

From workspace signals to coordinated response

Connect HarfangLab's Workspace Detection and Response platform with Sekoia to centralize endpoint events, enrich investigations with threat intelligence, and coordinate response across the SOC.

A stronger response to endpoint-driven threats

Endpoint security generates a constant flow of alerts, telemetry, and investigation data. Without central correlation and threat context, analysts can spend too much time switching between tools, validating alerts, and manually coordinating response actions. The Sekoia and HarfangLab integration brings endpoint data into the SOC workflow, where it can be correlated with other security events, enriched with cyber threat intelligence, and used to trigger response actions directly from Sekoia.

This creates a more connected operating model:

- HarfangLab EDR provides endpoint visibility, detection, and protection.
- Sekoia centralizes security data, adds context, applies detection logic, and orchestrates response.
- Security teams investigate and act from a unified operational workflow.

How the integration works

① COLLECT ENDPOINT EVENTS IN SEKOIA

HarfangLab can forward security events, telemetry, and logs to Sekoia. The documented integration uses TCP/SSL Syslog with RFC5424 formatting. Supported data includes authentication, drivers, network activity, processes, and web activity⁽¹⁾.

The Sekoia intake can receive examples such as:

- Process and PowerShell activity
- Network and DNS events
- YARA, Sigma, antivirus, and self-protection detections
- Persistence and privilege changes
- File activity
- Windows Event Logs
- Agent inventory and agent logs

② ADD CONTEXT AND DETECT THREATS

Sekoia combines different workspace data from HarfangLab with other security signals to support investigation and response by analysts and AI agents. Once endpoint data is available in Sekoia, analysts and AI agents can combine it with other security sources and threat intelligence. Sekoia detection rules can identify suspicious activity that was not necessarily flagged by the endpoint platform itself, while native HarfangLab alerts can also be centralized for investigation. Sekoia's detection catalogue continues to receive HarfangLab-specific maintenance, including improvements to event mapping and parsing⁽²⁾⁽³⁾.

③ INVESTIGATE FROM A UNIFIED SOC WORKFLOW

Security teams can investigate HarfangLab events alongside data from other security controls. This helps analysts connect endpoint activity with related network, identity, cloud, or threat-intelligence signals. The result is a clearer understanding of:

- What happened
- Which endpoints are affected
- Whether the activity is part of a wider campaign
- Which indicators, users, processes, or hosts are involved
- What action should be taken next

④ TAKE ACTION THROUGH SEKOIA

Sekoia's HarfangLab action library supports response and investigation workflows through the HarfangLab API. Documented actions include:

- Create indicators of compromise in HarfangLab
 - Enable blocking, quarantine, or endpoint detection for indicators
 - Add comments to HarfangLab threats
 - Update threat status
 - Isolate or de-isolate an endpoint or group of endpoints
 - Retrieve endpoint telemetry
 - List processes and named pipes
 - Resolve hostnames by IP address
 - Download a file from an endpoint
- These actions allow teams to move from detection to response without manually transferring information between platforms⁽⁴⁾⁽⁵⁾

Key use cases

CENTRALIZE HARFANGLAB ALERTS

Bring HarfangLab security events into Sekoia for centralized monitoring, triage, investigation, and reporting.

DETECT ACTIVITY BEYOND INDIVIDUAL ENDPOINT ALERTS

Apply Sekoia detection rules and threat intelligence to identify suspicious behaviors across endpoint telemetry, including activity that may not have generated a native HarfangLab alert.

ENRICH ENDPOINT INVESTIGATIONS

Combine HarfangLab events with external threat intelligence and other security signals to support analyst-led and agentic investigations, giving security teams more context around an incident.

DISSEMINATE THREAT INTELLIGENCE

Push relevant indicators from Sekoia into HarfangLab, with configurable options to enable detection, blocking, or quarantine on the endpoint.

COORDINATE RESPONSE ACTIONS

Use Sekoia Playbooks and Notebooks to trigger actions on HarfangLab, update threat status, add investigation notes, and support a consistent response process.

MAINTAIN ASSET VISIBILITY

The HarfangLab EDR asset connectors retrieve device and software asset information through the HarfangLab API and create standardized asset inventory data in Sekoia Assets⁽⁶⁾⁽⁹⁾.

What teams gain

MORE CONTEXT FOR EVERY ALERT

Endpoint signals can be enriched with threat intelligence and correlated with activity from other security controls.

FASTER, MORE CONSISTENT RESPONSE

Playbook-driven actions help analysts apply the appropriate response without manually moving between consoles.

BETTER USE OF EXISTING INVESTMENTS

Organizations can continue using HarfangLab for endpoint protection while extending its value through Sekoia's SOC, detection, threat-intelligence, and orchestration capabilities.

A UNIFIED SECURITY OPERATION

Security teams can centralize endpoint investigations, threat prioritization, and response workflows in Sekoia while retaining HarfangLab's endpoint capabilities.

Technical overview

CAPABILITY	INTEGRATION SCOPE
Endpoint event ingestion	HarfangLab telemetry, alerts, and logs forwarded to Sekoia
Transport	TCP/SSL Syslog using RFC5424
Detection	Sekoia correlation, threat intelligence, and detection rules
Asset visibility	HarfangLab device inventory retrieved through the API
Threat intelligence	Indicators can be created in HarfangLab from Sekoia workflows
Response	Endpoint isolation, de-isolation, quarantine, blocking, telemetry retrieval, and investigation actions
Investigation	Process, named-pipe, hostname, telemetry, and file-retrieval actions
Operational workflow	Sekoia Playbooks and Notebooks can trigger actions on HarfangLab

For Syslog ingestion, the documented setup requires a Sekoia intake key, TCP/SSL connectivity, RFC5424 formatting, and OpenSSL configuration on the HarfangLab side ⁽¹⁾.

A European approach to integrated cyber defense

The Sekoia and HarfangLab integration is also part of the broader European Defense Platform developed with Infinigate. This offer combines HarfangLab endpoint protection with Sekoia XDR, SOAR, threat intelligence, and AI capabilities, with the Sekoia console serving as a central investigation and remediation interface ⁽⁷⁾⁽⁸⁾.

The precise technical and commercial scope should be confirmed for each deployment, particularly regarding deployment model, licensing, asset volume, telemetry coverage, and available response actions.

Sources

1. [HarfangLab integration documentation](#)
2. [Sekoia detection rules changelog](#)
3. [Detection catalogue update, changelog entry 41022](#)
4. [HarfangLab action library documentation](#)
5. [Action library update, changelog entry 39095](#)
6. [HarfangLab EDR asset connector documentation](#)
7. [HarfangLab press release, European Defense Platform](#)
8. [HarfangLab blog, European Defense Platform](#)
9. [HarfangLab EDR software asset connector documentation](#)

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.

ABOUT HARFANGLAB

HarfangLab is the European leader in Workspace Detection and Response. As security teams juggle fragmented tools that compound coverage gaps across endpoints, identities, cloud environments, exposed assets, and AI agents, HarfangLab delivers a unified platform powered by a single lightweight agent and AI built for cyber. Certified by ANSSI and BSI, and recognized by Gartner and Forrester, HarfangLab extends detection and response across the modern workspace, from on-prem to the cloud, wherever work happens.

Discover the full picture at sekoia.com



One platform.
Total control.

And 320+ integrations to choose from

CONTACT US