citrix Analytics erkennt automatisch die Datenquellen, die Sie für Ihr Citrix Cloud-Konto abonniert haben.



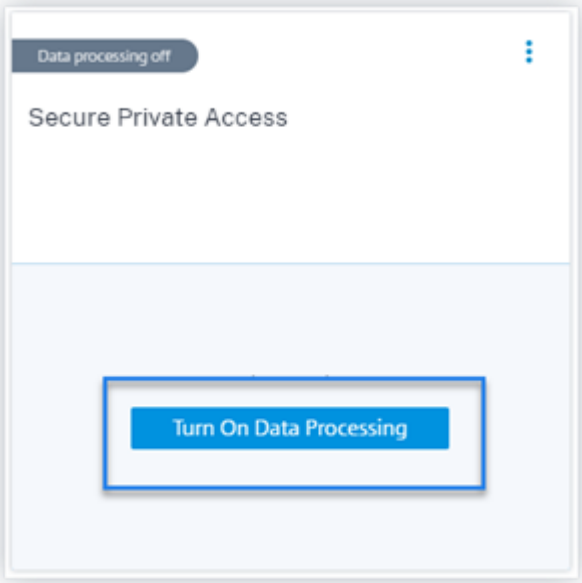
2. Auf der Seite **Datenquellen** werden die erkannten Datenquellen als Sitekarten angezeigt. Standardmäßig ist die Datenverarbeitung ausgeschaltet.

> **Wichtig**
>
> Citrix Analytics verarbeitet Ihre Daten, nachdem Sie Ihre Einwilligung erteilt haben.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

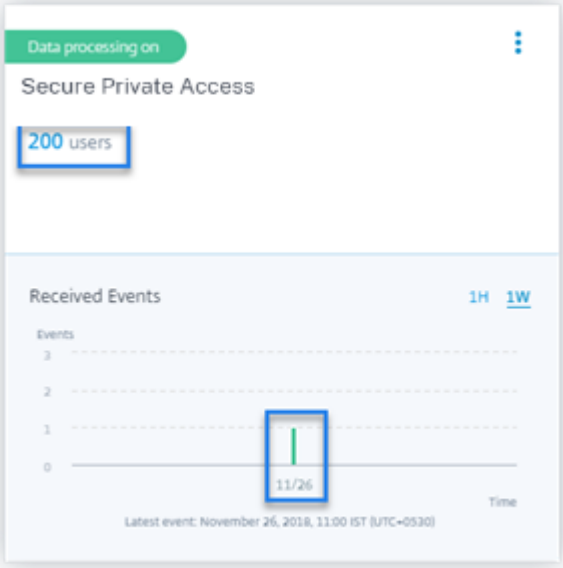


3. Klicken Sie **auf der Sitekarte, für die Citrix Analytics Ereignisse verarbeiten soll, auf Datenverarbeitung einschalten** . Klicken Sie beispielsweise auf der Citrix Secure Private Access-Sitekarte auf **Datenverarbeitung einschalten**.



4. Nachdem Sie die Datenverarbeitung aktiviert haben, verarbeitet Citrix Analytics die Ereignisse für die Datenquelle. Der Status der Site Card ändert sich in Datenverarbeitung. Sie können die Anzahl der Benutzer und die empfangenen Ereignisse basierend auf dem ausgewählten Zeitraum anzeigen.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



5. Befolgen Sie für alle erkannten Datenquellen die unter Erste Schritte angegebenen Schritte, um die Analyse zu aktivieren.

Test 5- Übertragen die Benutzeraktivitäten auf der Datenquelle Ereignisse genau an Analytics?

Citrix Analytics empfängt Benutzerereignisse aus den Datenquellen, wenn die Benutzer die Datenquellen aktiv verwenden. Die Benutzer müssen einige Aktivitäten an der Datenquelle ausführen, um Ereignisse zu generieren. Um beispielsweise Ereignisse aus der Apps and Desktops-Datenquelle zu empfangen, müssen die Apps and Desktops-Benutzer einige Dateien teilen, hochladen oder herunterladen.

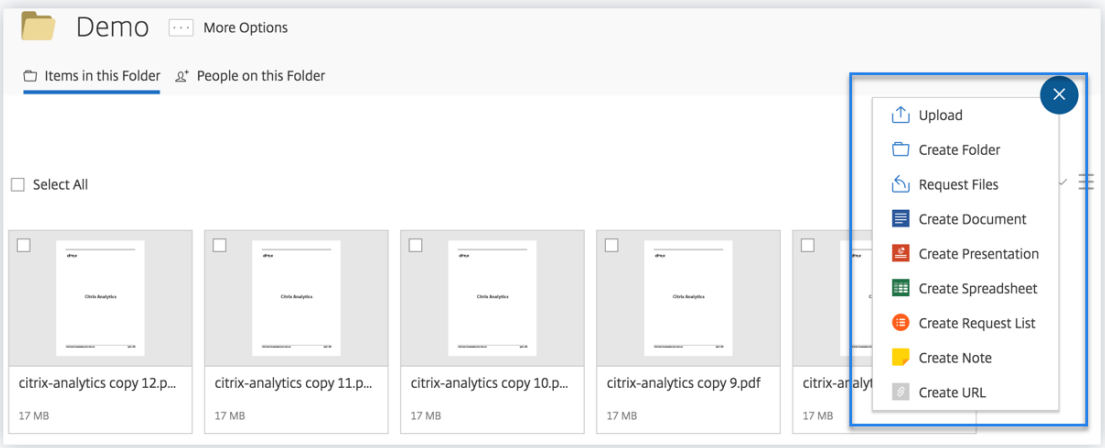
> **Hinweis**
>
> Citrix Analytics zieht nicht aktiv Daten aus Ihrer Umgebung.

Wenn Sie in Citrix Analytics keine Benutzerereignisse für Ihre Datenquelle sehen, besteht eine hohe Wahrscheinlichkeit, dass die Benutzer zu diesem Zeitpunkt nicht aktiv sind.

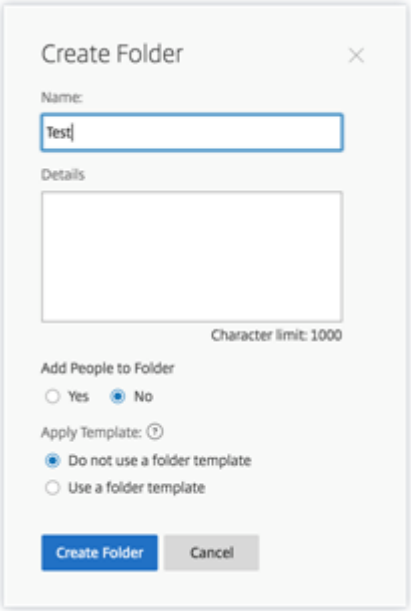
Führen Sie die folgende Aktivität aus, um zu überprüfen, ob Citrix Analytics die Benutzerereignisse korrekt empfängt. Diese Aktivität verwendet die Citrix Apps and Desktops-Datenquelle. Sie können eine ähnliche Aktivität mit anderen Citrix Produkten (Datenquellen) basierend auf Ihrem Abonnement ausführen.

1. Melden Sie sich beim Citrix Apps and Desktops Service an.
2. Führen Sie einige übliche Benutzeraktivitäten aus, z. B. Ordner erstellen, Dateien herunterladen, Dateien hochladen oder Dateien löschen.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

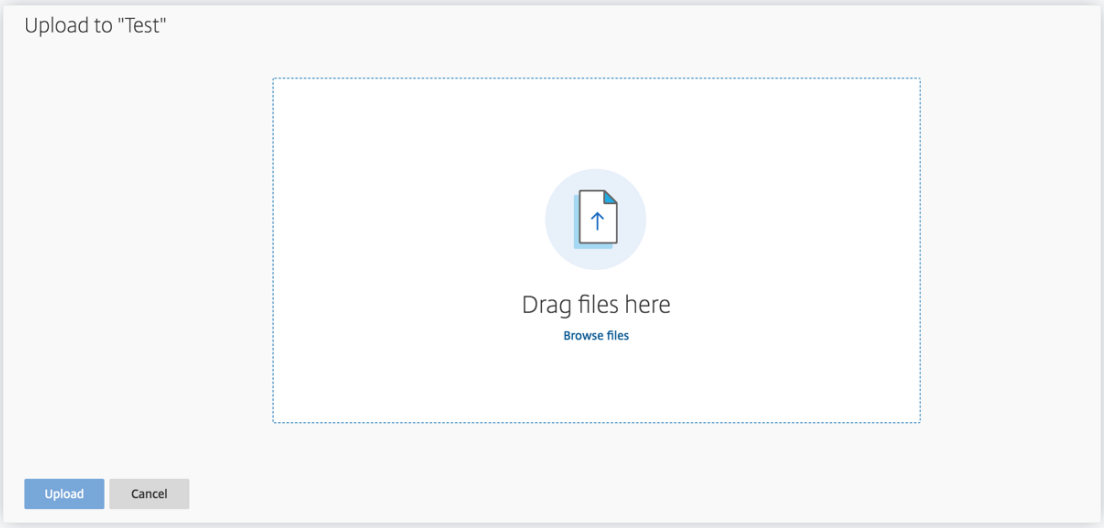


3. Erstellen Sie beispielsweise einen Testordner.

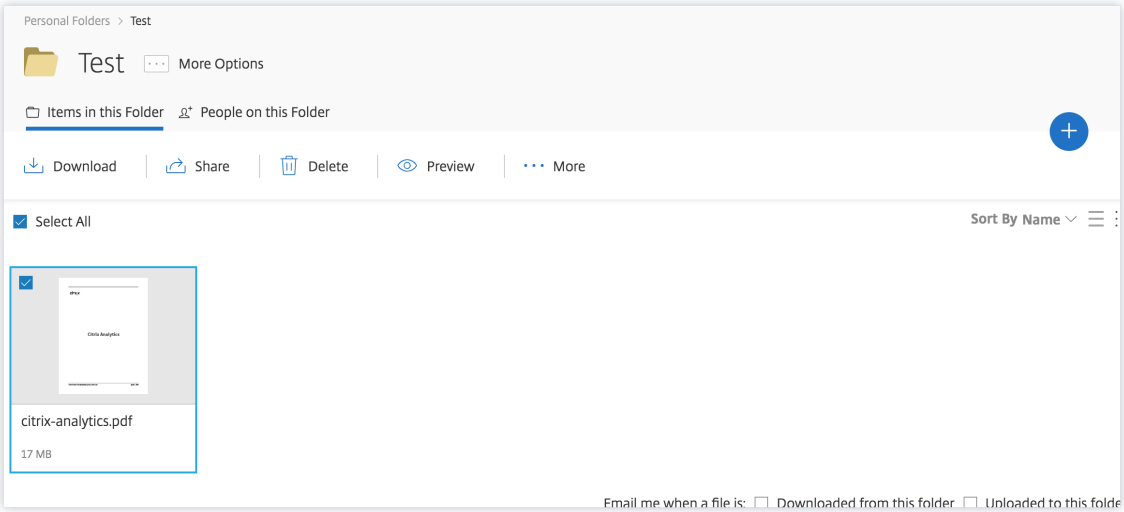


4. Laden Sie einige lokale Dateien hoch.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

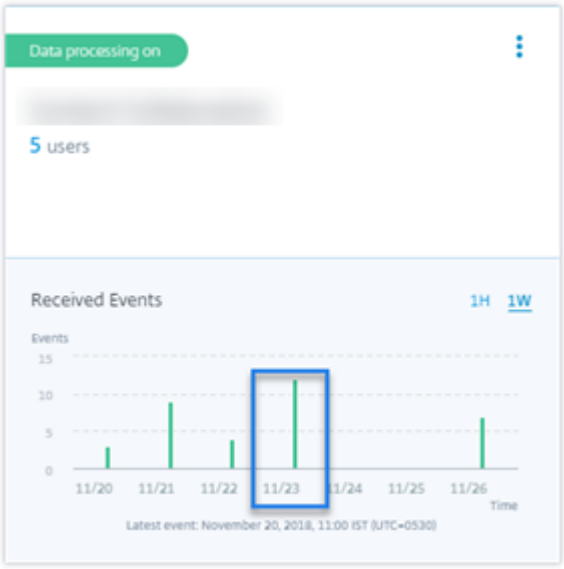


5. Löschen Sie einige Dateien im Ordner.



6. Kehren Sie zu Citrix Analytics zurück und sehen Sie sich die Seitenkarte **Apps and Desktops** auf der Datenquellenseite an. Citrix Analytics empfängt die Benutzerereignisse von der Apps and Desktops-Datenquelle und zeigt sie auf der Sitekarte an.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Test 6: Werden die Ereignisse der virtuellen Apps und Desktops an Analytics übertragen?

Einige Versionen der Citrix Workspace-App oder des Citrix Receiver-Clients senden Benutzerereignisse nicht an Citrix Analytics. Wenn Benutzer virtuelle Apps und Desktops über diese Clients starten, erkennt Citrix Analytics die Benutzer erst, wenn sie die unterstützten Ereignisse ausführen.

Beispielsweise sendet die Citrix Workspace-App für Linux 2006 oder höher die ***SaaS App Launch*** - und ***SaaS App End-Ereignisse*** nicht an Citrix Analytics. Ein Benutzer, der eine SaaS-App mit der Citrix Workspace-App für Linux startet, wird in Citrix Analytics nicht erkannt.

Unterstützte Ereignisse

In der folgenden Tabelle können Sie die Benutzerereignisse überprüfen, die von jeder Clientversion unterstützt werden.

