Pressemitteilung

Keeper Security bringt Agent Kit auf den Markt, um KI-gestützte Entwickler-Workflows abzusichern

Die neue Integration ermöglicht es KI-Coding-Agenten, Geheimnisse sicher abzurufen und Infrastruktur zu verwalten, ohne Zugangsdaten im Chatverlauf oder in der Versionsverwaltung offenzulegen

MÜNCHEN, 30. April 2026 – Keeper Security, führender Anbieter einer Zero-Trust- und Zero-Knowledge-Plattform für Identity Security sowie Privileged Access Management (PAM), hat heute die Einführung des Keeper Agent Kit bekannt gegeben. Das neue Kit aus spezialisierten KI-Funktionen integriert Keeper Secrets Manager und Keeper Commander direkt mit führenden KI-Coding-Agenten wie Claude Code, Cursor, Codex und GitHub Copilot, um komplexe Sicherheits- und Administrationsprozesse sicher zu automatisieren.

Da Unternehmen zunehmend agentenbasierte KI in ihre Entwicklungsprozesse integrieren, entsteht eine kritische Sicherheitslücke: privilegierte Zugangsdaten können in der Prompt-Historie von KI-Systemen offengelegt werden. Bisher mussten Entwickler API-Schlüssel oder Datenbankzugänge oft manuell in Chat-Oberflächen eingeben, wodurch sensible Daten unbeabsichtigt in Drittanbieter-Logs oder Trainingsdaten gespeichert werden konnten. Das Keeper Agent Kit soll dieses Risiko beseitigen, indem KI-Agenten direkt mit den abgesicherten CLI-Werkzeugen Keeper Commander und Keeper Secrets Manager CLI arbeiten.

„Das Keeper Agent Kit schafft einen klaren Rahmen dafür, wie KI-Agenten mit sensiblen Unternehmensdaten interagieren“, sagte Craig Lurey, CTO und Mitgründer von Keeper Security. „Indem die Agenten unsere lokal verschlüsselten CLI-Tools nutzen, führen sie Befehle innerhalb der authentifizierten Sitzung des Entwicklers aus. So bleibt unser Zero-Knowledge-Standard gewahrt, während Entwickler die Geschwindigkeit von KI nutzen können.“

Das Keeper Agent Kit ist auf moderne Entwickler-Workflows ausgelegt und bietet unter anderem:

- **Sicheren Abruf von Geheimnissen:** Zugangsdaten werden lokal eingebunden, ohne im Chat-Interface sichtbar zu werden.
- **Automatisierte Vault-Administration:** Nutzer, Teams und Audit-Ressourcen können über Keeper Commander verwaltet werden.
- **Vereinfachte Einrichtung:** Sicherheitswerkzeuge lassen sich automatisiert konfigurieren, um neue Projekte von Beginn an abzusichern.

Für Teams in gehosteten oder orchestrierten KI-Umgebungen bietet Keeper zudem eine Integration über einen Model Context Protocol (MCP)-Server, verfügbar für Docker- und Node-Umgebungen. Dadurch können Agenten Geheimnisse über einen laufenden MCP-Server statt über lokale CLI-Tools abrufen. Alle Aktionen der KI-Agenten unterliegen dabei denselben rollenbasierten Zugriffsrechten und Audit-Protokollen wie menschliche Nutzer.

„Sicherheitsteams sollten nicht zwischen Geschwindigkeit und Betriebssicherheit wählen müssen“, sagte Jeremy London, Director of Engineering, AI and Threat Analytics bei Keeper Security. „Mit dem Agent Kit machen wir KI von einem reinen Assistenten zu einem sicheren Partner, der die Sicherheitsgrenzen eines Unternehmens respektiert.“

Das Keeper Agent Kit ist ab sofort als Open-Source-Projekt unter der Apache-2.0-Lizenz verfügbar. Entwickler können es über das offizielle GitHub-Repository von Keeper Security beziehen.

###

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-unterstützte, 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.

Erfahren Sie mehr unter KeeperSecurity.com
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