Centrify Privilege Threat Analytics Service

Kontrollen auf Grundlage maschinellen Lernens für die moderne Gefahrenlandschaft

„Zero Trust Privilege"-Kontrollen müssen sich an den Risikokontext anpassen können. Gartner unterstützt CARTA – Continuous, Adaptive, Risk, and Trust Assessment –, was auch für privilegierten Zugriff unumgänglich ist. „Zero Trust Privilege" bedeutet zu wissen, dass, auch wenn die richtigen Zugriffsdaten von einem privilegierten Benutzer eingegeben wurden, die Anfrage jedoch einen riskanten Kontext enthält, vor Gewährung des Zugriffs eine umfangreichere Prüfung erforderlich ist. Moderne, auf maschinellem Lernen beruhende Algorithmen werden heutzutage dazu verwendet, um das Verhalten eines privilegierten Benutzers sorgfältig zu analysieren und „abnormale" oder „nicht normale" (und damit riskante) Aktivitäten zu erkennen, sodass das für das jeweilige Risiko angemessene Kontrollniveau angewendet werden kann.

Die Gefahrenlandschaft von heute erfordert adaptive Kontrollen

Cyberangriffe werden zunehmend komplexer, weshalb es sich bewährt hat, als Schutz vor Missbrauch privilegierter Zugriffsrechte mehrere Sicherheitsebenen einzurichten. In der Gefahrenlandschaft von heute sind Sicherheitskontrollen erforderlich, die sich an den Risikokontext anpassen und maschinelles Lernen zur sorgfältigen Analyse der Aktivitäten eines privilegierten Benutzers verwenden.

Eine adaptive Kontrolle warnt nicht nur in Echtzeit vor risikobehafteten Aktivitäten – sie ist auch in der Lage, aktiv auf Vorfälle zu reagieren, indem sie Sitzungen beendet, zusätzliche Überwachungsfunktionen aktiviert oder eine Sitzung für eine forensische Nachanalyse markiert.

Maschinelles Lernen bietet Unternehmen die Möglichkeit, Millionen von Ereignissen zu durchsuchen und regelmäßig die Nadel im Heuhaufen zu finden, was mithilfe manueller Forensik nie möglich wäre. Sogar noch ergiebiger ist es, auf maschinellem Lernen basierende Analysen in Echtzeit durchzuführen, um so wirklich adaptive, präventive Kontrollen anstelle einfacher Kontrollen im Nachgang eines Vorfalls zu ermöglichen.

Missbrauch privilegierten Zugangs genau und nahezu in Echtzeit identifizieren

Der Centrify Privilege Threat Analytics Service nutzt fortschrittliche Verhaltensanalysen in Kombination mit den adaptiven Multi-Faktor-Authentifizierungs-Funktionen (MFA) von Centrify Zero Trust Privilege, um eine zusätzliche Schutzschicht hinzuzufügen, und wendet eine adaptive MFA für abnormales Benutzerverhalten an. Ob Sie den Centrify Privilege Threat Analytics Service nutzen oder nicht, kann darüber entscheiden, ob Sie Opfer eines Sicherheitsverstoßes werden oder diesen bereits in seiner Entstehung aufhalten.

ADAPTIVE MULTI-FAKTOR-AUTHENTIFIZIERUNG

Fügen Sie eine zusätzliche Schutzebene hinzu, um Sicherheitsverletzungen mit einer risikogerechten, adaptiven MFA für IT-Administratoren aufzuhalten, die auf Windows- und Linux-Systeme zugreifen, Berechtigungen erweitern oder privilegierte Zugriffsdaten nutzen.

ANALYSE DES BENUTZERVERHALTENS

Nutzen Sie moderne, auf maschinellem Lernen basierende Algorithmen, um das Verhalten eines privilegierten Benutzers gründlich zu analysieren und um „anormale" oder „nicht normale" und demnach risikoreiche Aktivitäten zu erkennen und die Sicherheitsabteilung zu warnen oder darüber in Kenntnis zu setzen. Die Erkennung riskanter Aktivitäten wird auch bei Entscheidungen bezüglich Echtzeit-Zugangskontrollen eingesetzt, etwa im Rahmen der Authentifizierung oder erweiterten Authentifizierung. Darüber hinaus können Analysen des Verhaltens privilegierter Benutzer dazu verwendet werden, zu verifizieren, welche Privilegien wie oft genutzt werden. Dies kann bei Entscheidungen bezüglich der Änderung von Rollen und Berechtigungen hilfreich sein.