- **Ja**—Das Ereignis wird vom Client an Citrix Analytics gesendet.
- **Nein**—Das Ereignis wird vom Client nicht an Citrix Analytics gesendet.
- **NA**—Das Ereignis gilt nicht für den Kunden.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Ereignis	Workspace-App für Windows 1907 oder höher	Workspace-App für Mac 1910.2 oder höher	Workspace-App für Linux 2006 oder höher	Arbeitsbereich-App für Android - Aktuelle Version in Google Play verfügbar	Workspace-App für iOS — neueste Version im Apple App Store verfügbar	Workspace-App für Chrome — Aktuelle Version im Chrome Web Store verfügbar	Workspace-App für HTML5 2007 oder höher
Konto Logon	Ja	Ja	Ja	Ja	Ja	Nein	Nein
Sitzungs-Anmeldung	Ja	Ja	Ja	Ja	Ja	Ja	Ja
Sitzungsstart	Ja	Ja	Ja	Ja	Ja	Ja	Ja
Ende der Sitzung	Ja	Ja	Ja	Ja	Ja	Ja	Ja
App-Start	Ja	Ja	Ja	Nein	Ja	Ja	Ja
App-Ende	Ja	Ja	Ja	Nein	Ja	Ja	Ja
Datei Herunter-laden	Ja	Ja	Ja	Nein	Nein	Ja	Ja
Drucken	Nein	Ja	Ja	Nein	Nein	Ja	Ja
SaaS App starten	Ja	Ja	Nein	Nein	Nein	Nein	Nein
SaaS App Ende	Ja	Ja	Nein	Nein	Nein	Nein	Nein
SaaS App URL-Navigation	Ja	Ja	Nein	Nein	Nein	Nein	Nein
Zugriff auf SaaS App Zwischen-ablage	Ja	Ja	Nein	Nein	Nein	Nein	Nein

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Ereignis	Workspace-App für Windows 1907 oder höher	Workspace-App für Mac 1910.2 oder höher	Workspace-App für Linux 2006 oder höher	Arbeitsbereich-App für Android - Aktuelle Version in Google Play verfügbar	Workspace-App für iOS — neueste Version im Apple App Store verfügbar	Workspace-App für Chrome — Aktuelle Version im Chrome Web Store verfügbar	Workspace-App für HTML5 2007 oder höher
SaaS App Datei herunter-laden	Ja	Ja	Nein	Nein	Nein	Nein	Nein
SaaS App Datei drucken	Ja	Ja	Nein	Nein	Nein	Nein	Nein

Basierend auf dem Übertragungsstatus des Ereignisses können folgende Probleme auftreten:

- Wenn Benutzer eine Verbindung mit ihren Clients zu Citrix Virtual Apps and Desktops oder Citrix DaaS herstellen, werden die Benutzer möglicherweise erst in Citrix Analytics erkannt, wenn sie ein unterstütztes Ereignis (Aktivität) ausführen. Betrachten Sie beispielsweise zwei Benutzerereignisse - App Start und SaaS App Launch. Citrix Analytics, ein Benutzer, der die Citrix Workspace-App für iOS verwendet, empfängt das App Start-Ereignis, aber nicht das SaaS App Launch-Ereignis. Wenn der Benutzer also virtuelle Apps startet, wird das App Start-Ereignis an Citrix Analytics übertragen und der Benutzer wird erkannt. Wenn der Benutzer jedoch eine SaaS-App startet, erhält Citrix Analytics das SaaS App Launch-Ereignis nicht und der Benutzer wird nicht erkannt. Informationen zu entdeckten Benutzern finden Sie unter Entdeckte Benutzer.
- Ereignisse, die auf der Tabelle mit **Nein** gekennzeichnet sind, werden auf der Self-Service-Suchseite nicht angezeigt. Informationen zur Verwendung der Self-Service-Seite finden Sie unter Informationen zur Self-Service-Suche.

Empfehlung

Um die maximalen Vorteile von Analytics zu nutzen, empfiehlt Citrix Folgendes:

- **Windows-Benutzer**: Stellen Sie mit der Citrix Workspace-App für Windows 1907 oder höher eine Verbindung zu Citrix Virtual Apps and Desktops von Citrix und Citrix DaaS her.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

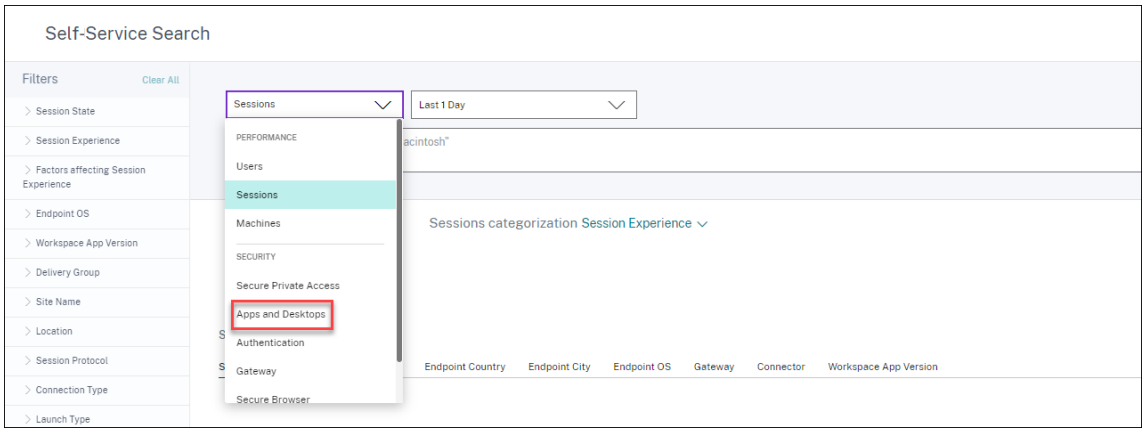
- **Mac-Benutzer**: Stellen Sie mithilfe der Citrix Workspace-App für Mac 1910.2 oder höher eine Verbindung zu Citrix Virtual Apps and Desktops von Citrix und Citrix DaaS her.

Test 7- Werden die Benutzerereignisse auf der Self-Service-Suchseite in Analytics angezeigt?

Führen Sie diese letzte Überprüfung durch, um sicherzustellen, dass die Ereignisse korrekt an Citrix Analytics übertragen werden.

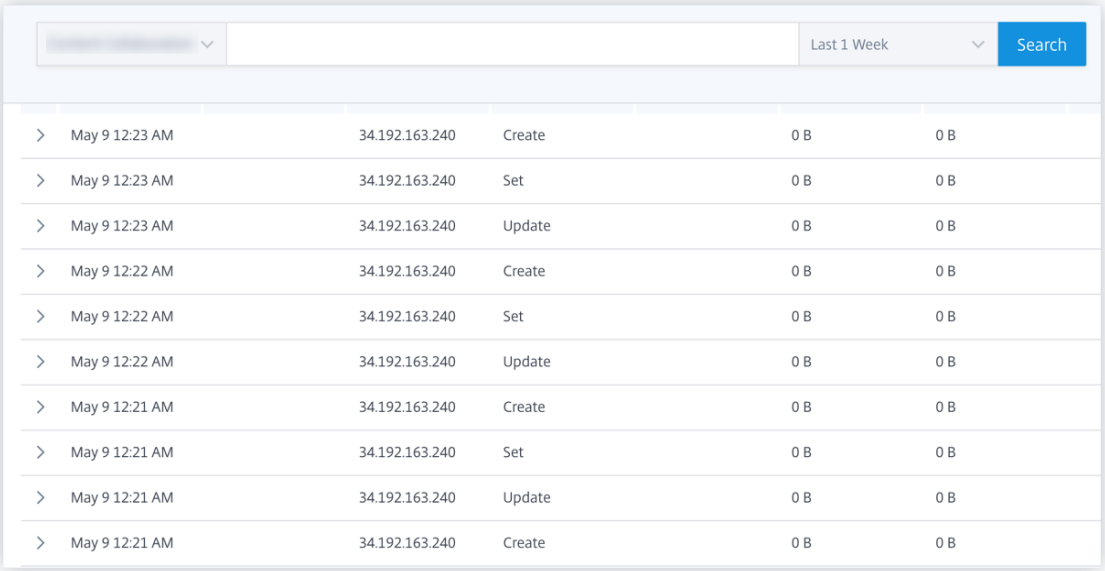
1. Klicken Sie in der oberen Leiste auf **Erweiterte Suche**, um zur Self-Service-Suchseite zu gelangen.

2. Wählen Sie die Datenquelle aus, um die entsprechende Suchseite und die Ereignisse anzuzeigen.



3. Um die mit den Apps and Desktops-Ereignissen verknüpften Daten anzuzeigen, wählen Sie **Apps and Desktops** aus der Liste aus, wählen Sie den Zeitraum aus, und klicken Sie dann auf **Suchen**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Weitere Informationen finden Sie unter Self-Service-Suche.

Test 8- Werden die Benutzer von Analytics entdeckt?

Wenn Ereignisse an Citrix Analytics fließen, werden die Benutzer, die die Ereignisse generieren, erkannt und im **Benutzer-Dashboard** angezeigt. Dieser Vorgang dauert normalerweise etwa ein paar Minuten, bis Sie sie im Dashboard anzeigen können.

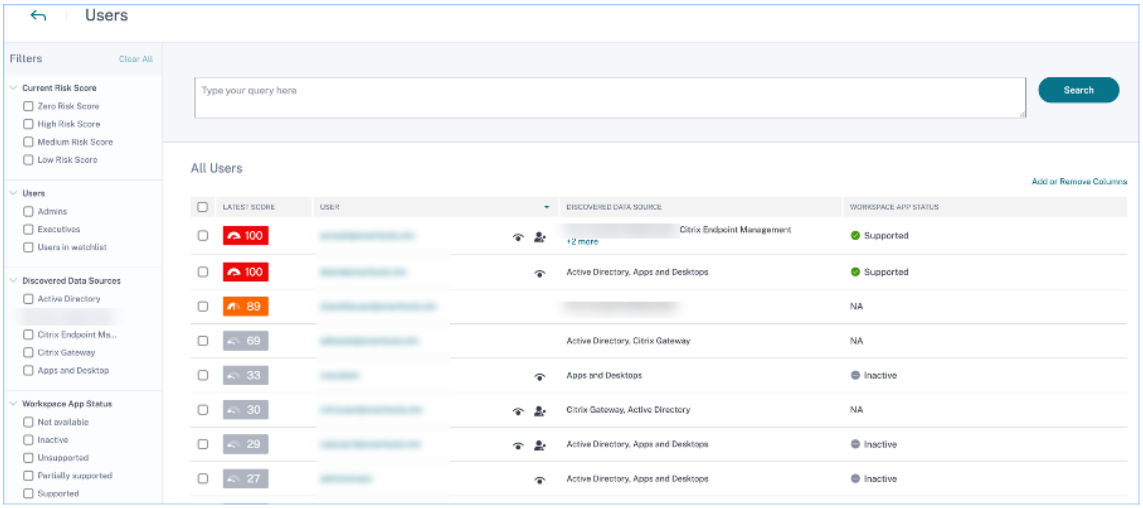
1. Klicken Sie im **Benutzer-Dashboard** auf den Link **Erkannte Benutzer**, um die vollständige Liste der von Citrix Analytics erkannten Benutzer anzuzeigen.

2. Auf der Seite **Benutzer** wird die Liste aller Benutzer angezeigt, die in den letzten 31 Tagen entdeckt wurden. Wählen Sie den Zeitraum aus, in dem die Vorkommen der Risikoindikatoren angezeigt werden sollen.

> **Hinweis:**
>
> Wenn Sie versuchen, einen höheren Wert als 31 Tage festzulegen, zeigt das System eine Fehlermeldung an, die besagt: **Ungültiger Datumsbereich. Der maximal zulässige**

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Zeitraum zwischen dem Start- und Enddatum beträgt 31 Tage.**



Wenn Ereignisse erfolgreich übertragen werden, funktioniert Ihre Citrix Analytics-Umgebung wie erwartet. Risikoindikatoren werden generiert, wenn Anomalien festgestellt werden.

Virtual Apps and Desktops-Ereignisse, SaaS-Ereignisse auslösen und Ereignisübertragung überprüfen

April 12, 2024

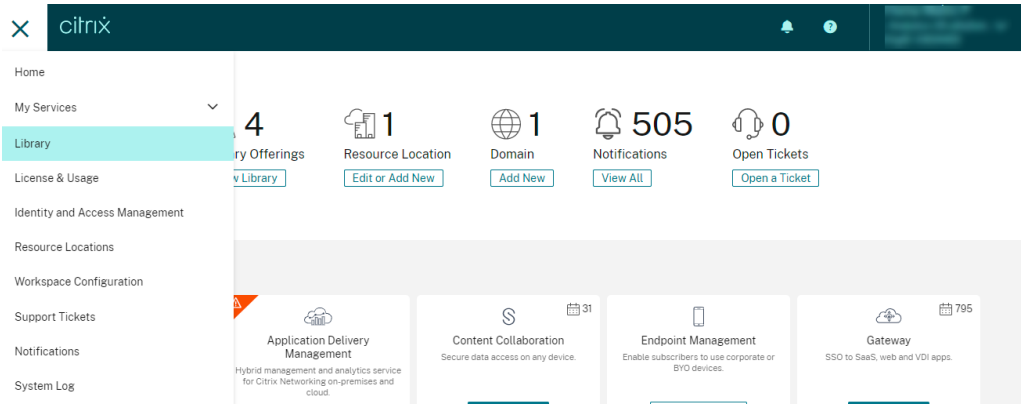
In diesem Abschnitt werden die Verfahren zum Auslösen von Apps- und Desktops-Ereignissen und SaaS-Ereignissen beschrieben und überprüft, ob Citrix Analytics for Security diese Benutzerereignisse aktiv empfängt.

Voraussetzungen

- Wenn Sie lokal verwenden Citrix Virtual Apps and Desktops, binden Sie Ihre on-premises Sites in Citrix Analytics ein und aktivieren Sie die Datenverarbeitung von der Sitekarte aus. Wenn Sie Citrix DaaS (früher Citrix Virtual Apps and Desktops Service) verwenden, aktivieren Sie die Datenverarbeitung direkt von der Sitekarte. Weitere Informationen finden Sie unter Citrix Virtual Apps and Desktops und Citrix DaaS-Datenquelle.
- Verwenden Sie die richtigen Versionen der Citrix Workspace-App oder Citrix Receiver auf den Endpunktgeräten der Benutzer, damit die Ereignisse korrekt an Citrix Analytics gesendet werden. Weitere Informationen finden Sie unter Citrix Virtual Apps and Desktops und Citrix DaaS-Datenquelle.

