DATENBLATT

One Identity Safeguard for Privileged Analytics

Erkennen und verhindern Sie Sicherheitsverstöße im Zusammenhang mit privilegiertem Zugriff

Vorteile

- Bietet durch Nachverfolgen und Visualisieren der Benutzeraktivität Einblicke in die Vorgänge in Ihrem IT-System
- Ständige Authentifizierung durch ständige Analyse der Dynamik der Tastendrücke und Mausbewegungen
- Ermittlung von ungewöhnlichen Abweichungen der Standard-Aktivität durch maschinelles Lernen
- Verkürzung der Zeit bis zur Erkennung eines Sicherheitsfalls mit Kontextinformationen und risikobasierter Priorisierung von aufgezeichneten Sitzungen
- Reduziert das Rauschen von Sicherheitswarnungen, sodass Sie sich auf die wichtigen Dinge konzentrieren können
- Erhöht die Sicherheit durch das Beenden von Verbindungen, wenn vor potenziell bedrohlichen Aktivitäten gewarnt wird

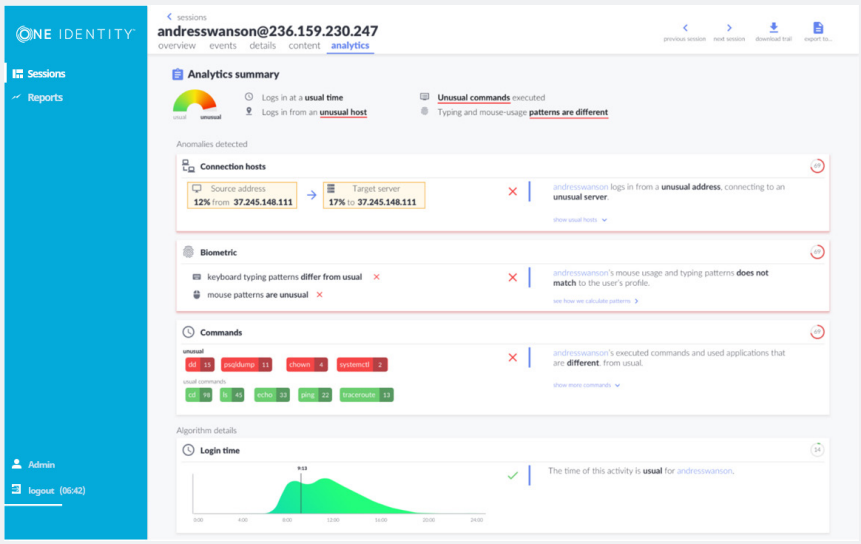
Überblick

Als Verantwortlicher für die IT-Sicherheit wissen Sie natürlich, dass Ihr Unternehmen kaum einer Sicherheitsverletzung über ein privilegiertes Konto entgehen kann. Heute benötigen Organisationen durchschnittlich 206 Tage[1], bis eine Sicherheitsverletzung erkannt wird. Und Zeit ist Geld – und Risiko. Ob die Sicherheitsverletzung also von einem gekaperten privilegierten Konto oder von einem Administrator auf Abwegen ausgeht: Je länger sie unentdeckt bleibt, desto mehr Zeit bleibt den Eindringlingen zum Suchen und Stehlen von Daten und desto höher werden Strafgelder und weitere forensische Kosten.

Wahrscheinlich haben Sie nicht nur Ihren vertrauenswürdigen Administratoren privilegierten Zugang gewährt. Vielleicht haben Sie expandiert und ausgegliederten Administratoren von externen Beratungsunternehmen, die sich an einem beliebigen Ort der Welt befinden könnten, Privilegien gewährt. Wie können Sie nun sicher sein, dass Administratoren mit privilegiertem Zugang diesen zu Ihrem Wohl und nicht zu Ihrem Schaden verwenden?

Mit One Identity Safeguard for Privileged Analytics wissen Sie, wer Ihre mit den meisten Risiken behafteten Benutzer sind, Sie richten Ihr Augenmerk ständig auf neue interne und externe Bedrohungen und können ungewöhnliches Verhalten von privilegierten Konten erkennen. Diese leistungsfähige Lösung verschafft Ihnen einen vollständigen Einblick in das Verhalten und die Aktivitäten Ihrer privilegierten Benutzer, und Sie können beim Auftreten eines Problems sofort aktiv werden und befinden sich in einer guten Position, um einer Verletzung des Datenschutzes zuvorzukommen.

[1] 2017 von Ponemon durchgeführte Studie zu den Kosten von Datenpannen (Cost of Data Breach)



Einfache Bestimmung von risikobehafteten Benutzern und Verhalten

Schnelle Erkennung mithilfe der Analyse-Zusammenfassung, ob die Aktivitäten eines Benutzers ungewöhnlich und potentiell riskant sind. Diese enthält eine Zusammenfassung der ungewöhnlichen Befehle, der biometrischen Aktivität und der Verbindungs-Hosts.