> **„Sobald Sie ein klares Bild der Bandbreite der von den Centrify Zero Trust Privilege Services bereitgestellten Funktionen erhalten, verstehen Sie, wie viele Sicherheitsprobleme Sie damit gleichzeitig lösen. Ich bin immer noch erstaunt über die Anzahl an Problemen, die ich mit einer einzigen Lösung angehen konnte."**
>
> — Matt Horn, IT Operations Manager, GSI

Sicheren Zugriff auf kritische Systeme verstärken

Fügen Sie bei Bedarf – und auf Grundlage der Risikobewertung – eine zusätzliche Schutzschicht hinzu, um die Gefahr kompromittierter privilegierter Zugriffsdaten zu verringern. Konfigurieren Sie eine verhaltensbasierte Zugriffskontrolle für IT-Administratoren, die auf Windows- und Linux-Server zugreifen, Berechtigungen erweitern oder privilegierte Zugriffsdaten nutzen.

- **Erkennen Sie anormales Verhalten, während es vonstatten geht, indem Sie risikogerechte Richtlinien für Benutzer durchsetzen, die eine privilegierte Sitzung starten, ein Passwort auschecken oder ein Privileg erweitern. Die Kombination aus risikogerechten Richtlinien und rollenbasieren Zugriffskontrollen, Benutzerkontext und MFA ermöglicht intelligente, automatisierte Echtzeit-Entscheidungen bei der Gewährung eines privilegierten Zugriffs. Diese dynamisch durchgesetzten Zugriffsrichtlinien gewähren dem Benutzer Zugriff, fordern ihn zur Eingabe eines zweiten Authentifizierungsfaktors auf oder blockieren den Zugriff vollständig.**
- **Die Centrify Zero Trust Privilege Services unterstützen die umfangreichste Bandbreite an Authentifikatoren und bieten so die Flexibilität, Ihre IT-Mitarbeiter mithilfe des am besten geeigneten Formfaktors zu authentifizieren und gleichzeitig Ihre bestehenden MFA-Systeme und -Authentifikatoren zu nutzen. Von Centrify unterstützte Authentifikatoren:**
  - **Mobile Push-Benachrichtigungen,**
  - **Sicherheitsfragen,**
  - **Telefonanruf mit PIN-Verifizierung,**
  - **OATH-Token,**
  - Server mit Einmal-Zugangscode,
  - FIDO-U2F-Sicherheitsschlüssel und
  - Smartcards.
- **Die adaptiven MFA-Funktionen von Centrify arbeiten einwandfrei mit bestehenden Investitionen in RSA, OATH-basierte Token und Smartcards wie PIV/CAC zusammen. Diese können alle zentral von Centrify verwaltet und in Ihrem gesamten Unternehmen durchgesetzt werden.**
- **Die mobile Centrify-App für iOS und Android bietet privilegierten Benutzern eine leicht zu bedienende Schnittstelle, über die sie MFA-Benachrichtigungen oder Workflow-Anforderungen für Genehmigungen erhalten. Zudem bietet die App eine Schnittstelle, über die Benutzer OATH-Token mit vom Centrify Privileged Access Service erstellten Seed- oder Geheimnistresoren verwalten können, um OTP-Codes zu validieren, was bei zahlreichen privilegierten Anwendungen und Diensten erforderlich ist, die ihre eigene OATH-konforme MFA-Validierung wie etwa die AWS® Console durchsetzen. Darüber hinaus unterstützt die mobile App das Aus-/Einchecken von Passwörtern im Notfall.**
- **Centrify unterstützt zudem MFA-Dienste für Netzwerkgeräte wie Router, Switches oder Firewalls, auf denen ein privilegierter Zugriff durch Administratoren erst nach einer vorherigen MFA möglich sein sollte.**

Benutzerverhaltensanalysen zur Verringerung Ihres Sicherheitsrisikos nutzen

In der heutigen Gefahrenlandschaft sind Sicherheitskontrollen erforderlich, die sich dem jeweiligen Risikokontext anpassen und maschinelles Lernen einsetzen, um das Verhalten eines privilegierten Benutzers sorgfältig zu analysieren. Eine adaptive Kontrolle warnt nicht nur in Echtzeit vor risikobehafteten Aktivitäten – sie ist auch in der Lage, aktiv auf Vorfälle zu reagieren, indem sie Sitzungen beendet, zusätzliche Überwachungsfunktionen aktiviert oder eine Sitzung für eine forensische Nachanalyse markiert.