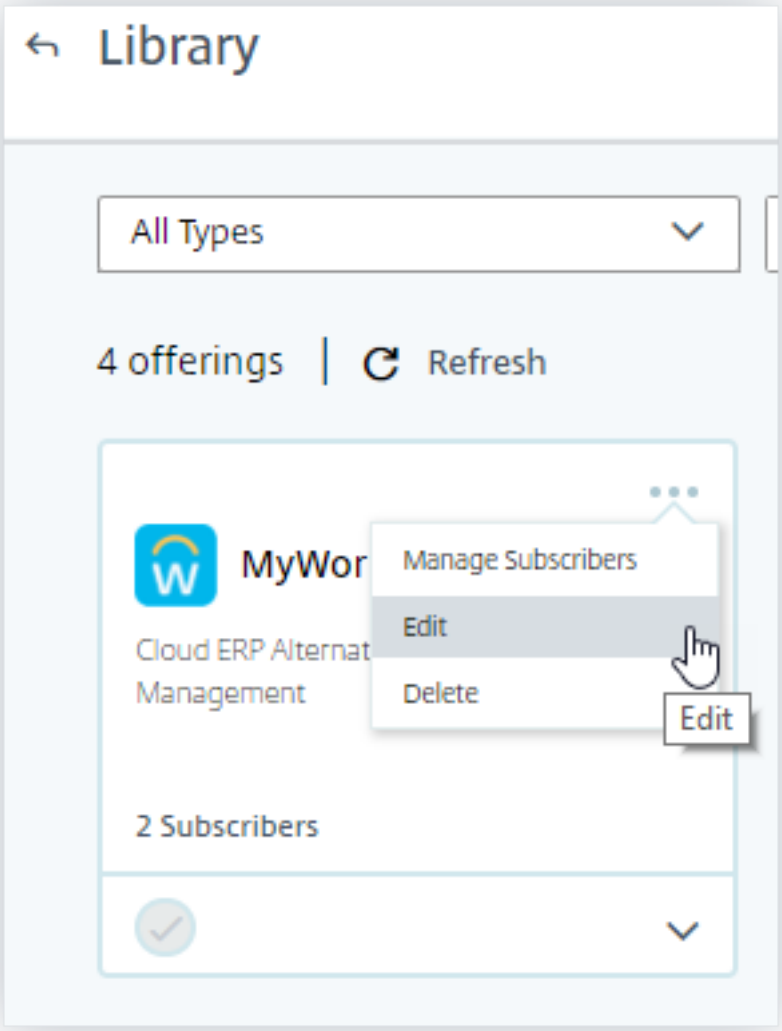
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Stellen Sie vor dem Auslösen des Druckereignisses von Ihrem virtuellen Desktop aus sicher, dass ein Drucker in Ihrer Apps- und Desktopumgebung konfiguriert und bereitgestellt ist. Weitere Informationen zum Verwalten eines Druckers finden Sie unter Drucken.
- Um SaaS-Ereignisse wie SaaS App Launch, SaaS-App-URL-Navigation und SaaS-App-Dateidownload auszulösen, müssen Sie eine konfigurierte SaaS-App aus Workspace verwenden. Zu den häufig verwendeten SaaS-Apps gehören Salesforce, Workday, Concur und GoTo Meeting.
  - Wenn keine konfigurierten SaaS-Apps vorhanden sind, müssen Sie eine SaaS-App konfigurieren und veröffentlichen. Weitere Informationen finden Sie unter Unterstützung für Software-as-a-Service-Apps. Stellen Sie beim Konfigurieren einer SaaS-App sicher, dass die folgenden Sicherheitsoptionen deaktiviert sind:
    - Zugriff auf Zwischenablage einschränken
    - Drucken einschränken
    - Navigation einschränken
    - Herunterladen einschränken
  - Wenn Sie eine bereits konfigurierte SaaS-App aus Ihrem Workspace verwenden möchten, um die Ereignisse auszulösen, stellen Sie sicher, dass die angegebenen erweiterten Sicherheitsoptionen für die SaaS-App deaktiviert sind:
    1. Gehen Sie zu Ihrem Citrix Cloud-Konto und wählen Sie **Bibliothek**aus.

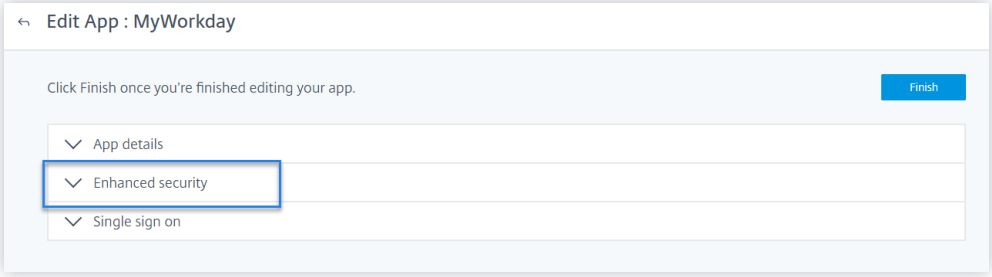


    2. Identifizieren Sie auf der Seite **Bibliothek** die SaaS-App, die Sie zur Überprüfung der Ereignisse verwenden möchten. Zum Beispiel Workday.
    3. Klicken Sie auf die Ellipsen und wählen Sie **Bearbeiten**aus.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

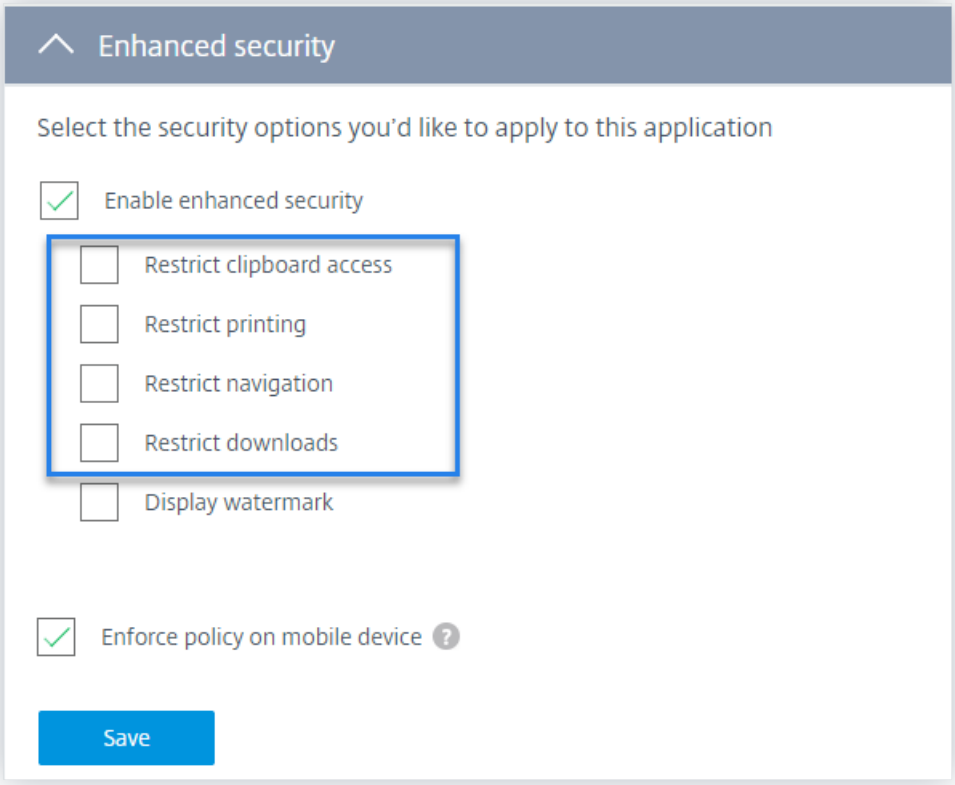


4. Klicken Sie auf der Seite **App bearbeiten** auf den Abwärtspfeil für Verbesserte Sicherheit.



5. Stellen Sie sicher, dass die folgenden Sicherheitsoptionen nicht ausgewählt sind.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Bekanntes Problem

Wenige Versionen der Citrix Workspace-App und Citrix Receiver senden einige Ereignisse nicht an Citrix Analytics. Daher kann Citrix Analytics keine Erkenntnisse liefern und Risikoindikatoren für diese Ereignisse generieren. Weitere Informationen zu dem Problem und seiner Problemumgehung finden Sie im bekannten Problem —CAS-16151.

Prozedur

Führen Sie nacheinander die folgenden Schritte aus, um die Ereignisse in Ihrer Apps- und Desktopumgebung auszulösen und sicherzustellen, dass Citrix Analytics for Security diese Ereignisse aktiv empfängt.

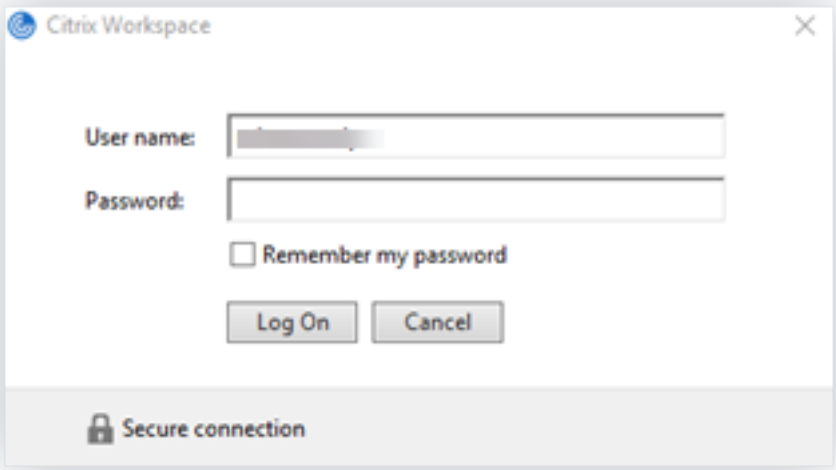
> **Hinweis**
>
> - Es kann einige Zeit dauern, bis die Ereignisse Citrix Analytics erreichen. Aktualisieren Sie die Citrix Analytics-Seite, wenn Sie die ausgelösten Ereignisse nicht sehen.
> - Für das Auslösen der SaaS-Ereignisse verwendet dieses Verfahren die Workday-App als

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

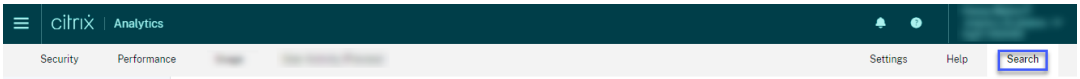
> Beispiel. Sie können alle konfigurierten SaaS-Apps aus Ihrem Workspace verwenden, um die SaaS-Ereignisse auszulösen.

- **Konto Logon**

  1. Starten Sie die Citrix Workspace-App oder Citrix Receiver, um auf Workspace oder Store-Front zuzugreifen.
  2. Geben Sie Ihre Anmeldeinformationen ein, um sich bei der Citrix Workspace-App oder Citrix Receiver anzumelden.

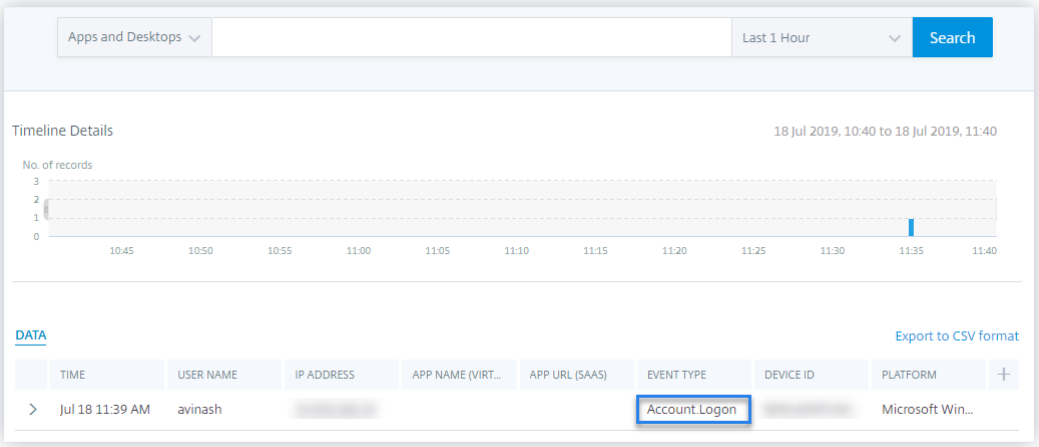


  3. Gehen Sie zu Citrix Analytics.
  4. Klicken Sie auf **Suchen** und wählen Sie **Apps und Desktops** aus der Liste aus.



