SentinelOne

Combine Alerts and Telemetry to Enrich Response Actions

SentinelOne & Sekoia.io Joint Solution Brief

Market Challenges

In the ever-evolving landscape of cybersecurity, organizations are continually seeking innovative solutions to enhance their network and data security of their on-prem / cloud / hybrid infrastructures. The proliferation of cybersecurity tools that work in silos makes it difficult for operational teams to be effective, requiring them to constantly navigate between the consoles of these tools.

The integration of SentinelOne EDR with Sekoia offers a compelling solution to solve this problem by centralizing security management within Sekoia. The Sekoia SOC platform federates your security stack and provides you with a unique control tower to manage your security operations, from detection to response.

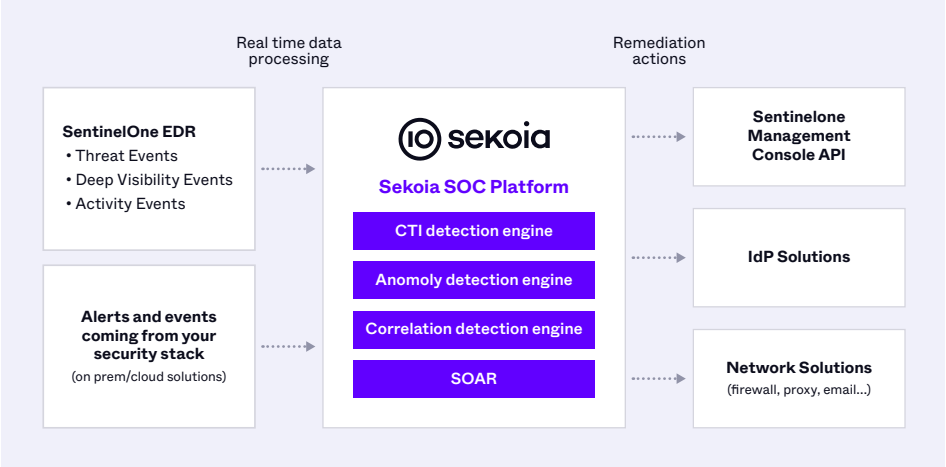
Joint Solution

Sekoia is a user-centric, intelligence-led SOC platform, enabling extensive real-time detection and response. We understand the many challenges faced by SOC teams: protecting complex IT environments, juggling various tools and administration consoles, sorting through a multitude of alerts, recruiting qualified personnel, all while complying with increasingly stringent regulations.

Sekoia effectively solves these challenges with a plug-and-play platform with 750+ detection rules verified by CTI analysts, for instant security of your cloud & on-premises ecosystem. With 160+ integrations, Sekoia's open architecture and flexible APIs make integrating easy.

The integration between Sekoia and SentinelOne EDR allows you to retrieve threat, activity and telemetry events in the Sekoia SOC platform, correlate and enrich them with other sources of information and remediate to alerts and incidents from the Sekoia SOC platform using SentinelOne EDR capabilities.

How It Works



sekoia

Joint Solution Highlights

- Centralize SentinelOne alerts and telemetry within the Sekoia real-time detection pipeline
- Combine multiple levels of threat detection from Sekoia and SentinelOne
- Leverage the SentinelOne response capabilities within complex playbooks

> "The seamless integration of SentinelOne EDR within the Sekoia SOC platform allows our customers to multiply the potential of a component of their security stack. Sekoia SOC platform adds several levels of threat detection based on SentinelOne telemetry and leverages the EDR response capabilities within hybrid playbooks.

Georges Bossert
CTO, SEKOIA.IO

Solution Use Cases

Alerts And Telemetry In One Real-Time Detection Pipeline

The SentinelOne EDR alerts and telemetry are consumed in real time by the Sekoia SOC platform:

- Data is automatically normalized and enriched with Sekoia observables database (60M+)
- Sekoia detection engines are combined to detect threats within SentinelOne
- CTI detection engine relies on the exclusive Sekoia CTI database (6M+ of IoC) to find the traces related to the attackers activities
- 750+ built-in SIGMA rules natively feed the Sekoia detection engines to detect attackers TTPs
- Anomaly detection engine uses ML to catch suspicious behaviors
- Correlation detection engine is able to cross low signals coming from different log sources
- Specific Sekoia detection rules related to SentinelOne guarantee a full visibility of all SentinelOne alerts within the Sekoia SOC platform

Automated Retrohunt

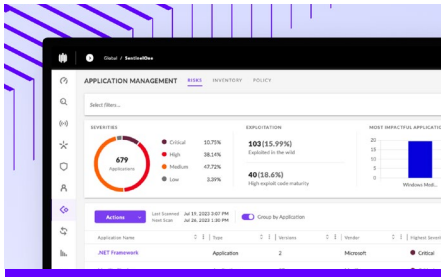
When a new IoC is added to the Sekoia CTI database, the SOC platform will automatically search for this indicator in your logs, including historical data. This feature, combined with very strict IoC lifecycle management, ensures powerful automated retrohunt capabilities, with very few false positives. Necessary remediation actions can be taken retrospectively based on SentinelOne telemetry and other ingested log sources.

Using SentinelOne Response Capabilities Within Playbooks

Sekoia excels in orchestration and incident response through its centralized platform. Its automation capabilities enable swift and consistent responses to streamline incident management by enhancing operational efficiency through its playbooks. Together, Sekoia and SentinelOne further empowers security teams to seamlessly orchestrate and control security tools across the entire IT landscape.

Integration Benefits

+ Modernize your security operations through a threat intelligence driven SOC platform
+ Enhance your analysts productivity with a unique console to manage all your security operations
+ Leverage your existing security stack by utilizing 160+ built-in third party integrations
+ Ingest and correlate SentinelOne telemetry



Ready for a Demo?

Visit the SentinelOne website for more details, or give us a call at +1-855-868-3733

sentinelone.com

Innovative. Trusted. Recognized.

Gartner

A Leader in the 2023 Magic Quadrant for Endpoint Protection Platforms

MITRE ENGENUITY

Record Breaking ATT&CK Evaluation

+ 100% Protection. 100% Detection
+ Outstanding Analytic Coverage, 4 Years Running
+ 100% Real-time with Zero Delays

Gartner Peer Insights

96% of Gartner Peer Insights™

EDR Reviewers Recommend SentinelOne Singularity

FedRAMP · TEVORA PCI DSS Attestation HIPAA Attestation · AICPA SOC · STAR LEVEL ONE · VB100 VIRUS · SE Labs BEST Innovator WINNER 2021 · AAA · Trusted Cloud Provider CSA

About SentinelOne

SentinelOne is the world's most advanced cybersecurity platform. The SentinelOne Singularity™ Platform detects, prevents, and responds to cyber-attacks at machine speed, empowering organizations to secure endpoints, cloud workloads, containers, identities, and mobile and network-connected devices with intelligence, speed, accuracy, and simplicity. Over 11,500 customers—including Fortune 10, Fortune 500, and Global 2000 companies, as well as prominent governments—all trust SentinelOne to Secure Tomorrow.

About Sekoia.io

Sekoia.io is a European cybersecurity company whose mission is to develop the best protection capabilities against cyber-attacks. Its intelligence-led operational security SaaS platform acts as a true control tower for effective, real-time detection and response to cyber threats. Sekoia.io believes that effective protection must enable customers to fully utilize their existing technologies.

sentinelone.com

sales@sentinelone.com
+1 855 868 3733

© SentinelOne 2024