KEEPER | Pressemitteilung

Neue Keeper-Sentinel-Integration nimmt den gestiegenen Missbrauch von Identitäten und Privilegien ins Visier

Die SIEM-Integration beschleunigt die Bedrohungserkennung und -reaktion durch Echtzeittransparenz bei Anmeldeaktivitäten und privilegiertem Zugriff.

MÜNCHEN, 24. Oktober 2025 – Keeper Security, ein führender Cybersecurity-Anbieter für Zero-Trust- und Zero-Knowledge Privileged Access Management (PAM)-Software zum Schutz von Passwörtern, Passkeys, privilegierten Konten, Geheimnissen und Remote-Verbindungen, kündigt heute die native Integration mit Microsoft Sentinel an. Die Integration ermöglicht es Unternehmen, auf Anmeldeinformationen basierende Bedrohungen schneller und präziser zu erkennen und darauf zu reagieren, indem Echtzeitdaten von Keeper direkt in die Security Information and Event Management (SIEM)-Lösung Microsoft Sentinel gestreamt werden. Sicherheitsteams erhalten dadurch tiefgehende Einblicke in die Nutzung von Anmeldeinformationen, privilegierte Aktivitäten und potenzielle Bedrohungen – sowohl in kommerziellen wie auch in Azure-Government-Umgebungen.

Anmeldeinformationsbasierte Angriffe sind und bleiben der wichtigste Angriffsvektor in heutigen Unternehmensumgebungen. Laut dem Verizon Data Breach Investigations Report 2025 sind kompromittierte Zugangsdaten weiterhin die Hauptursache für Sicherheitsverletzungen. Um dieses Risiko wirksam zu verringern, benötigen Unternehmen Echtzeiteinblicke darin, wie Passwörter, Geheimnisse und privilegierte Konten genutzt und verwaltet werden.

Die neue Integration steht sowohl kommerziellen Unternehmen als auch Kunden aus dem öffentlichen Sektor als Ein-Klick-Bereitstellung über den Microsoft Sentinel Content Hub zur Verfügung und macht die manuelle Einrichtung oder Eingabe von Workspace-IDs überflüssig. Die Keeper-Sentinel-Integration übernimmt automatisch alle erforderlichen Verbindungseinstellungen, einschließlich sicherer Autorisierung und Datenweiterleitung, sodass Unternehmen schnell und unkompliziert ein Enterprise-taugliches Monitoring privilegierter Zugriffe aktivieren können. Darüber hinaus sorgt diese Integration auch auf nicht-menschlichen Identitäten – wie Dienstkonten und automatisierte Systeme, die häufig über privilegierte Zugriffsrechte verfügen – für die notwendige Transparenz. Durch die Überwachung sowohl menschlicher als auch maschineller Aktivitäten erhalten Organisationen eine umfassende Sicht auf die Nutzung von Anmeldeinformationen, schließen Sicherheitslücken und reduzieren blinde Flecken.

„Mit dieser Integration wird Keeper zu einer Art Echtzeitsignal für Microsoft Sentinel und liefert Sicherheitsteams umsetzbare Informationen darüber, wer wann und wo auf welche Ressourcen zugreift“, sagt Craig Lurey, CTO und Mitgründer von Keeper Security. „Anmeldeinformationsbasierte Angriffe nehmen weiter zu. Wir stellen die Transparenz bereit, die Organisationen benötigen, um schnell zu reagieren und Sicherheitsverletzungen zu verhindern.“

Wesentliche Vorteile:

- **Zentrale Transparenz bei Anmelde- und Zugriffsrisiken:** Übertragung von Keeper-Ereignisdaten in Echtzeit an Microsoft Sentinel zur zentralen Überwachung von Aktivitäten im Kontext von Anmeldeinformationen und privilegierten Zugriffen.
- **Schnellere Bedrohungserkennung und -reaktion:** Automatisierung von Warnmeldungen und Aktionen auf Basis wichtiger Ereignisse wie Passwortänderungen, Richtlinienaktualisierungen und verdächtiger Anmeldeaktivitäten.
- **Vereinfachte Compliance und Audits:** Automatische Protokollierung detaillierter Aktivitäten zur Unterstützung regulatorischer Berichterstattung und interner Prüfungen.
- **Individuelle Dashboards und Regeln:** Nutzung integrierter Analysen und Dashboards oder Anpassung der Erkennungs-Workflows an unternehmensspezifische Richtlinien.
- **Umfassende Kontrolle über menschliche und maschinelle Zugriffe:** Überwachung der Nutzung von Anmeldeinformationen durch sowohl menschliche Benutzer als auch nicht-menschliche Identitäten, einschließlich Dienstkonten und automatisierter Systeme.

Da Identitäten im Mittelpunkt moderner Cyberattacken stehen, sorgt die SIEM-Integration für eine Anmeldeinformationsintelligenz sowie Bedrohungserkennung. Dies hilft Security-Teams, ihre Abwehr zu stärken, schneller zu reagieren und Bedrohungen immer einen Schritt voraus zu sein.

Weitere Informationen finden unter docs.keeper.io oder direkt im Microsoft Sentinel Content Hub.

###

Über Keeper Security:
Keeper Security ist eines der am schnellsten wachsenden Unternehmen für Cybersicherheitssoftware, das Tausende von Organisationen und Millionen von Menschen in über 150 Ländern schützt. Keeper ist ein Pionier der Zero-Knowledge- und Zero-Trust-Sicherheit für jede IT-Umgebung. Das Herzstück, KeeperPAM®, ist eine KI-fähige, Cloud-native Plattform, die alle Benutzer, Geräte und Infrastrukturen vor Cyberangriffen schützt. Keeper wurde für seine Innovationen im Gartner Magic Quadrant für Privileged Access Management (PAM) ausgezeichnet und sichert Passwörter und Passkeys, Infrastrukturgeheimnisse, Remote-Verbindungen und Endpunkte mit rollenbasierten Durchsetzungsrichtlinien, Least-Privilege und Just-in-Time-Zugriff. Erfahren Sie auf KeeperSecurity.com, wie Keeper Ihr Unternehmen vor den heutigen Cyberbedrohungen schützen kann.

Folgen Sie Keeper auf Facebook Instagram LinkedIn X YouTube TikTok

Pressekontakt für Keeper in DACH:
Alexandra Schmidt, +49 170 387 10 64
Thilo Christ, +49 171 622 06 10
keeper@tc-communications.de