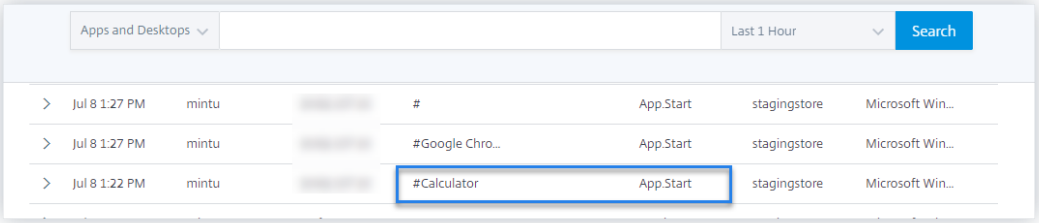
  5. Zeigen Sie auf der Suchseite die Daten für das **Account.Logon-Ereignis an** . Erweitern Sie die Zeile, um die Ereignisdetails anzuzeigen.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



- **App-Start**

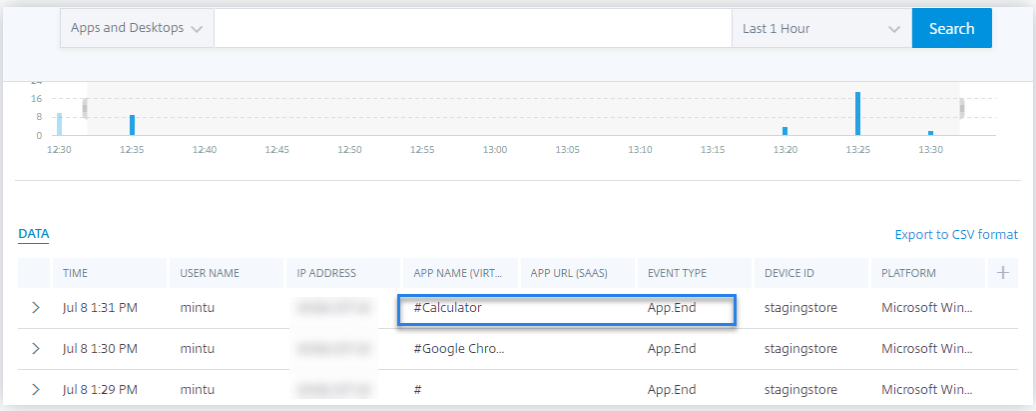
  1. Starten Sie die Citrix Workspace-App oder Citrix Receiver, um auf Workspace oder StoreFront zuzugreifen.
  2. Starten Sie eine Anwendung wie den Taschenrechner.
  3. Gehen Sie zu Citrix Analytics.
  4. Klicken Sie auf **Suchen** und wählen Sie **Apps und Desktops** aus.
  5. Zeigen Sie auf der Suchseite die Daten für die **App.Start-Ereignisdaten** an. Erweitern Sie die Zeile, um die Ereignisdetails anzuzeigen.



- **App-Ende**

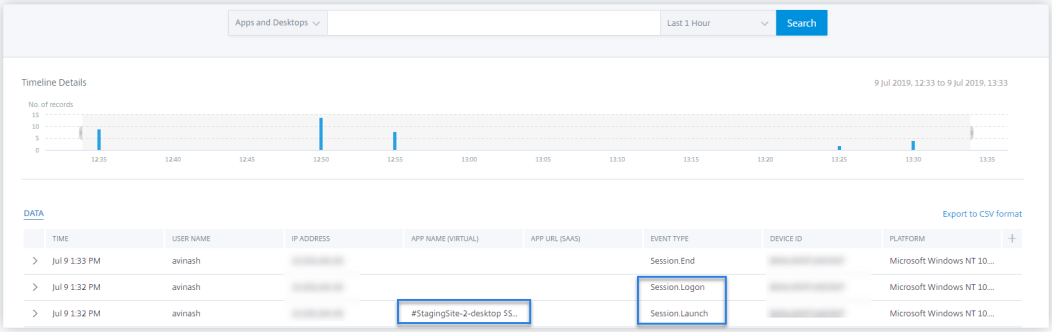
  1. Schließen Sie den Taschenrechner, den Sie bereits in Ihrem Workspace oder StoreFront gestartet haben.
  2. Gehen Sie zu Citrix Analytics.
  3. Klicken Sie auf **Suchen** und wählen Sie **Apps und Desktops** aus.
  4. Zeigen Sie auf der Suchseite die Daten für die **App.End-Ereignisdaten** an. Erweitern Sie die Zeile, um die Ereignisdetails anzuzeigen.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



- **Sitzungsanmeldung und Sitzungsstart**

  1. Starten Sie die Citrix Workspace-App oder Citrix Receiver, um auf Workspace oder Store-Front zuzugreifen.
  2. Starten Sie Ihren virtuellen Desktop.
  3. Gehen Sie zu Citrix Analytics.
  4. Klicken Sie auf **Suchen** und wählen Sie **Apps und Desktops** aus.
  5. Zeigen Sie auf der Suchseite die Daten für die Ereignisse **Session.Logon** und **Session.Launch** an. Erweitern Sie die Zeile, um die Ereignisdetails anzuzeigen.

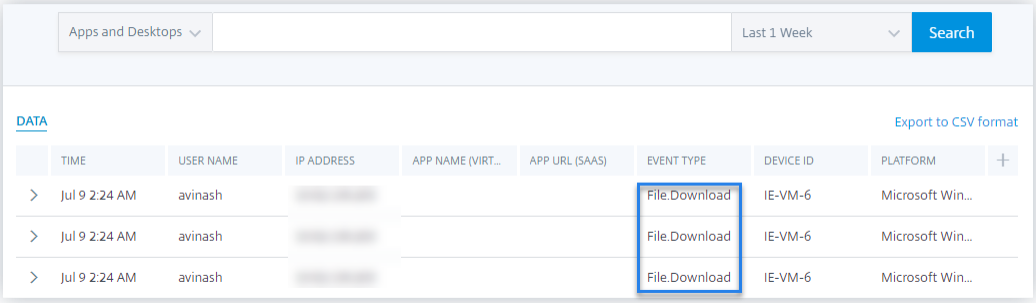


- **Datei Herunterladen**

  1. Starten Sie die Citrix Workspace-App oder Citrix Receiver, um auf Workspace oder Store-Front zuzugreifen.
  2. Starten Sie Ihren virtuellen Desktop.
  3. Kopieren Sie eine Datei von Ihrem virtuellen Desktop auf Ihren lokalen Computer.
  4. Gehen Sie zu Citrix Analytics.
  5. Klicken Sie auf **Suchen** und wählen Sie **Apps und Desktops** aus.

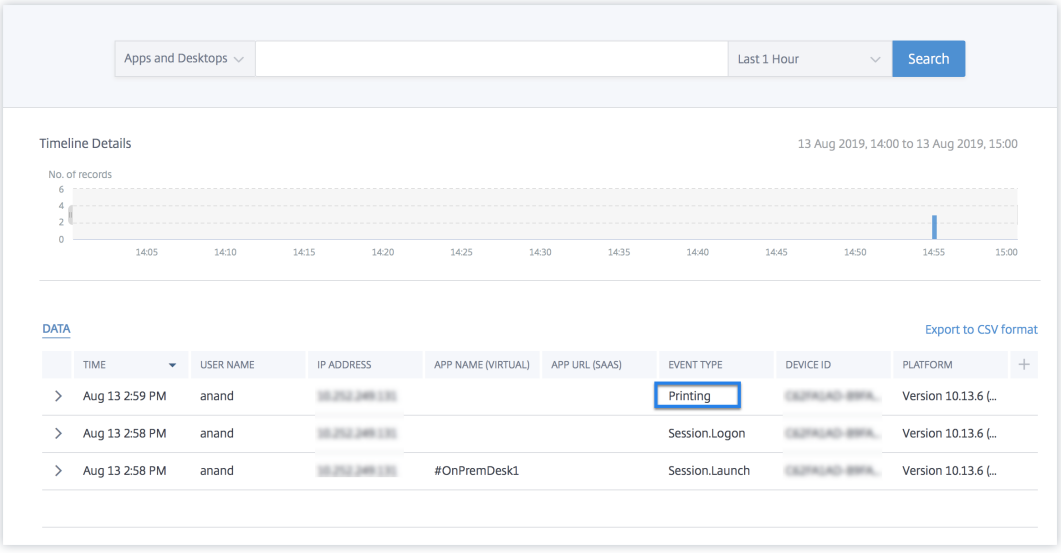
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

6. Zeigen Sie auf der Suchseite die Daten für das **File.Download-Ereignis** an. Erweitern Sie die Zeile, um die Ereignisdetails anzuzeigen.



- **Drucken**

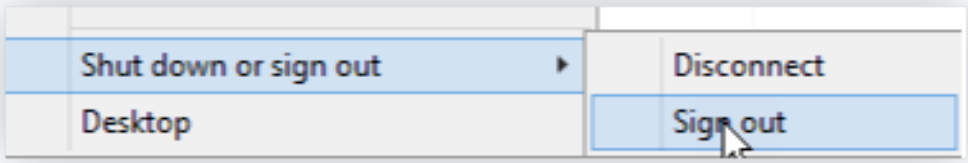
1. Starten Sie Citrix Workspace-App oder Citrix Receiver, um auf Workspace zuzugreifen
2. Starten Sie Ihren virtuellen Desktop.
3. Drucken Sie ein Dokument mit einem Drucker, der mit Ihrem virtuellen Desktop konfiguriert ist.
4. Gehen Sie zu Citrix Analytics.
5. Klicken Sie auf **Suchen** und wählen Sie **Apps und Desktops** aus.
6. Zeigen Sie auf der Seite Suchen die Daten für das **Druckereignis** an. Erweitern Sie die Zeile, um die Ereignisdetails anzuzeigen.



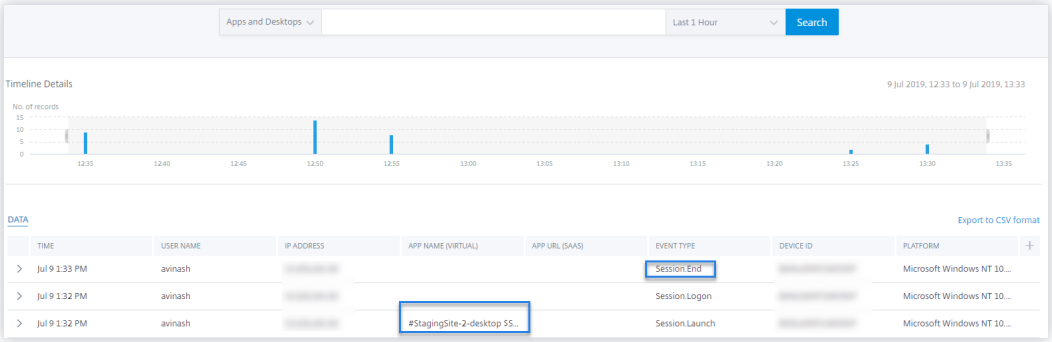
- **Ende der Sitzung**

1. Melden Sie sich von Ihrem virtuellen Desktop aus ab. Wenn Sie beispielsweise einen virtuellen Windows-Desktop verwenden, wählen Sie die Option **Abmelden** .

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



2. Gehen Sie zu Citrix Analytics.
3. Klicken Sie auf **Suchen** und wählen Sie **Apps und Desktops** aus.
4. Zeigen Sie auf der Suchseite die Daten für das **Session.End-Ereignis** an. Erweitern Sie die Zeile, um die Ereignisdetails anzuzeigen.



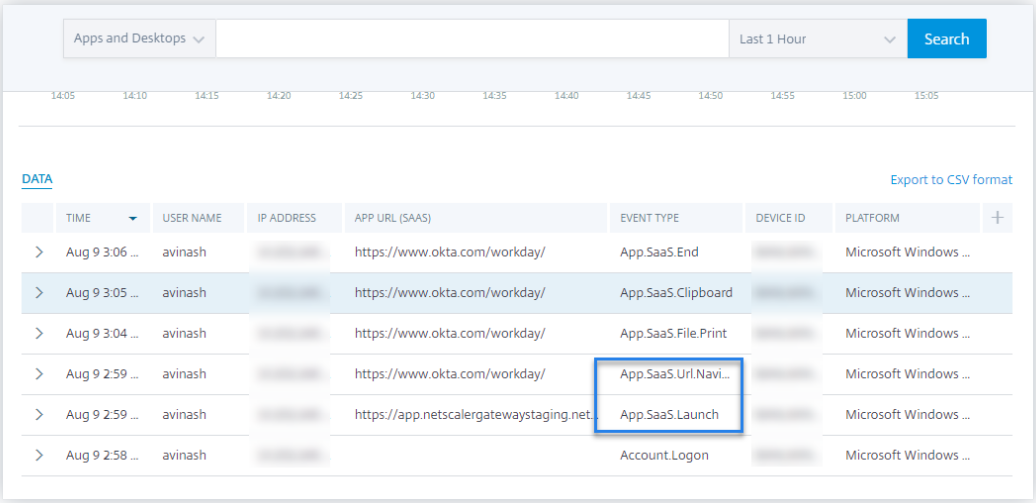
- **SaaS-App-Start und SaaS-App-URL-Navigation**

1. Starten Sie die Citrix Workspace-App oder Citrix Receiver, um auf Workspace oder Store-Front zuzugreifen.
2. Starten Sie eine SaaS-Anwendung wie Workday und warten Sie, bis die Workday-Seite geladen wurde. Navigieren Sie in Workday auf den Webseiten.

> **Hinweis**
>
> Stellen Sie sicher, dass die Option **Navigation einschränken** im Abschnitt Verbesserte Sicherheit deaktiviert ist. Weitere Informationen finden Sie unter **Voraussetzungen**.

