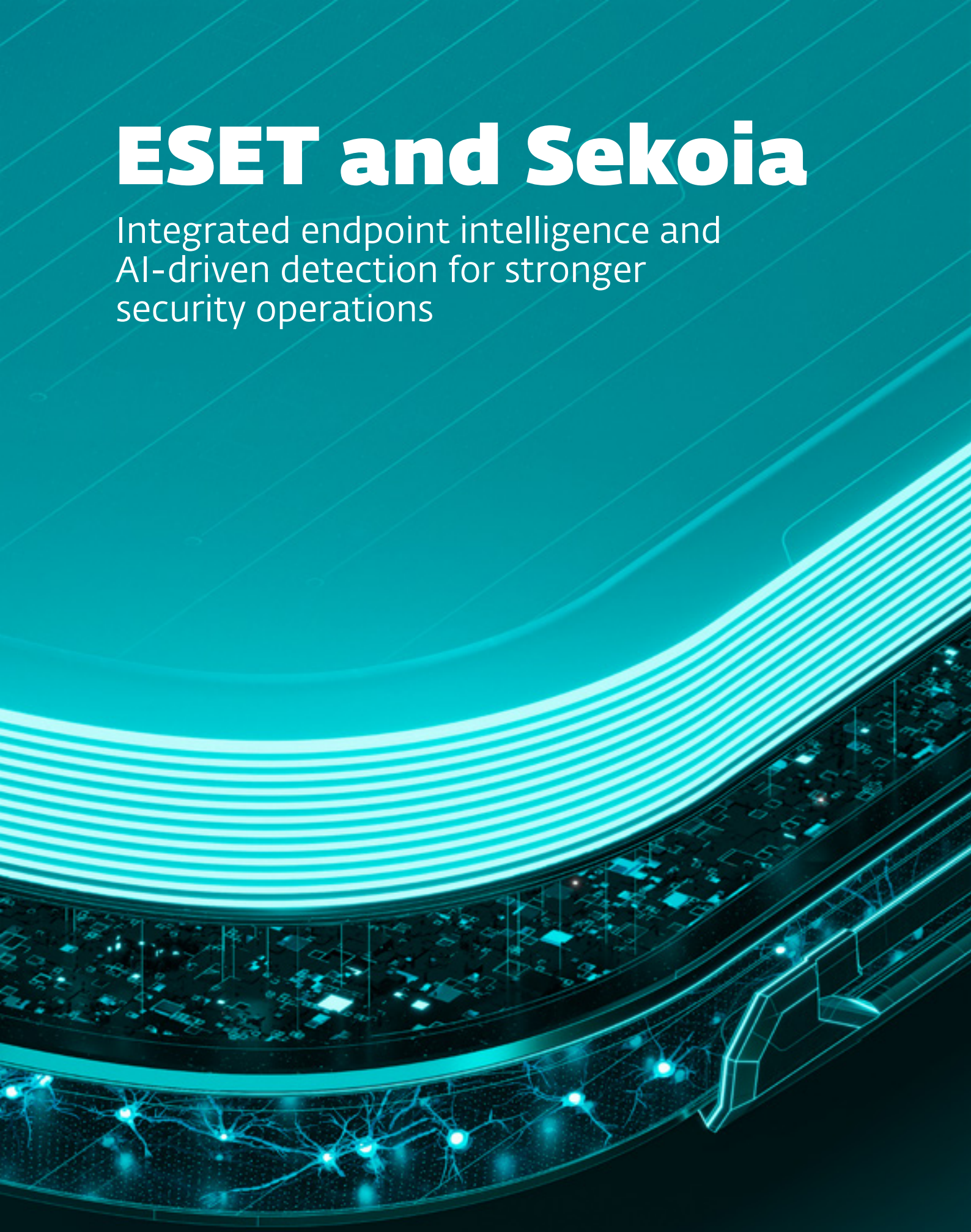
ESET and Sekoia

Integrated endpoint intelligence and AI-driven detection for stronger security operations



Cybersecurity
Progress. Protected.

SOLUTION BRIEF

Enriched endpoint telemetry and automated response for faster incident resolution

Security teams face growing pressure to detect and contain threats quickly while working across multiple tools and data sources. When endpoint alerts are isolated from broader detection and response workflows, investigations take longer and critical context can be missed. Organizations need integrated security operations that enhance visibility without increasing complexity.

ESET PROTECT's integration with Sekoia Defend brings endpoint protection and AI-driven detection together in a coordinated workflow. By forwarding endpoint telemetry and alerts from ESET PROTECT to Sekoia Defend, the integration enables enriched correlation, advanced detection logic, and automated response actions. This synergy helps SOC teams resolve incidents faster and more efficiently.

KEY BENEFITS

FAST DEPLOYMENT

Enable syslog export in ESET PROTECT, configure Sekoia intake, and get up and running in minutes.

ADVANCED DETECTION CAPABILITIES

Combine ESET endpoint telemetry with Sekoia's CTI-powered Sigma rules to enhance threat coverage and detection depth.

UNIFIED VISIBILITY

Endpoint events from ESET flow seamlessly into Sekoia's single pane of glass, enriched with contextual data and correlated alerts across all environments.

