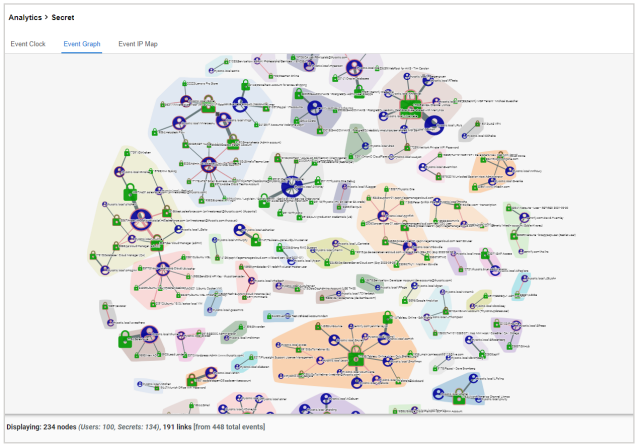
Privileged Behavior Analytics

Sicherheitsverstöße und Datendiebstahl frühzeitig erkennen

Sicherheitsrisiken senken

Wenn Ihr Unternehmen seine Sicherheit verbessert und sein Risiko senkt, spart Ihre Abteilung Zeit, Geld und Ressourcen. Gleichzeitig wird Ihre aktuelle Investition in Secret Server und Privilege Manager noch rentabler.

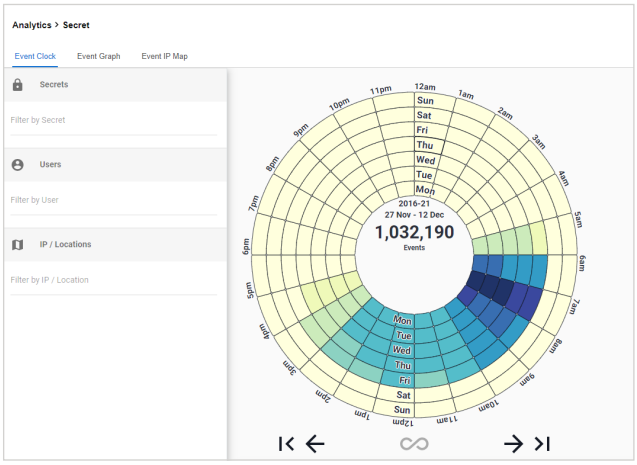
Mit Privileged Behavior Analytics können IT- und Sicherheitsadministratoren Sicherheitsverstöße erkennen, bevor sie stattfinden, unternehmensweit die Vergabe von und den Zugriff auf privilegierte Konten und Zugangsdaten analysieren und eine weitere Sicherheitsebene in Ihre Secret-Server- und Privilege-Manager-Lösung einziehen.



Erkennen früher Anzeichen von Sicherheitsverstößen

Ist ein Zugriff auf ein privilegiertes Konten um 3 Uhr morgens in Ihrem Unternehmen etwas Ungewöhnliches?

Ein plötzlich ungewöhnliches Verhalten eines Nutzers kann ein frühes Anzeichen für eine Datenverletzung oder eine Insider-Bedrohung sein. Privileged Behavior Analytics erkennt dieses anomale Verhalten sofort und meldet Ihrem Sicherheitsteam umgehend einen Cyberangriff oder eine Insider-Bedrohung, noch bevor es zu einer Datenverletzung kommt.



Priorisieren der wichtigsten Warnmeldungen

Wie wissen Sie, auf welche Sicherheitswarnung oder Aktivität Sie als Erstes reagieren sollen?

Maschinelles Lernen und Verhaltensmustererkennung helfen Ihnen, die Aktivitäten in Ihrem System zu priorisieren, indem sie Sie auf besonders dringende Ereignisse hinweisen. Somit wissen Sie sofort, wenn eine verdächtige Aktivität stattfindet und was als Erstes zu tun ist. Sortieren Sie Ihre Warnmeldungen nach Bedrohungsgrad, sodass Sie sich zuerst auf kritische Warnmeldungen konzentrieren können.

