Pressemitteilung

Keeper Security führt native Jira-Integrationen ein, um die Reaktion auf Sicherheitsvorfälle und die Governance für privilegierten Zugriff zu vereinheitlichen

Neue Jira-Integrationen verbinden Sicherheitswarnungen, Zugriffsanfragen und Genehmigungen in einem einzigen, geregelten Workflow, während die Umsetzung zentral in Keeper erfolgt.

MÜNCHEN, 4. März 2026 – Keeper Security, eine führende Plattform für Zero-Trust- und Zero-Knowledge-Identitätssicherheit sowie Privileged-Access-Management (PAM), gibt heute zwei neue native Integrationen für Atlassian Jira bekannt. Die Integrationen mit der weit verbreiteten Software für Issue- und Projekt-Tracking betten die Reaktion auf Sicherheitsvorfälle sowie die Governance privilegierter Zugriffe direkt in bestehende Jira-Workflows ein, während die Umsetzung der Zugriffsrechte weiterhin zentral in Keeper gesteuert wird.

Jira spielt eine zentrale Rolle dabei, wie Unternehmen Sicherheitsvorfälle, operative Anfragen und Änderungsprozesse verwalten. Sicherheitswarnungen werden in Jira erfasst und priorisiert, Behebungsmaßnahmen zugewiesen und Genehmigungen als Teil des Workflows dokumentiert. Dennoch bleiben in vielen Umgebungen Incident Response und die Durchsetzung der Zugriffsrechte voneinander getrennt und basieren auf manuellen Übergaben, E-Mail-Genehmigungen oder Ad-hoc-Prozessen, die Risiken und Verzögerungen verursachen. Die Jira-Integrationen von Keeper schließen diese Lücke, indem sie die Sicherheitserkennung, Reaktion und Zugriffsverwaltung in einem einzigen Workflow vereinen und gleichzeitig die Durchsetzung, Verschlüsselung und Audit-Kontrollen zentral innerhalb der Keeper-Plattform halten.

Die Integrationen bestehen aus zwei auf Forge basierenden Anwendungen, die unterschiedliche, sich jedoch ergänzende Funktionen erfüllen. Die Jira-ITSM-Integration verarbeitet Sicherheitsereignisse und -vorfälle, während die Jira-Workflow-Integration steuert, wie Zugriffe im Zusammenhang mit diesen Ereignissen oder allgemeinen betrieblichen Anforderungen beantragt und gewährt werden. Gemeinsam verbinden sie Erkennung, Reaktion und Zugriffsdurchsetzung in Jira, wobei Keeper weiterhin als führendes System („System of Record“) für Sicherheitskontrollen fungiert. Die Jira-Workflow-Integration nutzt den Commander Service Mode von Keeper und stellt sicher, dass kryptografische Operationen innerhalb der Kundenumgebung verbleiben, wodurch das Zero-Knowledge-Sicherheitsmodell von Keeper gewahrt bleibt.

„Sicherheitsteams untersuchen Vorfälle nicht nur in Jira, sondern koordinieren dort auch die erforderlichen Zugriffsänderungen zu deren Behebung“, sagt Craig Lurey, CTO und Mitgründer von Keeper Security. „Diese branchenweit erste Integration erweitert Genehmigungen für privilegierte Zugriffe und entsprechende Workflows auf die Tools, die Sicherheits- und IT-Teams täglich nutzen. So ist gleichzeitig sichergestellt, dass strenge Verschlüsselungskontrollen weiterhin bestehen bleiben.“

Mit der Jira-ITSM-Integration können von Keeper generierte Sicherheitswarnungen automatisch als Jira-Vorgänge erstellt werden. So ist gewährleistet, dass Vorfälle ohne manuelle Ticketerstellung erfasst, priorisiert und nachverfolgt werden. Jeder Vorgang enthält den vollständigen Ereigniskontext sowie strukturierte Alarmdaten, sodass die Teams die Auswirkungen bewerten und umgehend mit der Behebung beginnen können.

