Sekoia

AI-SOC-PLATTFORM | SEKOIA DEFEND

Mehr Transparenz und Kontrolle für Ihre Security Operations

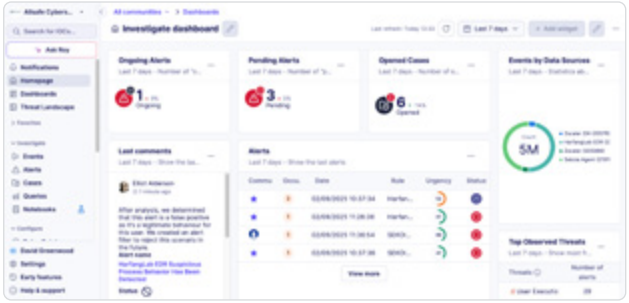
Sekoia Defend bietet Security-Teams einen zentralen Überblick, intelligente Erkennung und KI-gestützte Reaktionsprozesse für Cloud- und On-Premises-Umgebungen.

Warum Sekoia Defend?

Unternehmen setzen eine Vielzahl unterschiedlicher Tools ein. Sind diese nicht miteinander verknüpft, fehlen wichtige Zusammenhänge zwischen sicherheitsrelevanten Ereignissen. Das verzögert eine schnelle Reaktion, da Analysten Warnmeldungen häufig ohne den notwendigen Kontext bewerten müssen.

GENAU HIER SETZT SEKOIA DEFEND AN.

Die Plattform vereint Threat Intelligence, Erkennung, Untersuchung und Reaktion in einer zentralen SaaS-Lösung und wurde speziell für die Anforderungen moderner Security Operations Center (SOC) entwickelt.



Kernfunktionen

- **Einheitliche SaaS-Plattform:** Zentrale Oberfläche für SIEM-, SOAR- und XDR-Funktionen.
- **CTI im Mittelpunkt:** Cyber Threat Intelligence bildet die Grundlage der Plattform.
- **Offen und erweiterbar:** Mehr als 300 sofort nutzbare Integrationen sowie Unterstützung für individuelle Konnektoren.
- **Schneller produktiver Einsatz:** Bereitstellung innerhalb weniger Stunden statt Monate. Der Sekoia Agent, Threat Intelligence und verifizierte Erkennungsregeln sorgen von Beginn an für umfassende Abdeckung.
- **Transparente Preisgestaltung:** Planbare Modelle auf Basis von Assets oder Datenvolumen.

So funktioniert's

ÜBERWACHEN

Vollständige Transparenz über die gesamte Infrastruktur – in der Cloud und On-Premises.

ERKENNEN

Mit CTI angereicherte Regeln sowie Anomalie- und Verhaltensanalysen erkennen Bedrohungen, die anderen Lösungen entgehen.

UNTERSUCHEN

KI-gestütztes Case Management gruppiert Warnmeldungen automatisch und stellt den relevanten Kontext bereit.

REAGIEREN

Manuelle und automatisierte Reaktionsmaßnahmen werden durch KI und vorkonfigurierte Playbooks unterstützt und effizient umgesetzt.

Vorteile auf einen Blick

JEDE DATENQUELLE. JEDE UMGEBUNG.

Der Sekoia Agent erfasst Daten aus Cloud-Services, On-Premises-Systemen und Endgeräten. Individuelle Integrationen lassen sich über eine geführte Oberfläche erstellen - ohne Vendor-Lock-in.

CTI ALS GRUNDLAGE

Die Threat Intelligence von Sekoia ergänzt jede Warnmeldung um relevanten Kontext. So lassen sich Sicherheitsvorfälle schneller und fundierter bewerten.

SKALIERBARE ECHTZEITERKENNUNG

Tausende kuratierte Sigma-Regeln decken aktuelle Taktiken, Techniken und Verfahren (TTPs) ab. Regeln lassen sich einfach anpassen oder erweitern – ohne proprietäre Syntax.

COMPLIANCE ALS BASIS

Regionsspezifische Datenhaltung ermöglicht die Speicherung von Daten gemäß lokalen regulatorischen Anforderungen. Die Plattform gewährleistet vollständige Datenhoheit und Transparenz sowie auditfähige Protokollierung und Kontrollmechanismen – auch für anspruchsvolle Compliance-Anforderungen.

KI-ASSISTENT ROY

ROY unterstützt Analysten bei der Erstellung von Erkennungsregeln, der Priorisierung von Warnmeldungen und der Reaktion auf Bedrohungen. Grundlage sind bewährte Security-Best-Practices. ROY entlastet insbesondere Junior-Analysten und unterstützt gleichzeitig erfahrene SOC-Teams.

KI-GESTÜTZTES INCIDENT MANAGEMENT

Sekoia korreliert Warnmeldungen automatisch zu Sicherheitsvorfällen und schafft einen vollständigen Lageüberblick. Vorkonfigurierte Playbooks unterstützen die Reaktion und verkürzen die Zeit bis zur Behebung.

Produktvergleich

	Core	Advanced	Prime
Datenerfassung (inkl. Endpoint Agent)	✓	✓	✓
Asset discovery	✓	✓	✓
30 Tage Hot Storage	✓	✓	✓
Verifizierte Erkennungsregeln	✓	✓	✓
CTI-angereicherte Warnmeldungen	✓	✓	✓
Cloud SOAR	✓	✓	✓
KI-Assistent (ROY)	✓	✓	✓
Rollenbasierte Zugriffskontrolle		✓	✓
Individuelle IoC-Sammlungen		500 000	5 Millionen
On-Premises SOAR		✓	✓
Mehrere Communities verwalten			✓
KI-gestütztes Incident Management			✓
Zugriff auf Intelligence Prime*	Optional	Optional	✓ ab 3.000 Assets

*Mehr Informationen enthält das Datenblatt zu Sekoia Intelligence.

FORRESTER®

“[Sekoia] wurde im Bericht The Security Analytics Platform Landscape 2024 als bedeutender Anbieter ausgezeichnet.”

Security Analytics Platform Landscape 2024

Gartner

“[Sekoia] treibt Innovationen mit erweiterten Funktionen für Erkennung und Reaktion voran und nutzt dabei Generative KI, ITDR sowie präventive Sicherheitsmechanismen.”

Techscape for Detection and Response Startups 2024

DE-Sekoia-One-Pager-Defend

Weitere Informationen unter sekoia.com

Bereit für ein modernes SOC?

Sekoia × DAGMA IT SECURITY

Sekoia Defend bietet eine leistungsfähige Plattform für moderne Security Operations Center. Sicherheitsvorfälle lassen sich schneller erkennen, analysieren und bearbeiten.

DEMO ANFORDERN