

Integrated Security Operations table

Integrated Security Operations at a glance

Integrated security operations bring detection, investigation, threat intelligence and response into one operating model.

The table below shows how Sekoia addresses the core capabilities required to operate security as one system.

Integrated security operations capability	How Sekoia addresses it	Selected proof points Q3 2026
SIEM core functions, including third-party tools	Native SIEM capabilities: real-time ingestion, normalization, detection, investigation and reporting across the customer's security stack.	MTTD: 8 sec False-positive rate: 0.008%
Native threat intelligence	Built-in CTI from Sekoia's threat research team, feeding detection rules, enrichment and hunting.	3 million exclusive live IOCs for detection 100 million objects for enrichment
Response and automation from one place	Native SOAR playbooks and response actions across existing security controls.	MTTR: 3.3 min
Agentic investigation and governed response	Agentic capabilities triage, enrich and investigate at scale under customer-defined human governance.	MTTI: 4.5 min Triage efficiency: 89.6%
Cross-source investigation workbench	One console for cross-source investigations, enriched alerts and AI-guided analysis.	187 ms average query time
Security-environment extensions	Security-environment extensions covering exposure, identity, cloud and other security controls through the same operational layer.	312 integrations
Open integrations and customer choice	Keep existing EDR, firewall and cloud controls as first-class sources and response points rather than replacing what already works.	Third-party stack integration
Other core Sekoia ambitions	How Sekoia addresses it	Selected proof points
Operator and MSSP delivery	Multi-tenant architecture enables MSSPs and MDRs to deliver integrated security operations outcomes across customers.	Built for operator-led delivery
Openness	Full-scope API coverage for 3 rd party wrappings	API doc, SDKs, MCP
Sovereignty and deployment choice	European ownership and deployment options, including self-hosted deployments, for organizations with strict data-control or infrastructure requirements.	5 cloud regions; self-hosted deployment available
Certifications and assurance	Security and compliance controls support regulated deployment requirements.	PCI DSS SOC 2 ISO 27001 ENS

This page presents Sekoia's perspective on integrated security operations and is not a Gartner assessment, scorecard or reproduction of Gartner research.