So können zugriffsbezogene Maßnahmen, die zur Behebung eines Vorfalls oder einer operativen Anfrage erforderlich sind, direkt aus Jira über die Jira-Workflow-Integration initiiert werden. Teams können im Rahmen desselben Workflows, mit dem der Vorfall oder die Aufgabe verwaltet wird, Zugriff auf Keeper-Vault-Ressourcen, gemeinsame Ordner, Servicekonten oder geschützte Systeme beantragen. Die Integration unterstützt zudem Genehmigungen im Endpoint Privilege Manager, sodass Administratoren Anfragen zum Ausbau von Privilegien direkt in Jira prüfen und bearbeiten können.

Zugriffsanfragen unterstützen konfigurierbare Ablaufzeiträume, wodurch ein zeitlich begrenzter Zugriff ohne dauerhafte Berechtigungen ermöglicht wird. Die gesamte Zugriffsdurchsetzung, kryptografische Kontrolle und Sitzungsprotokollierung verbleibt in Keeper, sodass Jira als Workflow-Oberfläche fungiert und nicht als Sicherheitsgrenze.

Dieser einheitliche Ansatz ermöglicht es Unternehmen:

- Unsichere Nebenkanäle wie E-Mail-Genehmigungen oder Screenshots zu eliminieren
- Incident Response und Zugriffsbehebung in einem einzigen „System of Record“ zusammenzuführen
- Least-Privilege-Zugriff konsistent über Cloud-, Hybrid- und On-Prem-Umgebungen hinweg durchzusetzen
- Vollständige Audit-Trails über Warnmeldungen, Genehmigungen und Zugriffsereignisse hinweg aufrechtzuerhalten

Die Jira-Integrationen unterstützen sowohl teams- als auch unternehmensverwaltete Jira-Projekte und basieren auf der Atlassian-Forge-Plattform für Jira-Cloud-Umgebungen. Flexible Feldzuordnungen ermöglichen es Unternehmen, Keeper-Alarmdaten und Zugriffs-Workflows an bestehende Jira-Konfigurationen, Vorgangstypen und Prioritäten anzupassen.

Durch die Einbettung der Zugriffsverwaltung in Jira-Workflows ermöglicht Keeper es Unternehmen, ihre Sicherheitsabläufe zu modernisieren und gleichzeitig die für Compliance, Audit und Risikomanagement erforderliche Zero-Trust- und Zero-Knowledge-Architektur beizubehalten – und das ganz ohne die Zugriffsdurchsetzung zu dezentralisieren,

„Diese Integrationen spiegeln Keepers übergreifende Plattformstrategie wider“, ergänzt Lurey. „Die Sicherheits-Workflows sollten sich daran anpassen, wie Teams üblicherweise arbeiten – die Durchsetzung darf jedoch niemals fragmentiert sein. In Jira werden Entscheidungen getroffen. In Keeper wird der Zugriff kontrolliert.“

Keeper bietet ein umfangreiches Set an Integrationen, mit denen Unternehmen ihre Sicherheits- und Identitäts-Workflows vereinheitlichen und stärken sowie den manuellen Aufwand reduzieren können. Keeper lässt sich mit Identitätsanbietern und Single-Sign-On-(SSO)-Systemen verbinden und unterstützt die automatisierte Benutzerbereitstellung über

SCIM-Tools (System for Cross-domain Identity Management), wodurch das On- und Offboarding reibungsloser und sicherer gestaltet werden kann.

Darüber hinaus integriert sich Keeper mit Security-Information- and Event-Management-(SIEM)-Lösungen, um Echtzeitdaten zu Anmeldeinformationen und Zugriffsaktivitäten in umfassende Sicherheitsüberwachungs- und Compliance-Dashboards einzuspeisen. Für Geschäftskunden optimieren diese Integrationen die Authentifizierung, verbessern die Bedrohungserkennung und Compliance, erhöhen die Transparenz bei Zugriffsaktivitäten und steigern die betriebliche Effizienz, indem Keeper in bestehende Enterprise-Tools und -Workflows eingebunden wird.

Keepers neue Jira Integrationen sind ab sofort verfügbar. Mehr Informationen unter KeeperSecurity.com.

###

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.

Erfahren Sie mehr unter KeeperSecurity.com
Folgen Keeper: 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