Exeon.AgentGuard

Verhaltensbasierte Bedrohungserkennung für Interaktionen mit KI.

KI-Agenten erhalten Zugriff schneller, als Sicherheitsteams Visibilität gewinnen.

KI-Assistenten und autonome Agenten können auf Unternehmensdaten zugreifen, Tools aufrufen und mit regulär erteilten Berechtigungen handeln.

Exeon.AgentGuard analysiert Interaktionen mit KI, **um mögliche Datenabflüsse aufzuzeigen und riskantes Agentenverhalten zu erkennen**.

Ihre Vorteile mit Exeon.AgentGuard

Die Aktivitäten aller KI-Agenten im Überblick

Erfahren Sie, welche Modelle, Tools und Ressourcen die KI-Agenten nutzen. Durch kompakte Zusammenfassungen und alle relevanten Informationen zu den Konten.

Agentenaktivitäten in Echtzeit nachvollziehen

Sehen Sie sich Agenten- und Nutzeraktivitäten wie Anweisungen, Tool-Calls und Datenflüsse im Detail an, um möglichen Sicherheitsrisiken auf den Grund zu gehen.

Datenabfluss durch KI-Agenten erkennen

Identifizieren Sie sensible Informationen in ausgehenden KI-Prompts und Dateien. Prüfen Sie externe Übertragungsziele und auffällige Datenmengen.

Gefährliches Agentenverhalten aufdecken

Erkennen Sie KI-Agenten, die vom erwarteten Verhalten abweichen oder mit legitimen Berechtigungen sicherheitskritische Aktionen ausführen.

Auf uns vertrauen

PostFinance · SWISS · cargolux · LGT · Schweizerische Eidgenossenschaft Confédération suisse Confederazione Svizzera Confederaziun svizra · KLINIKUM DO

Warum jetzt handeln

KI-Agenten überschreiten ihre Grenzen

53 % der befragten Unternehmen geben an, dass KI-Agenten gelegentlich ihre vorgesehenen Berechtigungen überschreiten.

Quelle: Cloud Security Alliance, April 2026

Sensible Daten in Gefahr

Bei **60 %** der Sicherheitsvorfälle im Zusammenhang mit KI werden vertrauliche Informationen kompromittiert.

Quelle: IBM, CDBR, Juli 2025

KI-Governance hinkt hinterher

63 % der von Datenpannen betroffenen Unternehmen hatten keine KI-Governance-Richtlinie oder entwickelten diese noch.

Quelle: IBM, CDBR, Juli 2025

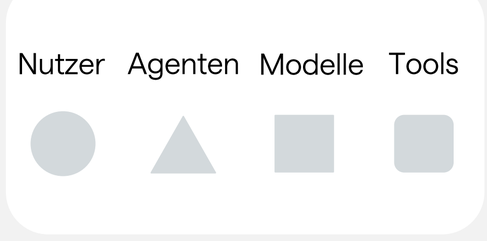
Agentenaktivitäten sind kaum nachvollziehbar

Nur **12 %** der Befragten können die Aktionen jedes Agenten durchgängig nachverfolgen – von den ersten Anweisungen über Tools und APIs bis zum Ergebnis.

Quelle: Salt Security, Oktober 2026

So funktioniert Exeon.AgentGuard

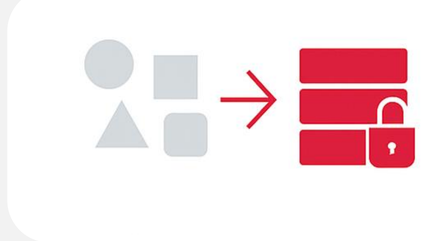
KI-Interaktionen



- Erfassen Sie Prompts, Dateien und Anweisungen über Ihren Web-Proxy (ICAP) oder über Ihre KI-Gateways

- KI-Prompts und Tool-Calls
- Aktivitäten angebundener Tools

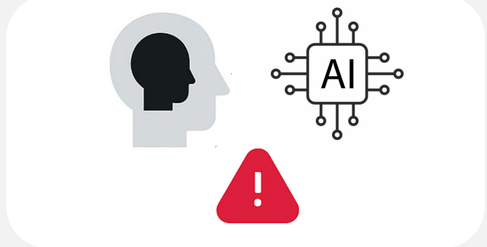
Lokale Datenaufbereitung



- Lokale Verarbeitung und Pseudonymisierung
- Deduplizierung und einheitliche Datenmodellierung

- Weniger Datenduplikate
- Vertrauliche Kontextinformationen bleiben in Ihrer internen IT-Umgebung

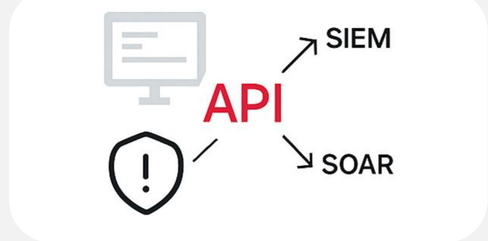
Risiken erkennen



- Individuell anpassbare Sigma-Regeln
- Analyse typischer Verhaltensmuster in Tools und Ressourcen

- Bekannte Richtlinienrisiken
- Aussagekräftige Abweichungen

Warnmeldungen gezielt untersuchen



- KI-Aktivitäten durchsuchen
- Den kompletten Ablauf einsehen
- Konkrete Hinweise prüfen

- Warnmeldungen nachvollziehen
- Risiken fundiert einschätzen

Interesse an Exeon.AgentGuard?

Exeon Analytics AG
exeon.ai
+41 44 500 77 21
contact@exeon.com

CYBERSECURITY MADE IN EUROPE™