Pressemitteilung

Keeper Security führt ServiceNow-Integration ein, um die Sichtbarkeit und Reaktion auf Cyberangriffe zu verbessern

Die neue Integration schließt die Sichtbarkeitslücke, die bei den meisten modernen Sicherheitsverletzungen ausgenutzt wird, indem Identitäts- und Zugriffswarnungen in Echtzeit direkt in bestehende Sicherheitsworkflows gestreamt werden.

MÜNCHEN, 10. Dezember 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 ServiceNow® IT Service Management (ITSM) und dem Modul Security Incident Response (SIR) bekannt. Die Integration ermöglicht es Unternehmen, Sicherheitswarnungen aus der gesamten Keeper-Plattform sicher direkt in ServiceNow zu übernehmen. Dadurch wird eine schnellere und konsistentere Untersuchung von Vorfällen im Zusammenhang mit Anmeldedaten, Geheimnissen und privilegiertem Zugriff ermöglicht.

Gestohlene Zugangsdaten sind nach wie vor einer der häufigsten Angriffspunkte für Cyberangriffe. Laut dem Verizon Data Breach Investigations Report 2025 sind 60 Prozent aller Cybersicherheitsverletzungen auf menschliches Versagen zurückzuführen, darunter kompromittierte Passwörter und der Missbrauch von Zugangsdaten. Die globale Studie von Keeper unterstreicht die Dringlichkeit des Schutzes der Identitätsebene. 69 Prozent der Unternehmen setzen Privileged Access Management (PAM) ein, um sich vor dem Diebstahl von Anmeldedaten zu schützen.

Viele dieser Bedrohungen gehen von privilegierten und administrativen Aktivitäten aus, die Unternehmen durch Lösungen wie KeeperPAM®, die Cloud-native PAM-Plattform von Keeper, absichern. Die neue ServiceNow-Integration hilft Teams dabei, diese Abwehrmaßnahmen zu operationalisieren, indem sie Identitäts- und Zugriffswarnungen mit hoher Priorität in die Workflows weiterleitet, die sie bereits für das Incident Management nutzen.

„Identitätsbasierte Angriffe werden immer raffinierter, aber die Grundlagen bleiben dieselben. Verteidiger benötigen zuverlässige Signale und sofortigen Kontext, und diese Integration liefert beides“, sagt Craig Lurey, CTO und Mitbegründer von Keeper Security. „Durch die Echtzeit-Übermittlung der privilegierten Zugriffstelemetriedaten von Keeper an ServiceNow können sich Sicherheitsteams auf die Analyse und das Ergreifen von Maßnahmen konzentrieren, anstatt Daten zusammenzufügen. Dies ist eine optimierte, praktische Methode, um die Sichtbarkeit dort zu verbessern, wo es am wichtigsten ist.“

Die Keeper Security ITSM-Anwendung bietet eine geführte Einrichtung und einen sicheren, durch OAuth 2.0 geschützten Webhook zum Empfang von Benachrichtigungen von der Keeper-Plattform. Sicherheitsteams können Aktivitäten wie BreachWatch®-Erkennungen von kompromittierten Passwörtern, Änderungen im Verhalten privilegierter Benutzer und risikoreiche Aktionen im Zusammenhang mit Anmeldedaten, Geheimnissen oder privilegierten Sitzungen operationalisieren. Die Integration wandelt eingehende

Warnmeldungen automatisch in SIR-Tickets mit vollständigen Kontextdetails um, sodass Analysten mit größerer Genauigkeit und weniger manuellen Schritten eine Einschätzung machen und Untersuchungen durchführen können.

Zu den wichtigsten Funktionen gehören:

- **Sichere Webhook-Erfassung**: Endpunktschutz mit OAuth 2.0 stellt sicher, dass Warnmeldungen nur von autorisierten Keeper-Systemen akzeptiert werden.

- **Automatisierte Erstellung von Vorfällen**: Eingehende Warnmeldungen werden SIR-Datensätzen zugeordnet, wodurch die manuelle Erstellung von Tickets entfällt und die Reaktionszeit verkürzt wird.

- **Benutzerdefinierte Prioritätenzuordnung**: Administratoren können Schweregrade, basierend auf dem Alarmtyp, zuweisen und so Keeper-Ereignisse mit bestehenden Reaktionsprozessen abstimmen.

- **Geführte Einrichtung und Token-Verwaltung**: Administratoren können die Verbindung konfigurieren und Authentifizierungstoken verwalten, ohne dass eine benutzerdefinierte Entwicklung erforderlich ist.

- **Umfassender Alarmkontext**: Alarm-Payloads enthalten detaillierte Metadaten, um eine effiziente Untersuchung zu unterstützen.

- **Zero-Knowledge-Sicherheitsarchitektur**: Keeper kann nicht auf Kundendaten zugreifen oder diese entschlüsseln, wodurch ein Höchstmaß an Datenschutz und Sicherheit gewährleistet ist.

„Angreifer warten nicht, daher sollten auch Unternehmen nicht auf kritische Signale warten, die einen Angriff stoppen können, bevor Schaden entsteht“, sagt Darren Guccione, CEO und Mitbegründer von Keeper Security. „Indem wir die privilegierten Zugriffsinformationen von Keeper in Echtzeit direkt in ServiceNow einbinden, bieten wir Unternehmen einen schnelleren Weg zur Erkennung und Reaktion auf der Identitätsebene, wo die meisten Angriffe beginnen.“

Da Unternehmen mit einer zunehmend verteilten Infrastruktur und einer Zunahme von Angriffen auf Zugangsdaten zu kämpfen haben, ist eine konsistente Sichtbarkeit über Identitäts- und privilegierte Zugriffstools hinweg unerlässlich. Die Integration von Keeper in ServiceNow schließt eine bestehende Lücke in der Überwachung und stärkt die Fähigkeit eines Unternehmens, identitätsbezogene Vorfälle schnell zu erkennen, zu untersuchen und zu beheben.

Die Integration ist ab sofort im ServiceNow Store verfügbar, zusammen mit einer vollständigen Dokumentation für die Bereitstellung.

###

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