Sicherheitsverstöße aufdecken, bevor sie stattfinden

Laut Forrester ereignen sich geschätzte 80 % aller Sicherheitsverletzungen mit privilegierten Konten. Diese Verletzungen werden durch Insider verursacht, die ihren privilegierten Zugriff missbrauchen. Doch nicht nur der Schutz aller privilegierten Konten ist wichtig. Daneben sollten auch Aufzeichnungen und Analysen erstellt werden, welche Person Zugriff auf welches privilegierte Konto hat und wann und wie dieses verwendet wird.

Privileged Behavior Analytics von Delinea hilft Ihnen, einen potenziellen Sicherheitsverstoß zu erkennen, noch bevor er stattgefunden hat. Unsere Cloud-basierte Lösung nutzt maschinelles Lernen, um das Verhalten rund um privilegierte Konten innerhalb von Secret Server, unserer Privileged-Access-Management-Lösung, zu analysieren. Ihr Sicherheitsteam wird umgehend über anormales Verhalten alarmiert – ein frühes Anzeichen für eine Gefährdung oder eine Verletzung der Datensicherheit.

Mit Privileged Behavior Analytics und Secret Server können Sie im Handumdrehen das zeitliche Verhalten Ihrer Nutzer analysieren und so feststellen, ob ungewöhnliche Aktivitäten stattfinden. Ausgestattet mit einer „Secret Access Clock“, ermöglicht Privileged Behavior Analytics Sicherheitsteams, das Zugriffsverhalten rasch zu analysieren. Durch eine Filterfunktion innerhalb dieser Analysetools haben Sie die Möglichkeit, ein spezifisches Secret oder Nutzerverhalten während eines bestimmten Zeitraums anzuzeigen.

Delinea konzentriert sich auf das verwundbarste Angriffsziel: privilegierte Konten. Dank eines mehrschichtigen Sicherheitsmodells, das von den Endpunkten bis zu den Zugangsdaten alle Aspekte des privilegierten Zugriffs umfasst, sind Sie gegen Angriffe optimal gewappnet.

Wer kann auf welche Konten zugreifen?

Privileged Behavior Analytics liefert Ihnen einen schnellen Überblick über Ihre privilegierten Konten und alle Nutzer, die darauf Zugriff haben. Nutzer und Secrets werden zu „Communities“ zusammengefasst, die Mini-Ökosysteme bilden. So ist auf einen Blick ersichtlich, ob ein Secret in einer Personengruppe enthalten ist oder ob Nutzer auf Secrets anderer Abteilungen zugreifen.

Welche Warnmeldungen sind die wichtigsten?

Privileged Behavior Analytics nutzt verhaltensbasierende Werte, die auf Machine-Learning-Algorithmen basieren. Diese berücksichtigen das zeitliche Verhalten, das Zugriffsverhalten, die Wichtigkeit der Zugangsdaten und ähnliches Benutzerverhalten. Sobald ein Nutzer von diesen Basiswerten abweicht, wird ihm vom jeweiligen Algorithmus ein Bedrohungswert zugewiesen. Das System sortiert diese Bedrohungswerte nach ihrer Priorität, sodass Sie sich zuerst den Warnmeldungen widmen können, die für Ihr Unternehmen das höchste Risikopotenzial darstellen.

Delinea

Delinea ist ein führender Anbieter für Privileged-Access-Management-Lösungen (PAM), die nahtlose Sicherheit in das moderne, hybride Unternehmen bringen. Unsere Lösungen helfen Unternehmen, Daten, Geräte, Code und Cloud-Infrastrukturen zu schützen, Risiken zu mindern, Compliance zu gewährleisten und die Sicherheitsverwaltung zu vereinfachen. Delinea beseitigt unnötige Komplexität und ermöglicht effektive Zugriffskontrolle für tausende Kunden weltweit, darunter mehr als die Hälfte aller Fortune-100-Unternehmen. Zu unseren Kunden zählen Kleinunternehmen ebenso wie die weltweit größten Finanzinstitute, Geheimdienste und Unternehmen mit kritischer Infrastruktur. **delinea.com**