3. Gehen Sie zu Citrix Analytics.
4. Klicken Sie auf **Suchen** und wählen Sie **Apps und Desktops** aus.
5. Zeigen Sie auf der **Suchseite** die Daten für die Ereignisse **App.SaaS.Launch** und **App.SaaS.URL.Navigation** an. Erweitern Sie die Zeile, um die Ereignisdetails anzuzeigen.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

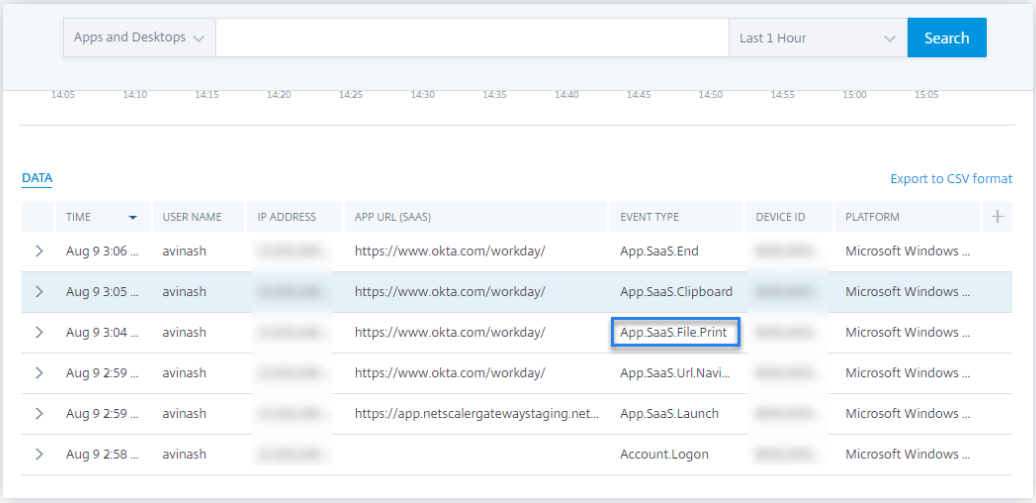


- **SaaS App Datei drucken**

  1. Drucken Sie die Workday-Seite, die Sie gerade anzeigen.

     > **Hinweis**
     >
     > Stellen Sie sicher, dass die Option **Drucken einschränken** im Abschnitt Verbesserte Sicherheit deaktiviert ist. Weitere Informationen finden Sie in den **Voraussetzungen**.

  2. Gehen Sie zu Citrix Analytics.
  3. Klicken Sie auf **Suchen** und wählen Sie **Apps und Desktops** aus.
  4. Zeigen Sie auf der Suchseite die Daten für das Ereignis **app.saas.File.print** an. Erweitern Sie die Zeile, um die Ereignisdetails anzuzeigen.



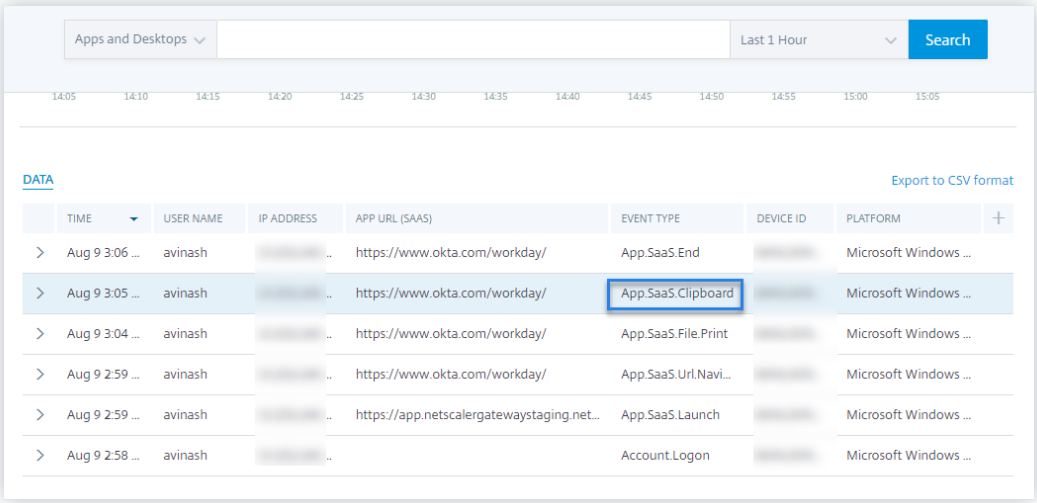
- **Zugriff auf SaaS App Zwischenablage**

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

1. Kopieren Sie auf der Workday-Seite Text in die Zwischenablage Ihres Systems.

> **Hinweis**
>
> Stellen Sie sicher, dass die Option **Zugriff auf die Zwischenablage beschränken** im Abschnitt Verbesserte Sicherheit deaktiviert ist. Weitere Informationen finden Sie in den **Voraussetzungen**.

2. Gehen Sie zu Citrix Analytics.
3. Klicken Sie auf **Suchen** und wählen Sie **Apps und Desktops** aus.
4. Zeigen Sie auf der Suchseite die Daten für das **app.saas.Clipboard-Ereignis an** . Erweitern Sie die Zeile, um die Ereignisdetails anzuzeigen.



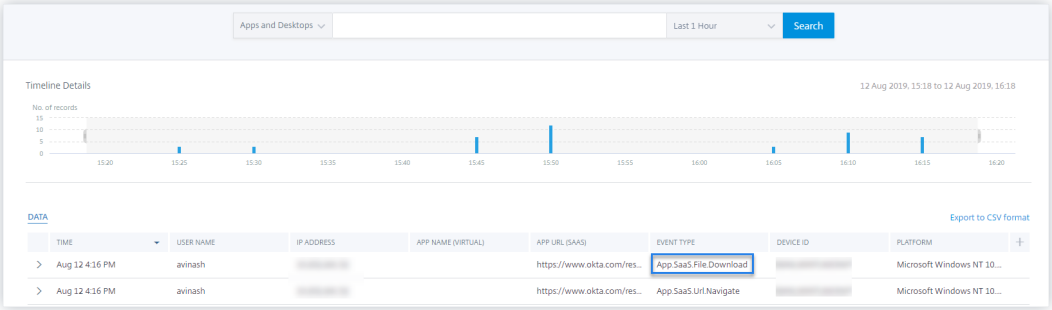
- **SaaS App Datei herunterladen**

1. Suchen Sie auf der Workday-Seite nach einem öffentlichen Dokument wie Whitepaper, und laden Sie das Dokument herunter.

> **Hinweis**
>
> Stellen Sie sicher, dass die Option **Downloads einschränken** im Abschnitt Verbesserte Sicherheit deaktiviert ist. Weitere Informationen finden Sie in den **Voraussetzungen**.

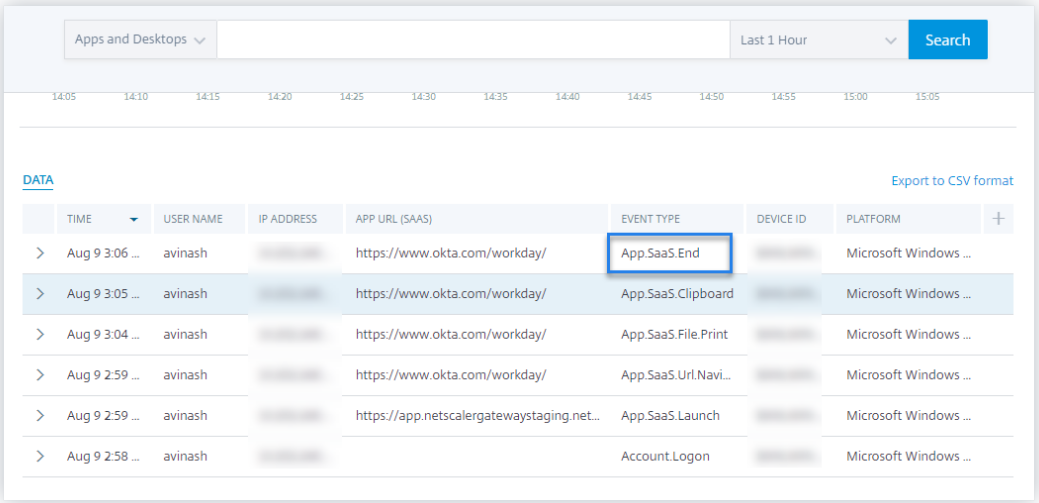
2. Gehen Sie zu Citrix Analytics.
3. Klicken Sie auf Suchen und wählen Sie **Apps und Desktops**aus.
4. Zeigen Sie auf der Seite Suchen die Daten für das Ereignis **app.saas.File.Download** an. Erweitern Sie die Zeile, um die Ereignisdetails anzuzeigen.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



- **SaaS App Ende**

  1. Schließen Sie die Workday-Seite.
  2. Gehen Sie zu Citrix Analytics.
  3. Klicken Sie auf **Suchen** und wählen Sie **Apps und Desktops** aus.
  4. Zeigen Sie auf der Suchseite die Daten für das Ereignis **app.saas.end** an. Erweitern Sie die Zeile, um die Ereignisdetails anzuzeigen.



- **VDA.Drucken**

  Voraussetzungen

  Bevor Sie das Druckereignis auslösen, lesen Sie den Abschnitt Drucktelemetrie für Citrix DaaS aktivieren.

  Führen Sie die folgenden Aktionen aus, um ein Druckereignis auszulösen:

  1. Öffnen Sie ein Textdokument mit Notepad oder einer anderen App, in der das Drucken zulässig ist.
  2. Klicken Sie auf **Datei > Drucken** oder drücken Sie **Strg+P**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

3. Wählen Sie unter Drucker auswählen den gewünschten Drucker aus, klicken Sie auf **Übernehmen** und dann auf "Drucken".

- **VDA.Zwischenablage**

  Voraussetzungen

  Bevor Sie das Druckereignis auslösen, lesen Sie den Abschnitt Telemetrie in der Zwischenablage für Citrix DaaS aktivieren.

  Gehen Sie wie folgt vor, um ein Zwischenablage-Ereignis auszulösen:

  1. Öffnen Sie ein Textdokument mit Notepad oder einem beliebigen Texteditor.
  2. Wählen Sie den zu kopierenden Inhalt aus.
  3. Klicken Sie mit der rechten Maustaste auf Kopieren oder drücken Sie Strg+C.

Keine Benutzerereignisse von unterstützter Citrix Workspace-Appversion empfangen

July 12, 2022

Wenn Sie keine Ereignisse von einem Benutzer sehen, der eine Citrix Workspace-App-Version verwendet, die von Citrix Analytics unterstützt wird, liegt das Problem möglicherweise in einem der folgenden Probleme:

- Konfigurieren in StoreFront
- Anforderung für den Webstart

Konfigurieren in StoreFront

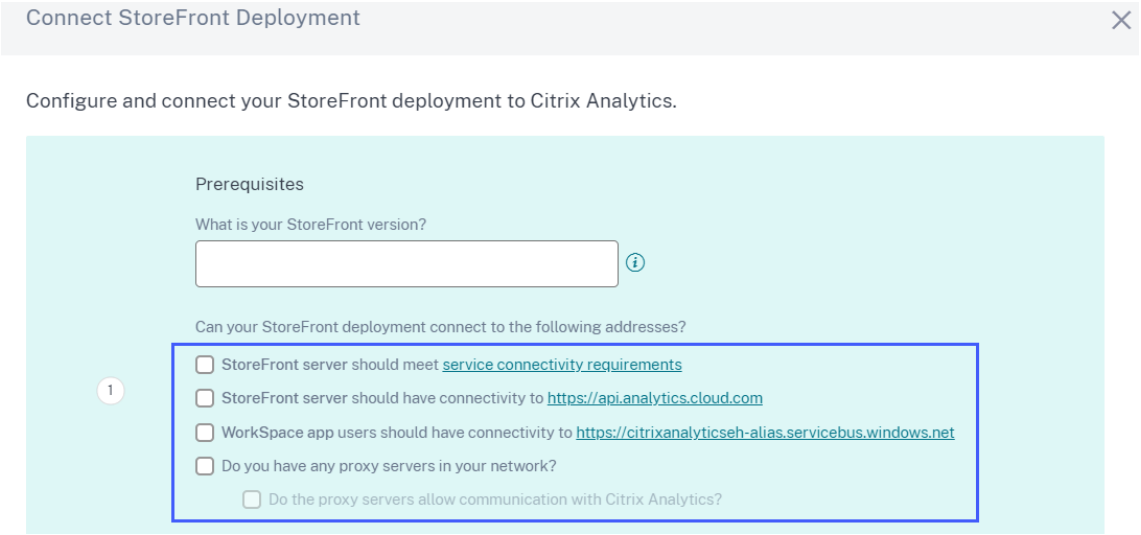
Wenn eine StoreFront-Bereitstellung mit Citrix Analytics verbunden ist, überprüfen Sie den **Zeitstempel Letzte Aktualisierung**. Die Uhrzeit muss mindestens einmal pro Woche aktualisiert werden, wenn Benutzer aktiv auf StoreFront zugreifen. Häufige Aktualisierungen deuten auf eine fehlerfreie Verbindung zwischen StoreFront-Bereitstellung und Citrix Analytics hin. Andernfalls gibt es einige Konnektivitätsprobleme.

Überprüfen Sie die folgenden Konnektivitätsanforderungen:

- Der StoreFront-Server muss die System- und Konnektivitätsanforderungen erfüllen.
- Der StoreFront-Server muss eine Verbindung herstellen können `https://api.analytics.cloud.com`

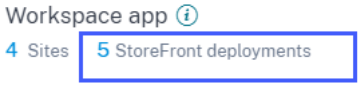
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Benutzer der Workspace-App müssen eine Verbindung herstellen können `https://citrixanalyticseh-alias.servicebus.windows.net`
- Ihr Proxyserver muss die Verbindung zum Citrix Analytics-Ereignishub zulassen:
  - **Region der Vereinigten Staaten**: `https://citrixanalyticseh-alias.servicebus.windows.net/`
  - **Region der Europäischen Union**: `https://citrixanalyticseheu-alias.servicebus.windows.net/`
  - Region**Asien-Pazifik Süd**: `https://citrixanalyticsehaps-alias.servicebus.windows.net/`



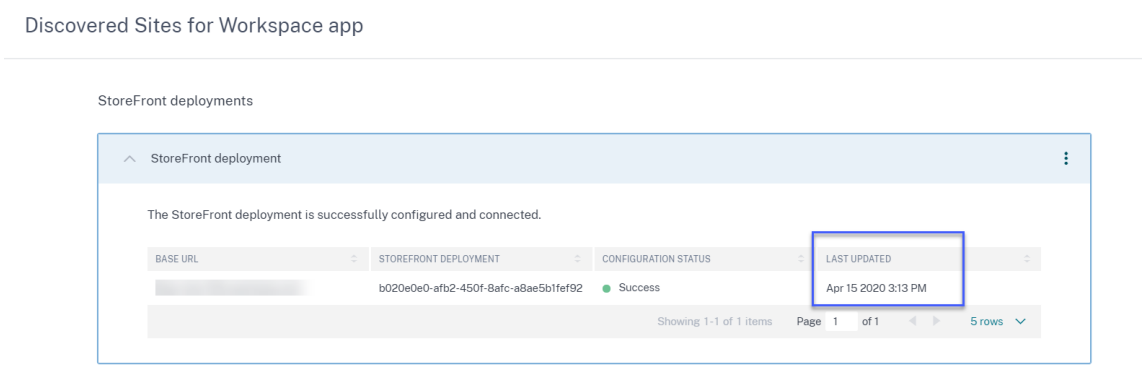
Um die Uhrzeit der letzten Aktualisierung zu überprüfen:

1. Klicken Sie auf **Einstellungen > Datenquellen**.
2. Klicken Sie auf der Sitekarte der Workspace-App auf die Anzahl der verbundenen StoreFront-Server.



