

Exeon.UEBA für SAP

Hochskalierbare und datenschutzkonforme Analyse von Nutzerverhalten und Entitäten

„Moderne Angreifer brechen nicht mehr ein – sie loggen sich ein.“

Gestohlene Zugangsdaten und missbräuchlich genutzte SAP-Berechtigungen sind heute der zentrale Angriffspfad in SAP-Systeme. Klassische SAP-Überwachung basiert auf statischer, regelbasierter Logik – und übersieht oft Verhaltensanomalien.

Exeon.UEBA erkennt **verdächtiges Verhalten über SAP-Identitäten, Transaktionen, Tabellen und Mandanten hinweg** – in Echtzeit und mit vollständiger Datenhoheit.

Ihre Vorteile mit Exeon.UEBA für SAP



Zentrale Sicht über SAP-Identitäten hinweg

Überwachung von SAP-Benutzern, Admins, Dienstkonten und Schnittstellen, On-Prem oder in der Cloud.



Flexible Anbindung von SAP-Umgebungen

Schnelle Einbindung von SAP Security Audit Logs (SALs) und umgebende Systemlogs durch smarte Log-Modellierung.



Reduktion von Daten und Kosten

Intelligentes Datenhandling reduziert das SAP-Logvolumen und verbessert dabei die Erkennungseffizienz.



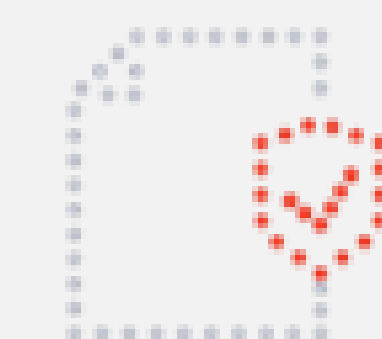
Echtzeit-Datenverarbeitung zur sofortigen Erkennung

Stream-basierte Analysen erkennen verdächtiges SAP-Verhalten sofort – auch bei Milliarden von Datenpunkten.



Duale Detektion: SAP-Expertenwissen + KI

Vorkonfigurierte SAP-Detektionsregeln kombiniert mit KI-Verhaltensanalyse decken Anomalien und Insider-Bedrohungen auf.



Hoher Datenschutz und volle Datensouveränität

Pseudonymisierung von Anwenderdaten mit On-Prem Bereitstellung gewährleisten DSGVO-konforme Analysen.

Trusted by

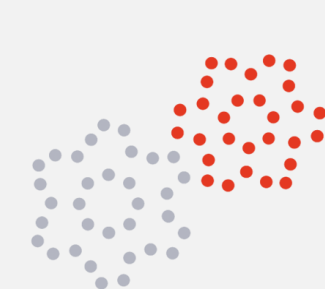
Wieso **jetzt** reagieren



Kompromittierte Konten

Missbrauch von Zugangsdaten war auch im Jahr 2025 die häufigste Sicherheitsverletzung.

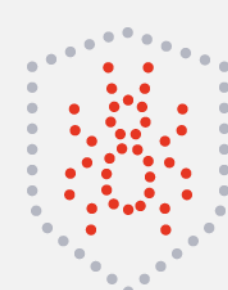
Source: Verizon DBIR 2025



KI-gesteuertes Social Engineering

72% der Unternehmen berichten von steigenden Cyberrisiken durch KI-Angriffe.

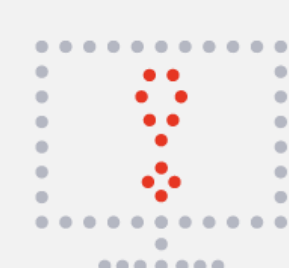
Source: SoSafe Cybercrime Trends 2025



Auswirkungen von Ransomware

78% der Organisationen waren von Ransomware betroffen.

Source: CrowdStrike State of Ransomware 2025



Risiken in der Lieferkette

Angriffe über Drittanbieter nehmen weiterhin stark zu.

Source: Verizon DBIR 2025

Exeon.UEBA für SAP **in Aktion**

Ungewöhnliche SAP-Aktivitäten

Problem: Gestohlene Zugangsdaten werden für legitime SAP-Aktivitäten genutzt.

UEBA-Funktionalität:

- Überwacht Zugriffe, Aktionen und Berechtigungen
- Lernt das Verhalten pro Benutzer und über die gesamte Umgebung hinweg

Ergebnis:

- Markiert erstmalige kritische Transaktionen
- Alarme bei Verhaltensauffälligkeit von Identitäten

Nutzen: Erkennung von Zugangsdaten-Missbrauch.

Änderungen von Privilegien

Problem: Erweiterungen von Privilegien und kritische Änderungen bleiben oft unbemerkt.

UEBA-Funktionalität:

- Überwacht Änderungen an Benutzern, Rollen und Passwörtern
- Verfolgt Transaktionen und Debugger-Nutzung

Ergebnis:

- Warnmeldungen bei privilegierten Änderungen
- Erkennt verdächtige Konfig-Manipulationen

Nutzen: Unterbindet Angriffsaktivität in SAP.

Zugriff auf sensible Daten

Problem: Die Datenexfiltration über den legitimen SAP-Zugriff fällt nicht auf.

UEBA-Funktionalität:

- Überwacht sensible Tabellen und Zugriffe darauf
- Korreliert Datenexport mit Benutzerverhalten

Ergebnis:

- Meldet ungewöhnliche HR-, Finanz- oder Passwort-Tabellenzugriffe
- Erkennt abnormale Exportmuster

Nutzen: Risikoreduktion von Datendiebstahl aus SAP.

Sichere & konforme Überwachung

Problem: Regulierte Branchen benötigen eine SAP-Überwachung, ohne gegen DSGVO zu verstossen.

UEBA-Funktionalität:

- On-prem oder Air-gapped Betrieb
- Pseudonymisierung und Verschlüsselung von personenbezogenen Daten

Ergebnis:

- Datenschutzkonforme SAP-Überwachung
- Keine Identitätsdaten gehen in eine externe Cloud

Nutzen: Ermöglicht souveräne SAP-Sicherheit.

Sie möchten **Exeon.UEBA** für SAP testen?