Funktionen und Merkmale

Entdeckung von unbekannten Risiken in Echtzeit

Regelbasierte Sicherheitsfunktionen können weder neue Angriffsmethoden noch böswillige Betriebsangehörige erkennen. Safeguard for Privileged Analytics verfolgt und visualisiert die Aktivitäten von Benutzern in Echtzeit und führt so zu einem besserem Verständnis der Vorgänge in Ihrer IT-Umgebung. Es werden keine vordefinierten Korrelationsregeln benötigt, es funktioniert allein auf der Grundlage der vorhandenen Sitzungsdaten.

Musterfreier Ablauf

Anstatt ein „als bösartig bekanntes" Verhalten mithilfe von Mustererkennung zu ermitteln – was oft versagt – verwendet Safeguard for Privileged Analytics Daten, die in Ihrer IT-Umgebung erfasst wurden. Es wird eine Art Grundwert des normalen Verhaltens erstellt, und dann werden mithilfe verschiedener Techniken des maschinellen Lernens Abweichungen davon ermittelt.

Analyse des Bildschirminhalts

Durch Analyse des Bildschirminhalts von privilegierten Sitzungen und der aufgetretenen Befehle und Fenstertitel kann Safeguard for Privileged Analytics das Profil des Grundverhaltens mit den regelmäßig verwendeten Befehlen und Anwendungen der privilegierten Benutzer anreichern. Diese granulare Analyse erleichtert die Identifizierung von typischem Verhalten und die Erkennung von Diebstählen privilegierter Identitäten.

Verhaltensbiometrie

Jeder Benutzer besitzt ein eigentümliches Verhaltensmuster, sogar beim Ausführen von identischen Aktionen wie Tippen oder Bewegen der Maus. Die in Safeguard for Privileged Analytics eingebauten Algorithmen analysieren diese von Safeguard for Privileged Sessions erfassten Verhaltenscharakteristiken. Die Analyse der Tastendruckdynamik und der Mausbewegung sind nicht nur bei der Erkennung von Sicherheitsverstößen behilflich, sondern dienen auch zur ständigen biometrischen Authentifizierung.

Reduzierung von Warnungsrauschen

Privileged Analytics reduziert das von SIEM-Lösungen (Security Informationen und Event Management) generierte „Warnungsrauschen" durch Kategorisierung von Benutzerereignissen auf der Grundlage von Risiken und Abweichungen und stellt die verdächtigsten Ereignisse heraus. Warnungen können an SIEMs gesendet werden, oder Ihr Sicherheitsanalytiker kann auf der intuitiven Benutzeroberfläche eine priorisierte Liste von Ereignissen einsehen, sodass das Augenmerk auf die wichtigsten Ereignisse gerichtet werden kann.

Automatisierte Reaktion

In den meisten Angriffsszenarien geht Ereignissen mit großen Auswirkungen oft eine Erkundungsphase voraus. Daher ist Erkennung und Reaktion während dieser Phase entscheidend für das Verhindern der schädlichen Aktivität. Die nahtlose Integration mit Safeguard for Privileged Sessions ermöglicht eine automatische Beendigung von Sitzungen beim Auftreten eines hochverdächtigen Ereignisses oder beim Erkennen eines böswilligen Verhaltens.

Der One Identity Ansatz für die privilegierte Zugriffsverwaltung

Das One Identity Portfolio bietet derzeit das branchenweit umfassendste Angebot an Lösungen für die Verwaltung privilegierter Konten. Doch damit nicht genug: Im One Identity Safeguard for Privileged Analytics Softwareportfolio finden Sie auch Lösungen für Sitzungs- und Kennwortverwaltung sowie die präzise Delegierung von UNIX Root-Konten und Active Directory Administratorkonten, Add-Ons für Enterprise-Bereitstellungen des Open Source-Tools sudo und Keylogger für UNIX Root-Aktivitäten. Alle diese Optionen sind eng in unsere branchenführende Active Directory Bridging-Lösung integriert.

Über One Identity

One Identity unterstützt Unternehmen bei der erfolgreichen Umsetzung von Identitäts- und Zugriffsmanagement (IAM). Mit unserem einzigartigen Portfolio an Lösungen für Identity Governance, Zugriffsverwaltung, Verwaltung privilegierter Konten und Identity-as-a-Service-Lösungen können Organisationen ihr volles Potenzial entwickeln, ohne Einschränkung durch Sicherheit, und profitieren dabei vom Schutz vor Bedrohungen. Weitere Informationen finden Sie unter OneIdentity.com.

Datasheet_2019_PAM-Privileged-Analytics_US_RS_41021