3. Überprüfen Sie bei der StoreFront-Bereitstellung die Uhrzeit der letzten Aktualisierung.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Wenn der letzte aktualisierte Zeitstempel auch nach Erfüllung der Konnektivitätsanforderungen nicht häufig aktualisiert wird, konfigurieren Sie Ihren StoreFront neu. Weitere Informationen finden Sie unter Onboard Virtual Apps and Desktops Sites mit StoreFront.

Anforderung für den Webstart

Ein Benutzer kann virtuelle Apps und Desktops auf eine der folgenden Arten starten:

- Greifen Sie über die Citrix Workspace-App auf Citrix Store oder Citrix Workspace zu. Dieser Ansatz wird als Native Launch bezeichnet.
- Öffnen Sie die Citrix Store-URL oder die Citrix Workspace-URL in einem Webbrowser. Klicken Sie auf eine Anwendung oder einen virtuellen Desktop, um die entsprechende ICA-Datei herunterzuladen. Öffnen Sie dann die ICA-Datei mit einem Webbrowser, um die Anwendung oder den virtuellen Desktop zu starten. Dieser Ansatz wird als Webstart bezeichnet.

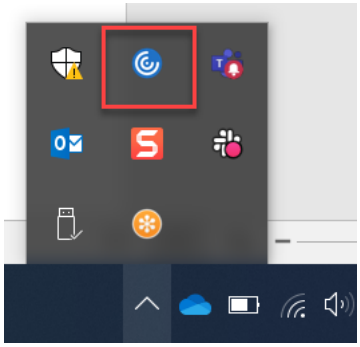
Stellen Sie für den Webstart sicher, dass das Benutzergerät über einen der folgenden Clients verfügen muss, der auf dem Betriebssystem des Geräts basiert.

Client	Version	Build
Citrix Workspace-App für Windows	2006.1 oder höher	20.6.0.38 oder höher
Citrix Workspace-App für Mac	2006 oder höher	20.06.0.7 oder höher

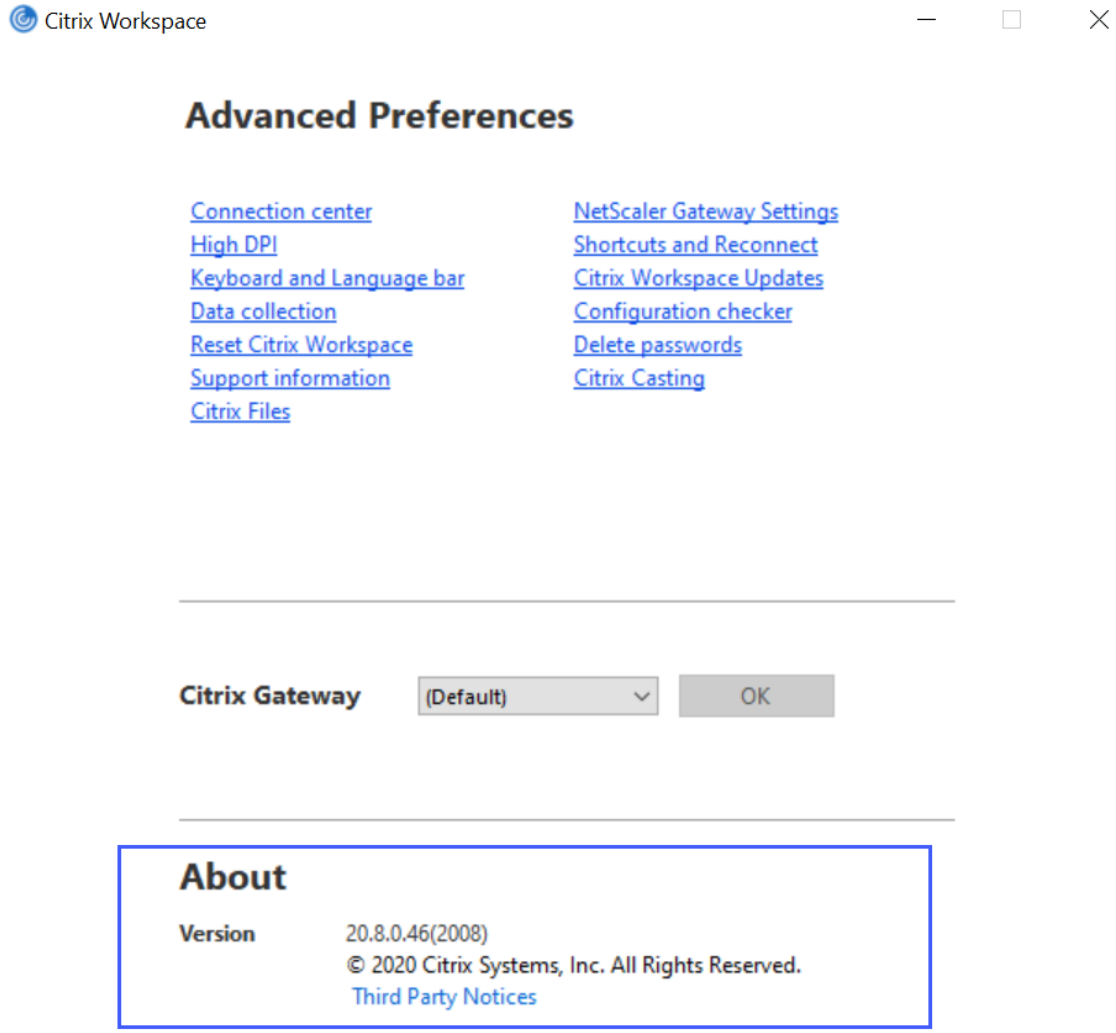
So überprüfen Sie die Version der Citrix Workspace-App:

1. Klicken Sie auf dem lokalen Computer des Benutzers mit der rechten Maustaste auf das Citrix Workspace-App-Symbol.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



2. Klicken Sie auf **Erweiterte Einstellungen** und überprüfen Sie den Abschnitt **Info**, um die Version anzuzeigen.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Konfigurierter Sitzungsaufzeichnungsserver kann keine Verbindung herstellen

July 12, 2022

Ihr Sitzungsaufzeichnungsserver kann nach der Konfigurationkeine Verbindung zu Citrix Analytics herstellen. Daher wird der konfigurierte Server nicht auf der Sitekarte der **Sitzungsaufzeichnung** angezeigt.

Gehen Sie wie folgt vor, um dieses Problem zu beheben:

1. Führen Sie auf Ihrem konfigurierten Sitzungsaufzeichnungsserver den folgenden PowerShell-Befehl aus, um die Client-Maschinen-Identifizierung (CMID) zu überprüfen

```
Get-WmiObject -class SoftwareLicensingService | select
    Clientmachineid
```

2. Wenn CMID leer ist, fügen Sie die folgenden Registrierungsdateien in den angegebenen Pfaden hinzu.

Name	Registrierungspfad	Schlüsseltyp	Wert
AuditorUniqueID	Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\Server\	Zeichenfolge	Geben Sie Ihre UUID ein.
EnableCASUseAuditorUniqueID	Computer/HKEY_LOCAL_MACHINE/SOFTWARE/Citrix/SmartAuditor/Server/	REG_DWORD	1

3. Starten Sie die folgenden Dienste neu:
    - Analysedienst der Citrix Sitzungsaufzeichnung
    - Speichermanager der Citrix Sitzungsaufzeichnung

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

StoreFront-Server kann nicht mit Citrix Analytics verbunden werden

January 4, 2023

Nach dem Importieren der Konfigurationseinstellungen von Citrix Analytics auf Ihren StoreFront-Server kann der StoreFront-Server keine Verbindung zu Citrix Analytics herstellen.

Informationen zum Importieren von Konfigurationseinstellungen auf einen StoreFront-Server finden Sie unter Integrieren von Websites Virtual Apps and Desktops mit StoreFront.

Der CAS-Onboarding-Assistent hilft bei der Überprüfung und Behebung der in diesem Artikel beschriebenen Probleme. Weitere Informationen finden Sie unter Onboarding-Assistent für Citrix Analytics Service (CAS).

Gehen Sie wie folgt vor, um das Problem zu beheben:

1. Pingen Sie auf dem StoreFront-Server die regionsspezifischen Endpunkte von Citrix Analytics, um die Konnektivität zwischen dem StoreFront-Server und dem Citrix Analytics-Server zu testen. Stellen Sie außerdem sicher, dass die Voraussetzungen erfüllt sind.

   > **Hinweis**
   >
   > Auf Ihrem StoreFront-Server können Sie die Konnektivität testen, indem Sie die regionsspezifischen Endpunkte direkt anpingen oder einen Webbrowser öffnen und auf die regionsspezifischen Endpunkte zugreifen.

2. Aktivieren Sie die ausführliche Protokollierung im StoreFront-Server, um die Protokolle zu verfolgen. Weitere Informationen zur ausführlichen Protokollierung finden Sie im Artikel CTX139592.
3. Öffnen Sie den Internetinformationsdienste-Manager (IIS) und überprüfen Sie Folgendes:
   - Wenn sich die StoreFront-Site unter der IIS-Standardsite befindet, startet IIS die StoreFront-Site neu.
   - Wenn sich die StoreFront-Site in anderen Treibern befindet oder nicht unter der Standard-Site, öffnen Sie das Befehlsfenster und geben Sie ein `iisreset`.
4. Führen Sie folgenden Befehl aus, um die Citrix Analytics-Einstellungen zu importieren:

   ```
   Import-STFCasConfiguration -Path "configuration file path"
   ```

5. Führen Sie den folgenden Befehl aus, um die importierten Einstellungen zu überprüfen:

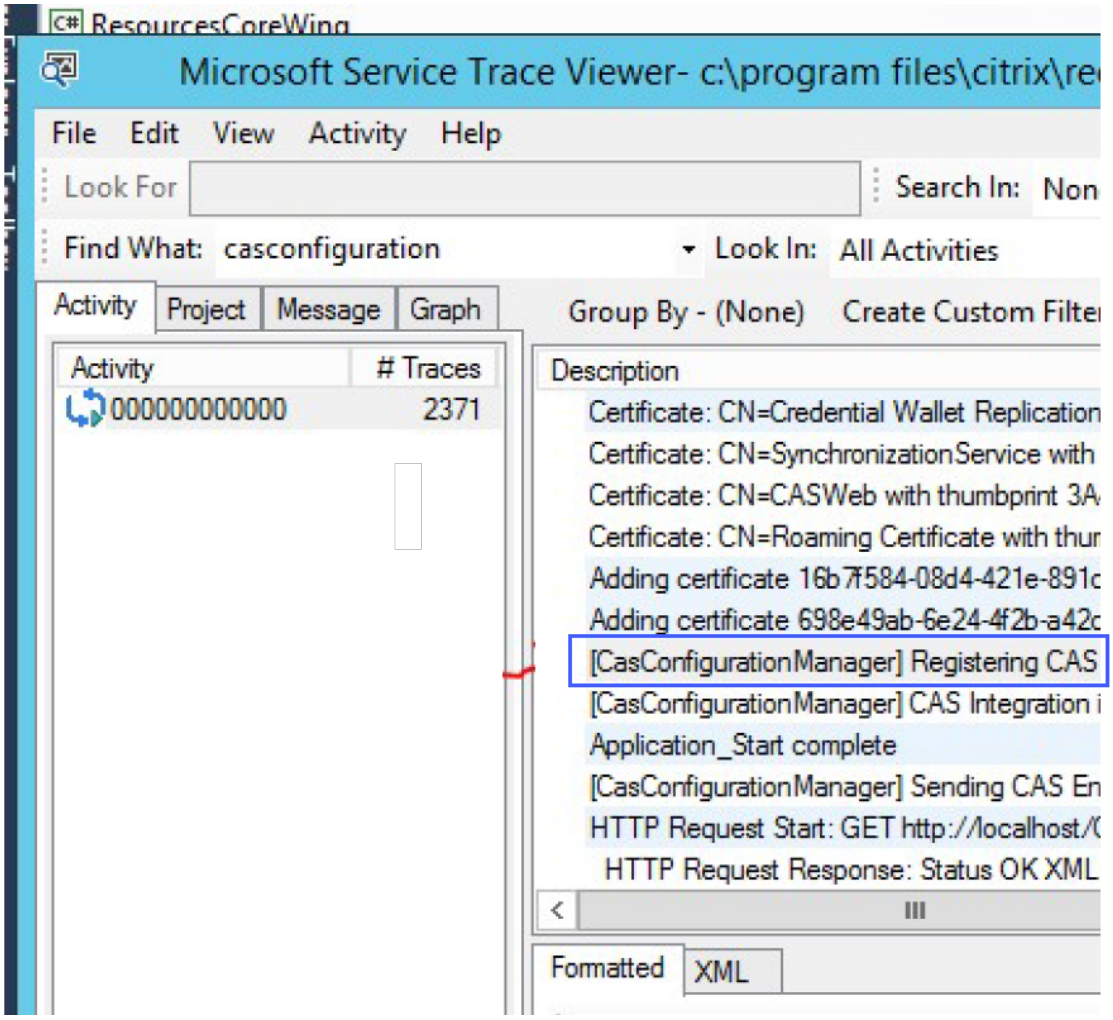
   ```
   Get-STFCasConfiguration
   ```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