AUTOMATED RESPONSE WORKFLOWS

Leverage Sekoia playbooks to isolate devices, trigger scans, and remediate threats using ESET PROTECT APIs directly from the incident console.

KEY FEATURES

SECURE SYSLOG TELEMETRY FORWARDING

ESET PROTECT exports JSON events—including Threat, HIPS, Firewall, and Audit logs—via secure syslog (TLS) to Sekoia intake.

INTEGRATED DETECTION AND SOAR ACTIONS

Correlated alerts inside Sekoia Defend can trigger automated playbooks that initiate response actions in ESET PROTECT, such as host isolation or on-demand scanning.

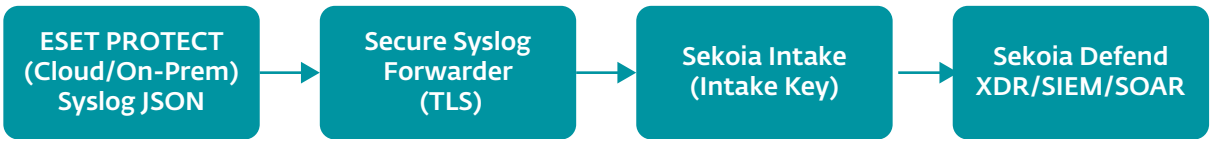
DATA NORMALIZATION AND CTI ENRICHMENT

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

HOW IT WORKS

ESET PROTECT (Cloud or On-Prem) exports endpoint telemetry in JSON format via secure syslog (TLS). Events are sent to a configured forwarder, which includes the Sekoia Intake Key and securely forwards data 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 playbooks and ESET PROTECT APIs.

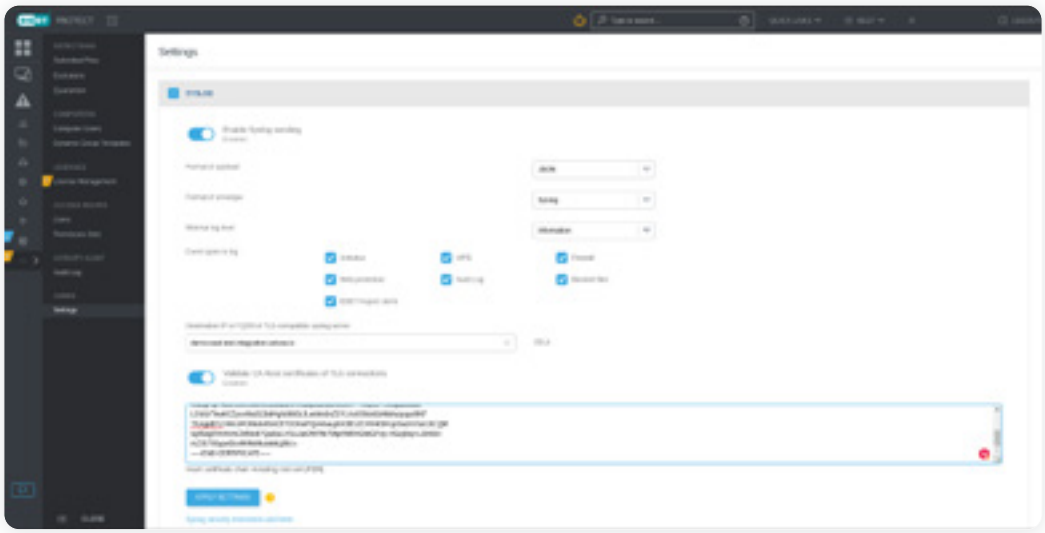


Events: Threats, HIPS, Firewall, Audit (JSON via Syslog)
Transport:TLS-secured syslog with Sekoia Intake Key in header

Use Case

ESET generates alerts from Threat, HIPS, or Audit events indicating suspicious behavior on an endpoint. These events are securely forwarded to Sekoia Defend, where they are enriched with CTI and evaluated using Sigma-based detection logic.

If malicious activity is confirmed, analysts can immediately initiate response actions—such as isolating the affected host or triggering a scan—directly from the Sekoia console. The result is rapid containment, enriched investigation context, and streamlined response orchestration.



About ESET

PROACTIVE DEFENSE. MINIMIZE RISKS WITH PREVENTION.

Experience best-in-class protection thanks to ESET's in-house global cyber threat intelligence, compiled and examined for over 30 years, which drives our extensive R&D network led by industry-acclaimed researchers. ESET PROTECT, our cloud-first XDR cybersecurity platform, combines next-gen prevention, detection, and proactive threat-hunting capabilities. ESET protects your business so you can unlock the full potential of technology.

About Sekoia

Sekoia.io is a European cybersecurity technology company and leading provider of detection and response solutions, boosted by AI and Cyber Threat Intelligence. By combining threat anticipation through knowledge of attackers with automation of detection and response, the Sekoia AI SOC platform provides security teams with a unified view and total control over their information systems. Its open approach and interoperability with third-party solutions enable organizations to take full advantage of their existing technologies. Sekoia.io gives its customers the means to focus their human resources on high-value-added missions, optimize their cyber-defense strategy, and regain the advantage against advanced cyber threats.