- **Nutzen Sie eine Reihe individuell anpassbarer Dashboards und interaktiver Widgets, um ein besseres Verständnis über die IT-Risiken und Zugriffsmuster in Ihrer Infrastruktur zu erlangen. Dank der Anpassung der Sicherheitsrichtlinien auf das jeweilige Verhalten der einzelnen Benutzer und das automatische Markieren von riskantem Verhalten erhalten Sie unmittelbaren Einblick in das mit einem bestimmten Benutzerkonto verbundene Risiko und sparen sich somit den Aufwand, Millionen von Protokolldateien und riesige Mengen historischer Daten zu durchforsten.**
- **Erhalten Sie ein besseres Verständnis in Bezug auf Zugriffe und Ereignisse durch einen exakten Blick auf Ereignisse, Systeme, Standorte, Zeitpunkte, privilegierte Anweisungen und vieles mehr. IT-Benutzer können sich einzelne Ereignisse genau ansehen, um sich mit den Risikoeigenschaften eines bestimmten Ereignisses vertraut zu machen. Das Risiko wird für jedes Ereignis in Echtzeit berechnet und für jede anormale Aktivität als hoch, mittel oder niedrig eingestuft.**
- **Erhalten Sie einen optimierten Einblick in anormale Aktivitäten dank einer detaillierten Übersicht über die Timeline. Ermitteln Sie die jeweiligen Faktoren, die zu einer Anomalie beigetragen haben, um so ein umfassendes Verständnis einer potenziellen Gefährdung zu erlangen – und das alles von einer einzigen Konsole aus. Sicherheitsteams können sich den Systemzugriff und die erkannten Anomalien mithilfe von Analysetools wie Dashboards, Explorer View und Recherchetools in hoher Auflösung ansehen.**
- **Privilegierte Zugriffsdaten werden erfasst und gespeichert, um eine solide Abfrage mithilfe von Protokollmanagement-Tools und der Integration von externen Berichterstattungs-Tools zu ermöglichen. Dank der optimierten Integration von SIEM-Tools wie Micro Focus® ArcSight™, IBM® QRadar™ und Splunk® werden Risiken oder verdächtige Aktivitäten schnell erkannt.**
- **Nutzen Sie sämtliche Webhook-fähigen Anwendungen (z. B. Slack® oder bestehende On-Board-Ereignisabwehrsysteme wie PagerDuty®), um die Ausgabe von Warnmeldungen in Echtzeit zu ermöglichen, was den Bedarf an mehreren Touchpoints für Warnmeldungen beseitigt und so die Reaktionszeit verkürzt. Bei Eintritt eines Alarmereignisses bietet der Centrify Privilege Threat Analytics Service dem Benutzer die Möglichkeit, Warnmeldungen über Webhook mühelos in Anwendungen von Drittanbietern abzusetzen. Dank dieser Funktion kann der Benutzer auf einen Bedrohungsalarm reagieren und die Auswirkungen eindämmen.**
- **Erhalten Sie spezifische und detaillierte Informationen zu verdächtigen Aktivitäten auf privilegierten Konten. IT-Administratoren können direkt über den Warnbildschirm unmittelbare Gegenmaßnahmen ergreifen, um potenzielle Risiken oder einen laufenden Angriff abzuwehren, und eine Sitzung auf Grundlage des jeweiligen Risikos manuell oder automatisch beenden.**
- **Mittels des Centrify Privilege Threat Analytics Service analysierte Ereignisse werden dazu verwendet, normale Verhaltensmuster für einen Benutzer bei jeder Anmeldung oder privilegierten Aktivität, einschließlich Befehlen, zu charakterisieren, sodass Anomalien in Echtzeit identifiziert werden können und eine risikobasierte Zugriffskontrolle ermöglicht wird. Hochrisikoereignisse werden sofort markiert, und die IT-Abteilung wird über diese in Form von Warnmeldungen und Benachrichtigungen unmittelbar informiert. So wird die Analysezeit verkürzt und der Aufwand der Risikobewertung in den hybriden IT-Umgebungen von heute erheblich verringert.**

Unsere Mission besteht darin, die Hauptursache für Sicherheitsverletzungen – den Missbrauch privilegierter Zugriffsrechte – zu stoppen. Centrify ermöglicht es seinen Kunden mit einem Cloud-fähigen „Zero Trust Privilege"-Ansatz, den Zugang zu Infrastruktur, DevOps, Cloud, Containern, Big Data und anderen Angriffsflächen in modernen Unternehmen zu sichern. Weitere Informationen erhalten Sie unter www.centrify.com.

Hauptsitz (USA) +1 (669) 444 5200
Europa, Naher Osten und Afrika (EMEA)
+44 (0) 1344 317950
Asien/Pazifik +61 1300 795 789
Brasilien +55 11 3958 4876
Lateinamerika +1 305 900 5354
sales@centrify.com

Centrify®

www.centrify.com