

SOLUTION BRIEF

Nucleon EDR and Sekoia

Where Zero Trust-powered EDR meets the autonomous agentic SOC.

The challenge

Security teams face growing endpoint threat surfaces while working across fragmented tools. When EDR alerts are isolated from broader detection and response workflows, investigations take longer and critical context is missed.

Organizations need integrated endpoint and SOC capabilities that bridge prevention, detection, and response without adding operational complexity.

Nucleon EDR's integration with Sekoia Defend brings Zero Trust endpoint protection and AI-driven detection together in a unified workflow.

By forwarding endpoint system and network telemetry from Nucleon EDR to Sekoia Defend, the integration enables enriched correlation, advanced detection logic, and automated response, helping SOC teams act faster (and with greater confidence).

Key benefits

FAST AND SIMPLE DEPLOYMENT

Enable syslog export in the Nucleon EDR Console, configure the Sekoia intake, and start streaming endpoint events in minutes.

ADVANCED THREAT DETECTION

Combine Nucleon's Zero Trust telemetry and AI-detected threats with Sekoia's CTI-powered detection rules to enhance coverage and eliminate endpoint blind spots.

UNIFIED ENDPOINT VISIBILITY

Nucleon endpoint events flow seamlessly into Sekoia's single pane of glass, enriched with threat intelligence and correlated with broader security signals across your entire environment.

AUTOMATED INCIDENT RESPONSE

Harness Sekoia playbooks to trigger containment actions (including endpoint isolation, process termination, and forensic data collection) directly from the incident console.

Key features



SECURE SYSLOG TELEMETRY FORWARDING

Nucleon EDR exports system and network events (process executions, file access, network connections) via secure syslog (TLS/RFC5424) to Sekoia's intake, for both on-premises and cloud deployments.



DATA NORMALIZATION AND CTI ENRICHMENT

Sekoia parses incoming Nucleon events, enriches them with cyber threat intelligence, and applies detection rules for contextualized alerting and streamlined investigation.



INTEGRATED DETECTION AND AUTOMATED RESPONSE

Correlated alerts inside Sekoia Defend can trigger automated playbooks, enabling response actions such as endpoint isolation or forensic data collection, directly linked to Nucleon EDR capabilities.

How it works

Nucleon EDR (Cloud/On-Prem) exports endpoint telemetry (process executions, network events, file reads and writes) via secure syslog (TLS) using the RFC5424 format. Events are tagged with the Sekoia Intake Key and forwarded directly to Sekoia Intake.

Within Sekoia Defend, events are parsed, normalized, enriched with CTI, and processed through detection rules. Correlated alerts are escalated with full context, enabling analysts to investigate incidents and initiate automated response actions through integrated Sekoia playbooks.

```
Nucleon EDR System & Network Events Sekoia
Intake Sekoia Defend
(Cloud/On-Prem)
→ (JSON via Syslog TLS)
→ (Intake Key)
→ Parse / Enrich / Detect / Respond
```

Use case

Nucleon EDR detects an unknown process executing on an endpoint, flagged by its AI engine as a potential ransomware variant. The alert and associated telemetry are immediately forwarded to Sekoia Defend via secure syslog. Sekoia enriches the event with CTI indicators and correlates it with lateral movement signals detected across the environment, escalating a high-priority alert to the SOC analyst. From the Sekoia console, the analyst initiates endpoint isolation and a memory dump. Containment is achieved within minutes of the initial detection, with full investigation context readily available.

ABOUT NUCLEON SECURITY

Nucleon Security delivers the first Zero Trust-based Endpoint Detection & Response platform, enhanced by advanced AI for malware detection and analysis. Nucleon EDR provides deep visibility and total control over endpoint environments, combining prevention, detection, response, and remediation in a single lightweight agent. Its sector-specific AI models and Zero Trust enforcement block advanced attack techniques while simplifying incident investigation through a centralized console.

ABOUT SEKOIA

Sekoia is the European cybersecurity company building the Cyber Operations Platform for the AI era. Unifying threat detection and response, cyber threat intelligence, exposure management, and agentic AI, Sekoia is rebuilding cybersecurity from the ground up. Through the Autonomous SOC, machines investigate at scale while security teams govern operations with clarity and control. Fully open and agnostic by design, the platform empowers organizations to achieve true strategic and tech autonomy. From SMEs supported by MSSPs to Fortune 2000 enterprises, Sekoia makes advanced defense accessible to all.

Discover the full picture at sekoia.com



One platform. Total control.

And 320+ integrations to choose from

CONTACT US