6. Wenn sich die StoreFront-Site in anderen Treibern befindet oder nicht unter der Standard-Site, öffnen Sie das Befehlsfenster. Geben Sie `iisreset` ein, damit die StoreFront-Site Citrix Analytics-Einstellungen
7. Rufen Sie die ausführlichen StoreFront-Protokolldateien von folgendem Speicherort ab:

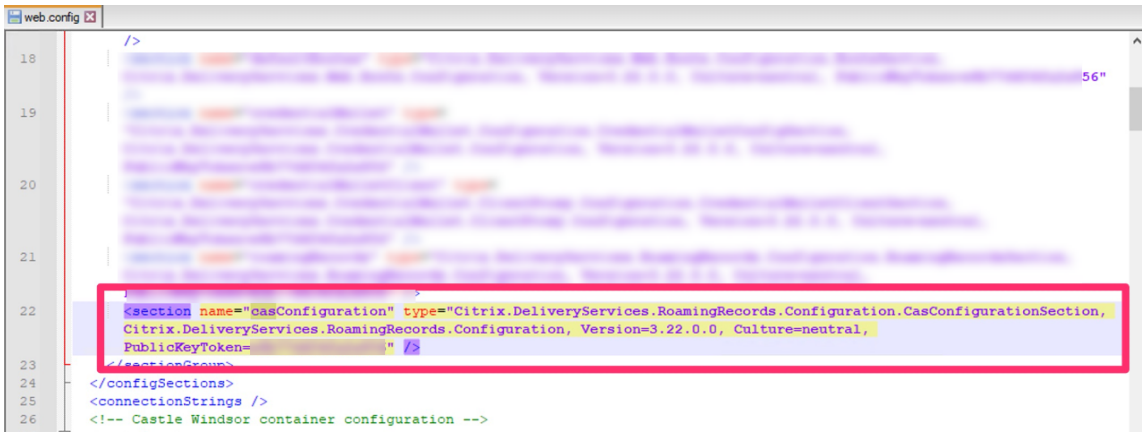
```
1 C:\Program Files\Citrix\Receiver StoreFront\Admin\trace
```

   Unter dem oben genannten Speicherort finden Sie mehrere svclog-Dateien, die in der Ereignisanzeige geöffnet werden können.
8. Verwenden Sie den Microsoft Service Trace Viewer, um die folgenden Protokolle zu öffnen:
   - StoreFront-Protokolle
   - Ausführliche Protokolle der Roaming-Site
9. Stellen Sie in den Protokollen sicher, dass die Abschnitte **CasConfigurationManager** und Citrix Analytics-Serverinformationen verfügbar sind.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

10. Wenn die Abschnitte von CasConfigurationManager nicht verfügbar sind, öffnen Sie die Datei web.config für die Roaming-Site, die Sie unter `roaming site\folder` finden.
11. Suchen Sie in der Datei `web.config` den Abschnitt **casConfiguration** und stellen Sie sicher, dass die Citrix Analytics-Serverinformationen verfügbar sind.



12. Stellen Sie auf den Windows Server-Computern, auf denen der StoreFront-Server installiert ist, Folgendes sicher:
    - Der TLS 1.2 Client ist aktiviert.
    - Mindestens eine der folgenden Verschlüsselungssammlungen ist aktiviert:
        - `TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384`
        - `TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256`
        - `TLS_DHE_RSA_WITH_AES_256_GCM_SHA384`
        - `TLS_DHE_RSA_WITH_AES_128_GCM_SHA256`

    Informationen zum Konfigurieren der TLS-Verschlüsselungssammlungsreihenfolge finden Sie in der Microsoft-Dokumentation.
13. Wenn Sie Windows Server 2012-Computer verwenden, stellen Sie sicher, dass Diffie-Hellman Exchange (ECDHE/DHE) aktiviert ist.
14. Stellen Sie sicher, dass die Windows Server-Computer, auf denen der StoreFront-Server installiert ist, die in der Microsoft-Dokumentationgenannten Registrierungseinstellungen enthalten müssen.

> **WICHTIG**
>
> Aktualisieren Sie die TLS/SSL-Verschlüsselungssammlungen mithilfe von Gruppenrichtlinien. Ändern Sie die TLS/SSL-Verschlüsselungssammlungen nicht manuell. Weitere Informationen zur Verwendung von Gruppenrichtlinien finden Sie in der Microsoft-Dokumentation.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Beispielsweise müssen die folgenden Registrierungseinstellungen auf Ihrem Windows Server-Computer verfügbar sein:

TLS 1.2 Kunde:

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\
   SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Client]
"Enabled"=dword:00000001
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\
   SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Client]
"DisabledByDefault"=dword:00000000

<!--NeedCopy-->
```

Diffie-Hellman-KEAs:

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\
   SecurityProviders\SCHANNEL\KeyExchangeAlgorithms\Diffie-Hellman
   ]
"Enabled"=dword:ffffffff
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\
   SecurityProviders\SCHANNEL\KeyExchangeAlgorithms\ECDH]
"Enabled"=dword:ffffffff

<!--NeedCopy-->
```

AES-128/AES-256-Verschlüsselungen:

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\
   SecurityProviders\SCHANNEL\Ciphers\AES 128/128]
"Enabled"=dword:ffffffff
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\
   SecurityProviders\SCHANNEL\Ciphers\AES 256/256]
"Enabled"=dword:ffffffff

