KEEPER | Pressemitteilung

Die Integration von Keeper Security in Google Security Operations erweitert die Transparenz von privilegierten Zugriffen

Durch das Streamen von privilegierten Zugriffsaktivitäten in Google Security Operations können Unternehmen Angreifer stoppen, bevor gestohlene Anmeldedaten zu umfassenden Sicherheitsverletzungen führen.

MÜNCHEN, 26. September 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, gibt heute eine neue Integration mit Google Security Operations bekannt. Die Integration überträgt privilegierte Zugriffsaktivitäten aus Keeper in die Google Security Operations-Plattform, die die Erkennung, Verwaltung und Reaktion auf Bedrohungen mit Frontline-Intelligence und KI vereint, um Unternehmen dabei zu helfen, neuen und aufkommenden Risiken immer einen Schritt voraus zu sein.

Da Angreifer zunehmend KI-gestützte Techniken und ausgeklügelte Cyberkampagnen einsetzen, müssen Unternehmen sowohl ihre Transparenz als auch ihre Reaktionsgeschwindigkeit verbessern. Durch die Kombination des Advanced Reporting and Alerts Module (ARAM) von Keeper mit Google Security Operations erhalten Sicherheitsteams in Echtzeit zentralisierte Einblicke in privilegierte Zugriffsaktivitäten in ihren Umgebungen. Ereignisse werden kontinuierlich direkt in Google Security Operations gestreamt, wodurch Sichtbarkeitslücken beseitigt und der Aufwand für manuelle Überwachung reduziert werden. Das Ergebnis ist eine schnellere und präzisere Erkennung und Reaktion auf potenzielle Sicherheitsverletzungen.

„Privilegierter Zugriff sollte niemals ein blinder Fleck sein“, sagte Craig Lurey, CTO und Mitbegründer von Keeper Security. „Durch die Integration unserer Funktionen in Google Security Operations bieten wir Unternehmen eine beispiellose Transparenz und Kontrolle über ihre sensibelsten Konten, wodurch Bedrohungen schneller erkannt und wirksamer abgewehrt werden können.“

Stärken der Cyberabwehr von Unternehmen

- **Echtzeitüberwachung:** Durch kontinuierliches Ereignis-Streaming von Keeper in Google Security Operations werden verdächtige oder nicht autorisierte Aktivitäten sofort erkannt.
- **Betriebliche Effizienz**: Automatisierte Berichterstellung und Warnmeldungen reduzieren manuelle Protokollüberprüfungen, sodass sich IT- und Sicherheitsteams auf strategische Prioritäten konzentrieren können.
- **Einhaltung gesetzlicher Vorschriften**: Umfassende Ereignisprotokollierung und Dokumentation der Zugriffskontrolle unterstützen Audits für die DSGVO-, PCI DSS-, SOC- und ISO-Standards.

- **Proaktiver Schutz**: BreachWatch®-Ereignisdaten können erfasst werden, um offengelegte Anmeldedaten zu identifizieren und Versuche der Kontoübernahme zu verhindern.

Die einheitliche, cloudnative Plattform von KeeperPAM® schützt Passwörter, Passkeys, Geheimnisse und privilegierte Sitzungen in Hybrid- und Multi-Cloud-Umgebungen. Durch den Einsatz von agentenbasierter KI ermöglicht KeeperPAM mit seiner KeeperAI-Funktion die Erkennung und Reaktion auf Bedrohungen in Echtzeit, sodass risikoreiche Sitzungen automatisch beendet und alle Benutzeraktivitäten analysiert und kategorisiert werden. Mit der Durchsetzung von Zugriffsrichtlinien mit geringsten Berechtigungen und der Bereitstellung verwertbarer Informationen aus jedem privilegierten Konto reduziert KeeperPAM das Risiko von Sicherheitsverletzungen und stärkt die Cyber-Resilienz von Unternehmen.

Weitere Informationen darüber, wie KeeperPAM mit Google Security Operations integriert wird, um die Unternehmenssicherheit zu stärken, gibt es unter www.keepersecurity.com.

###

Über Keeper Security:
Keeper Security verändert die Cybersicherheit für Millionen von Einzelpersonen und Tausende von Unternehmen weltweit. Die intuitive Cybersicherheitsplattform von Keeper ist mit einer End-to-End-Verschlüsselung ausgestattet und genießt das Vertrauen von Fortune-100-Unternehmen, um jeden Benutzer auf jedem Gerät und an jedem Standort zu schützen. Unsere patentierte Zero-Trust- und Zero-Knowledge-Lösung für das Privileged Access Management vereint die Verwaltung von Unternehmenspasswörtern, Geheimnissen und Verbindungen mit Zero-Trust-Netzwerkzugriffen und Remote-Browser-Isolation. Durch die Kombination dieser wichtigen Identitäts- und Zugriffsverwaltungskomponenten in einer einzigen cloudbasierten Lösung bietet Keeper beispiellose Transparenz, Sicherheit und Kontrolle und gewährleistet gleichzeitig die Einhaltung von Compliance- und Audit-Anforderungen. Erfahren Sie unter 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