Sekoia

AI SOC PLATFORM I SEKOIA DEFEND

Elevate your security operations

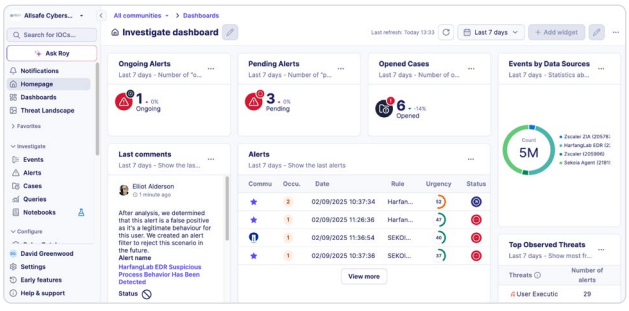
Sekoia Defend empowers security teams with unified visibility, intelligent detection, and fast, AI-guided response across cloud and on-prem environments.

Why Sekoia Defend?

Organizations rely on various tools. But these siloed setups aren't effective. When teams juggle disconnected tools, attackers can easily exploit the gap, and it takes more time to respond. This leaves analysts chasing alerts without the context they need to act.

SEKOIA DEFEND CHANGES THAT.

It brings together threat intelligence, detection, investigation, and response in one easy-to-use SaaS platform. And it's purpose-built for modern SOCs.



Key highlights

- **Unified SaaS platform:** A single interface for SIEM, SOAR, and XDR functions.
- **CTI first**: Built using threat intelligence at its heart
- **Open and extensible:** 300+ out-of-the-box integrations, plus support for custom connectors.
- **Fast time-to-value:** Deploy in hours, not months, with immediate coverage using our agent, threat intel, and verified detection rules.
- **Transparent pricing:** Predictable plans based on assets or data volume.

How it works

MONITOR

Complete visibility across your infrastructure, whether it's cloud or on-prem.

DETECT

CTI-enriched, anomaly-based, and behavioral rules catch threats others miss.

INVESTIGATE

AI-powered case management automatically groups alerts and surfaces relevant context.

RESPOND

Launch manual or automated response actions at scale, guided by AI and pre-built playbooks.

Benefits at a glance

ANY DATA, ANY SOURCE

Ingest from cloud services, on-prem systems, and endpoints with the Sekoia Agent. Create custom integrations with our guided interface, no vendor lock-in needed.

CTI AT THE CORE

Powered by Sekoia's elite threat intel team, the platform enriches every alert with actionable context, so analysts can respond faster and smarter.

REAL-TIME DETECTION, AT SCALE

Access thousands of curated Sigma-based rules covering the latest TTPs. Customize or extend with ease, no proprietary syntax required.

COMPLIANCE-READY BY DESIGN

Region-specific data residency allows you to choose where your data is stored to meet local regulations. The platform ensures full data ownership and visibility, with audit-ready logging and controls designed to support even the most demanding regulatory requirements.

YOUR SECURITY CO-PILOT: ROY

Our AI assistant, trained on security best practices, helps analysts write detection rules, triage alerts, and respond to threats. ROY boosts junior analyst productivity and augments seasoned teams.

AI-GUIDED INCIDENT MANAGEMENT

Sekoia automatically correlates alerts into incidents, providing full situational awareness. Execute response playbooks and cut time-to-resolution.

Plan comparison

	Core	Advanced	Prime
Data ingestion (incl. endpoint agent)	✓	✓	✓
Asset discovery	✓	✓	✓
30-days hot storage	✓	✓	✓
Verified detection rules	✓	✓	✓
CTI-enriched alerts	✓	✓	✓
Cloud SOAR	✓	✓	✓
AI assistant (ROY)	✓	✓	✓
Role-based access control		✓	✓
Custom IoC collections		500k	5m
On-prem SOAR		✓	✓
Manage multiple communities			✓
AI incident management			✓
Intelligence prime access*	Optional	Optional	✓ from 3k assets

*See the Sekoia Intelligence datasheet for full information.

FORRESTER®

"[Sekoia named] a notable vendor in The Security AnalyticsPlatform Landscape"

Security Analytics Platform Landscape 2024

Gartner

"[Sekoia] are innovating with advanced detection and remediation capabilities, leveraging generative AI, ITDR, and preemptive security."

Techscape for Detection and Response Startups 2025

Discover the full picture at sekoia.com

Ready to modernize your SOC?

Sekoia Defend offers a faster, smarter way to secure your organization.

GET A DEMO