<!--NeedCopy-->
```

SHA256/SHA384-Hashes:

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\
   SecurityProviders\SCHANNEL\Hashes\SHA256]
"Enabled"=dword:ffffffff
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\
   SecurityProviders\SCHANNEL\Hashes\SHA384]
"Enabled"=dword:ffffffff

<!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Häufig gestellte Fragen

November 16, 2023

Datenquelle

Was ist eine Datenquelle?

Datenquellen sind Dienste und Produkte von Citrix, die Daten an Citrix Analytics senden.

Weitere Informationen: Datenquelle

Wie füge ich eine Datenquelle hinzu?

Nachdem Sie sich bei Citrix Analytics angemeldet haben, wählen Sie auf dem **Begrüßungsbildschirm** die Option **Erste Schritte** aus, um Citrix Analytics eine Datenquelle hinzuzufügen. Alternativ können Sie auch eine Datenquelle hinzufügen, indem Sie zu **Einstellungen > Datenquellen** navigieren.

NetScaler ADM Agent

Was sind die Mindestanforderungen an Ressourcen, um einen Agenten auf einem Hypervisor on-premises zu installieren?

8 GB RAM, 4 virtuelle CPU, 120 GB Speicher, 1 virtuelle Netzwerkschnittstellen, 1 Gbit/s Durchsatz

Muss ich NetScaler ADM Agenten während der Bereitstellung einen zusätzlichen Datenträger zuweisen?

Nein, Sie müssen keinen zusätzlichen Datenträger hinzufügen. Der Agent wird nur als Vermittler zwischen Citrix Analytics und den Instanzen in Ihrem Unternehmensrechenzentrum verwendet. Es werden keine Bestands- oder Analysedaten gespeichert, für die ein zusätzlicher Datenträger erforderlich wäre.

Was sind die Standardanmeldeinformationen für die Anmeldung bei einem Agenten?

Die Standardanmeldeinformationen für die Anmeldung am Agenten lauten `nsrecover`/`nsroot`. Dadurch werden Sie an der Shell-Eingabeaufforderung des Agenten angemeldet.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Wie ändere ich die Netzwerkeinstellungen eines Agenten, wenn ich einen falschen Wert eingegeben habe?

Melden Sie sich bei der Agent-Konsole auf Ihrem Hypervisor an, greifen Sie mit den Anmeldeinformationen `nsrecover`/`nsroot`auf die Shell-Eingabeaufforderung zu. Führen Sie dann den Befehl aus `networkconfig`.

Warum benötige ich eine Service-URL und einen Aktivierungscode?

Der Agent verwendet die Dienst-URL, um den Dienst zu finden, und den Aktivierungscode, um den Agenten beim Dienst zu registrieren.

Wie kann ich die Dienst-URL erneut eingeben, wenn ich sie in der Agent-Konsole falsch eingegeben habe?

Melden Sie sich mit den Anmeldeinformationen `nsrecover`/an der Shell-Eingabeaufforderung des Agenten an`nsroot`, und geben Sie dann: ein `deployment_type.py`. Mit diesem Skript können Sie die Service-URL und den Aktivierungscode erneut eingeben.

Wie erhalte ich einen neuen Aktivierungscode?

Sie können einen neuen Aktivierungscode vom NetScaler ADM Service erhalten. Melden Sie sich beim NetScaler ADM Service an und navigieren Sie zu **Netzwerke > Agenten**. Wählen Sie auf der Seite **Agenten** in der Liste **Aktion auswählen** die Option **Aktivierungscode generieren** aus.

Kann ich meinen Aktivierungscode mit mehreren Agents wiederverwenden?

Nein, das geht nicht.

Wie viele NetScaler ADM Agents muss ich installieren?

Die Anzahl der Agents hängt von der Anzahl der verwalteten Instanzen in einem Rechenzentrum und dem Gesamtdurchsatz ab. Citrix empfiehlt, mindestens einen Agent für jedes Datencenter zu installieren.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Wie installiere ich mehrere NetScaler ADM Agents?

Klicken Sie auf der Seite Datenquellen auf das Pluszeichen (+) neben NetScaler Gateway, und befolgen Sie die Anweisungen zum Installieren eines anderen Agents.

Alternativ können Sie auf die NetScaler ADM-GUI zugreifen und zu Netzwerke > Agenten navigieren und auf **Agent einrichten** klicken, um mehrere Agents zu installieren.

Kann ich zwei Agenten in einem Hochverfügbarkeits-Setup installieren?

Nein, das geht nicht.

Was mache ich, wenn meine Agentregistrierung fehlschlägt?

- Stellen Sie sicher, dass Ihr Agent Zugriff auf das Internet hat (DNS konfigurieren).
- Stellen Sie sicher, dass Sie den Aktivierungscode korrekt kopiert haben.
- Stellen Sie sicher, dass Sie die Service-URL korrekt eingegeben haben.
- Stellen Sie sicher, dass die erforderlichen Ports geöffnet sind.

Die Registrierung war erfolgreich, aber woher weiß ich, ob der Agent gut läuft?

Sie können Folgendes tun, um zu überprüfen, ob der Agent einwandfrei läuft:

- Nachdem der Agent erfolgreich registriert wurde, greifen Sie auf NetScaler ADM zu und navigieren Sie zu **Netzwerke > Agenten**. Sie können die erkannten Agenten auf dieser Seite anzeigen. Wenn der Agent einwandfrei läuft, wird der Status durch ein grünes Symbol angezeigt. Wenn es nicht ausgeführt wird, wird der Status durch ein rotes Symbol angezeigt.
- Melden Sie sich bei der Shell-Eingabeaufforderung des Agenten an und führen Sie die folgenden Befehle aus: `ps -ax | grep masps -ax | grep ulfd` Stellen Sie sicher, dass die folgenden Prozesse ausgeführt werden.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

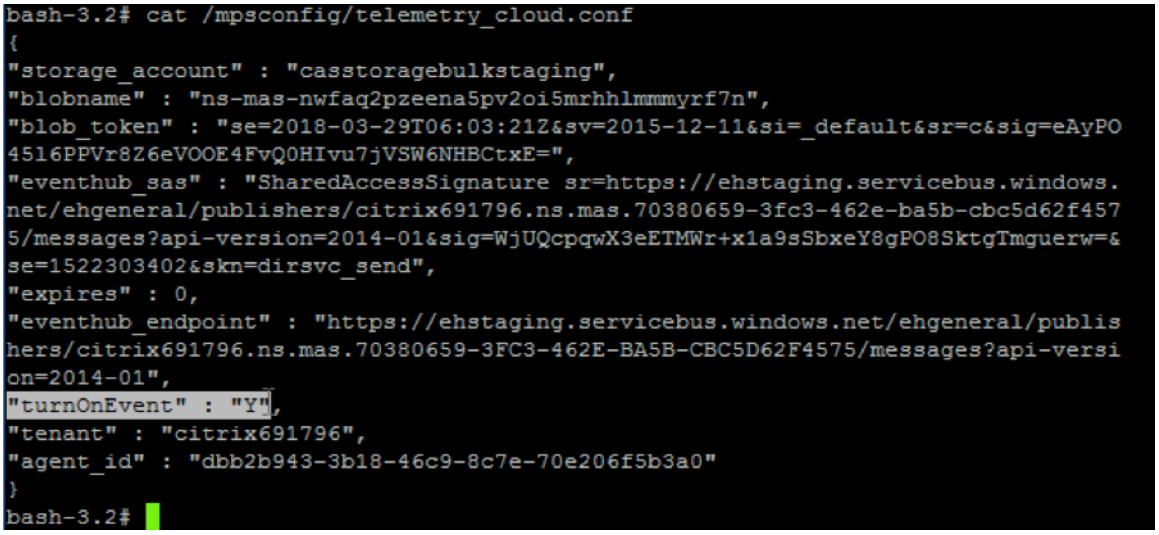
- Wenn einer der Prozesse nicht ausgeführt wird, führen Sie den Befehl **masd restart** aus. Dies kann einige Zeit dauern, um alle Daemons zu starten (etwa 1 Minute).
- Stellen Sie sicher, dass `agent.conf` nach erfolgreicher Registrierung des Agents in `/mpsconfig` erstellt wurde.

Onboarding von Citrix Gateway-Instanzen

Citrix Gateway-Instanzen werden zu Citrix Analytics hinzugefügt, aber woher weiß ich, ob Analytics auf dem Agent aktiviert ist?

Sie können anhand der Shell-Eingabeaufforderung des Agenten überprüfen, ob Analytics auf dem Agent aktiviert ist. Wenn Analytics erfolgreich auf dem Agenten aktiviert wurde, wird der Parameter `turnOnEvent` in der Datei `/mpsconfig/telemetry_cloud.conf` auf `Y` gesetzt.

Melden Sie sich bei der Shell-Eingabeaufforderung des Agents an und führen Sie den folgenden Befehl aus: cat `/mpsconfig/telemetry_cloud.conf` und überprüfen Sie den Wert des Parameters `turnOnEvent`.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Ich habe versehentlich den NetScaler Gateway-Onboardingassistenten geschlossen. Muss ich meine Konfiguration von Anfang an starten?

Nein. Citrix Analytics speichert den Fortschritt und zeigt die unvollständige Konfiguration als Kachel auf der Seite **Datenquellen > Einstellungen** an. Klicken Sie auf **Setup fortsetzen**, um die Konfiguration abzuschließen.

Onboarding der Website für Virtual Apps and Desktops

Wie schalte ich die Datenverarbeitung aus?

Wenn Sie die Datenverarbeitung von Ihrer Site zu Citrix Analytics vorübergehend deaktivieren möchten, klicken Sie einfach auf die **Sitekarte** und dann auf **Datenverarbeitung deaktivieren**.

Wenn ich meine Site zu Workspace hinzufüge und auf "STA testen"klicke, schlägt der Test fehl. Welche Schritte sind erforderlich?

Möglicherweise liegt ein Verbindungsproblem zwischen Ihrem NetScaler Gateway und Cloud Connectors vor. Informationen zur Fehlerbehebung finden Sie unter CTX232517 im Citrix Support Knowledge Center.

Wo erhalte ich Hilfe zu Citrix Analytics?

Im Diskussionsforum von Citrix Analytics unter https://discussions.citrix.com/forum/1710-citrix-analytics/ können Sie Fragen stellen und sich mit Experten von Citrix Analytics in Verbindung setzen.

Um am Forum teilzunehmen, müssen Sie sich mit Ihrer Citrix ID anmelden.

Zugangssicherung —Geolocation

Wie werden Geolokalisierungsdetails von Analytics abgeleitet?

Citrix Analytics verwendet die IP-Adresse des Geräts, von dem aus der Workspace Client gestartet wird. Citrix Analytics nutzt einen Drittanbieter für IP-Geolokalisierungsdaten, um den Standort eines Benutzers aus seiner IP-Adresse abzuleiten. Wenn Sie eine Sitzungsanmeldung durchführen, wird Ihr Standort (IPv4-Adresse) in ein Land oder eine Stadt aufgelöst, und die Zuordnung wird regelmäßig aktualisiert. Unternehmen können diese nach Ländern definierten Standorte verwenden, um Zugriffsmuster zu überwachen, von denen aus sie keine Geschäfte tätigen.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Wie hoch ist die Genauigkeit bei der Ableitung des Standorts eines Benutzers?

Citrix Analytics nutzt einen Drittanbieter für IP-Geolokalisierungsdaten, um den Standort eines Benutzers aus seiner IP-Adresse abzuleiten. GeoIP-Dienste können die meiste Zeit in der richtigen Stadt oder am richtigen Ort aufgelöst werden, GeoIP-Suchen sind jedoch nie vollständig korrekt. Manchmal kann sich der für einen Benutzer angezeigte Standort von seinem genauen Standort des Zugriffs unterscheiden.

Basierend auf der Dokumentation von IP GeoPointliegt der Abdeckungsgrad bei etwa 99,99% der weltweit zugewiesenen IP-Adressen (IPv4-routingfähige IP-Adressen). In Bezug auf die Standortgenauigkeit begleitet es jedes der wesentlichen Standortfelder (Land, Bundesland, Stadt, Postleitzahl) mit einem Konfidenzfaktor.

In welchen Fällen ist die Standortbestimmung ungenau?

Die Genauigkeit der Geolokalisierungsdaten hängt davon ab, wie das Gerät eine Verbindung zum Internet herstellt. Ein Gerät kann eine Verbindung zum Internet herstellen über:

- Mobile Gateways
- VPN oder Hosting-Einrichtung
- Regionaler oder internationaler Proxy-/Anonymisierserver

In solchen Fällen sind Geolokalisierungsdaten unabhängig von der Verwendung der Software des IP-Geolocation-Anbieters nicht genau.

Was sind die unterstützten Versionen der Citrix Workspace-App?

Es gibt Mindestversionen der Citrix Workspace-App, die für das Betriebssystem erforderlich sind, um das **IP-Adressattribut** an Citrix Analytics for Security zu senden. Weitere Informationen finden Sie in der Matrixtabelle oder in den als nicht verfügbar identifizierten Standorten .

In welchen Fällen erhalten wir keine geologischen Details?

Einzelheiten zur Geolocation finden Sie im Abschnitt Als nicht verfügbar identifizierte Standorte .

Welchen Geolocation-Dienst verwendet Citrix Analytics, um den Standort eines Benutzers zu melden? Wie melde ich einen falschen Standort für eine IP?

Citrix Analytics verwendet dateibasierte Geolocation-Dienste von Neustar, um Geolokalisierungsdaten für eingehende Zugriffe bereitzustellen. Es verfügt über eine öffentlich zugängliche IP-Korrekturseite, auf der Sie eine Korrekturanforderung selbst einreichen können. Sobald ein

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Korrekturantrag eingereicht wurde, wird der Antrag von Neustar auf Richtigkeit geprüft und bearbeitet.

Der GeoIP-Anbieter hilft dabei, so genaue Informationen wie möglich anzuzeigen. Leider kann es Fälle geben, in denen die GeoIP-Daten aufgrund der angeborenen Natur von GeoIP ungenau sind.

Glossar der Begriffe

April 12, 2024

- **Aktionen**: Geschlossene Reaktionen auf verdächtige Ereignisse. Es werden Maßnahmen angewendet, um zukünftige anomale Ereignisse zu verhindern. Weitere Informationen.
- **Cloud Access Security Broker (CASB)**: Lokaler oder Cloud-basierter Durchsetzungspunkt für Sicherheitsrichtlinien zwischen Cloud-Dienstnutzern und Cloud-Dienstanbietern. CASBs kombinieren und integrieren Sicherheitsrichtlinien des Unternehmens, wenn auf Cloud-basierte Ressourcen zugegriffen wird. Sie helfen Unternehmen auch dabei, die Sicherheitskontrollen ihrer on-premises Infrastruktur auf die Cloud auszudehnen.
- **Citrix ADC (Application Delivery Controller)**: Netzwerkgerät, das sich in einem Rechenzentrum befindet, das sich strategisch zwischen der Firewall und einem oder mehreren Anwendungsservern befindet. Behandelt den Lastausgleich zwischen Servern und optimiert die Endbenutzerleistung und Sicherheit für Unternehmensanwendungen. Weitere Informationen
- **Citrix ADM (Application Delivery Management)**: Zentralisierte Netzwerkverwaltungs-, Analyse- und Orchestrierungslösung. Von einer einzigen Plattform aus können Administratoren Netzwerkdienste für skalierbare Anwendungsarchitekturen anzeigen, automatisieren und verwalten. Weitere Informationen
- **Citrix ADM Agent**: Proxy, der die Kommunikation zwischen Citrix ADM und den verwalteten Instanzen in einem Rechenzentrum ermöglicht. Weitere Informationen
- **Citrix Analytics**: Cloud-Dienst, der Daten über Dienste und Produkte hinweg (on-premises und in der Cloud) sammelt und umsetzbare Erkenntnisse generiert, sodass Administratoren proaktiv mit Sicherheitsbedrohungen von Benutzern und Anwendungen umgehen, die App-Leistung verbessern und den kontinuierlichen Betrieb unterstützen können. Weitere Informationen
- **Citrix Cloud**: Plattform, die über den Citrix Cloud Connector in jeder Cloud oder Infrastruktur (on-premises, Public Cloud, Private Cloud oder Hybrid Cloud) eine Verbindung zu Ressourcen herstellt. Weitere Informationen
- **NetScaler Gateway**: Konsolidierte RAS-Lösung, die die RAS-Infrastruktur konsolidiert, um Single Sign-On für alle Anwendungen zu ermöglichen, ob in einem Rechenzentrum, in der Cloud oder als SaaS bereitgestellt. Erfahren Sie mehr.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Citrix Hypervisor**: Virtualisierungsverwaltungsplattform, optimiert für Anwendungs-, Desktop- und Servervirtualisierungsinfrastrukturen. Weitere Informationen
- **Citrix Workspace App** (früher bekannt als Citrix Receiver): Clientsoftware, die nahtlosen, sicheren Zugriff auf Anwendungen, Desktops und Daten von jedem Gerät, einschließlich Smartphones, Tablets, PCs und Macs, bietet. Weitere Informationen
- **DLP (Data Loss Prevention)**: Lösung, die eine Reihe von Technologien und Prüfmethoden beschreibt, um in einem Objekt enthaltene Informationen wie Datei, E-Mail, Paket, Anwendung oder Datenspeicher zu klassifizieren. Das Objekt kann sich auch im Speicher, in Verwendung oder über ein Netzwerk befinden. DLP-Tools können Richtlinien wie Protokollieren, Berichten, Klassifizieren, Verschieben, Kennzeichnen und Verschlüsseln dynamisch anwenden. DLP-Tools können auch Schutzmaßnahmen zur Verwaltung von Unternehmensdatenrechten anwenden. Weitere Informationen
- **DNS (Domain Name System)**: Netzwerkdienst, der verwendet wird, um Internet-Domänennamen zu finden und sie in Internetprotokolladressen (IP) zu übersetzen. DNS ordnet die von Benutzern bereitgestellten Website-Namen ihren entsprechenden IP-Adressen zu, die von Computern bereitgestellt werden, um eine Website unabhängig vom physischen Standort der Entitäten zu finden.
- **Datenverarbeitung**: Methode zur Verarbeitung von Daten aus einer Datenquelle zu Citrix Analytics. Weitere Informationen
- **Datenquelle**: Produkt oder Dienst, der Daten an Citrix Analytics sendet. Eine Datenquelle kann intern oder extern sein. [Erfahren Sie mehr] /en-us/citrix-analytics/data-sources.html).
- **Datenexport**: Produkt oder Dienst, der Daten von Citrix Analytics empfängt und Erkenntnisse liefert. Weitere Informationen
- **Erkannte Benutzer**: Gesamtzahl der Benutzer in einer Organisation, die Datenquellen verwenden. Weitere Informationen
- **FQDN (vollqualifizierter Domänenname)**: Vollständiger Domänenname für internen (StoreFront) und externen (Citrix ADC) Zugriff.
- **Maschinelles Lernen**: Art der Datenanalysetechnologie, die Wissen extrahiert, ohne explizit dafür programmiert zu werden. Daten aus einer Vielzahl potenzieller Quellen wie Anwendungen, Sensoren, Netzwerken, Geräten und Geräten werden in ein System für maschinelles Lernen eingespeist. Das System verwendet die Daten und wendet Algorithmen an, um eine eigene Logik aufzubauen, um ein Problem zu lösen, Erkenntnisse abzuleiten oder eine Vorhersage zu treffen.
- **Microsoft Graph Security**: Gateway, das Kundensicherheit und Unternehmensdaten miteinander verbindet. Bietet einfach zu überprüfende Warnungen und Behebungsoptionen, wenn eine Maßnahme ergriffen werden muss. Weitere Informationen

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Leistungsanalyse**: Dienst, der Einblick in die Details der Benutzersitzung in einer Organisation bietet. Weitere Informationen
- **Richtlinie**: Eine Reihe von Bedingungen, die erfüllt sein müssen, damit eine Aktion auf das Risikoprofil eines Benutzers angewendet werden kann. Weitere Informationen
- **Risikoindikator**: Kennzahl, die Informationen über das Ausmaß des Risikos des Unternehmens zu einem bestimmten Zeitpunkt liefert. Weitere Informationen
- **Risikobewertung**: Dynamischer Wert, der das aggregierte Risiko angibt, das ein Benutzer oder eine Entität für eine IT-Infrastruktur über einen vorab festgelegten Überwachungszeitraum darstellt. Weitere Informationen
- **Risikozeitplan**: Aufzeichnung des riskanten Verhaltens eines Benutzers oder einer Entität, sodass Administratoren ein Risikoprofil untersuchen und die Datennutzung, Gerätenutzung, Anwendungsnutzung und Standortnutzung verstehen können. Weitere Informationen
- **Riskanter Benutzer**: Benutzer, der riskant gehandelt hat oder riskantes Verhalten gezeigt hat. Weitere Informationen
- **Sicherheitsanalyse**: Erweiterte Analyse von Daten, die verwendet werden, um überzeugende Sicherheitsergebnisse wie Sicherheitsüberwachung und Bedrohungssuche zu erzielen. Weitere Informationen
- **Sicherer privater Zugriff**: Service, der die Integration von Single Sign-On, Remote-Zugriff und Inhaltsüberprüfung in einer einzigen Lösung für die End-to-End-Zugriffskontrolle ermöglicht. Weitere Informationen.
- **Splunk**: SIEM-Software (Security Information and Event Management), die intelligente Daten von Citrix Analytics empfängt und Einblicke in die potenziellen Geschäftsrisiken liefert. Weitere Informationen.
- **UBA (User Behavior Analytics)**: Baselining von Benutzeraktivitäten und -verhalten in Kombination mit Peer-Group-Analysen, um potenzielle Eindringlinge und böswillige Aktivitäten zu erkennen.
- **Watchlist**: Liste der Benutzer oder Entitäten, die Administratoren auf verdächtige Aktivitäten überwachen möchten. Weitere Informationen.

© 2024 Cloud Software Group, Inc. All rights reserved. Cloud Software Group, the Cloud Software Group logo, and other marks appearing herein are property of Cloud Software Group, Inc. and/or one or more of its subsidiaries, and may be registered with the U.S. Patent and Trademark Office and in other countries. All other marks are the property of their respective owner(s).