Unify protection, simplify security with ‹ Sekoia Defend ›

Experience an intuitive SOC platform where intelligence drives unparalleled threat detection, investigation and response.

In today's security landscape, organizations rely on various tools, but these siloed setups lack efficiency. The process of detecting, isolating, and resolving security incidents is resource-intensive and time-consuming, involving multiple consoles.

Security analysts are manually sifting through diverse data sources to find the root cause, while threat actors are cleverly exploiting security gaps.

To enhance protection across both cloud and on-premises ecosystems, organizations need to consolidate threat detection, investigation, hunting, and response across multiple domains with eXtended Detection and Response (XDR).

HIGHLIGHTS

Experience **real-time** threat detection and response like never before with our **unified and easy-to-use** SaaS solution, based on an open architecture, and powered by threat intelligence.

With an extensive catalog of integrations, exclusive threat intelligence, and verified detection rules, we deliver **unmatched time-to-value**, making our customers' protection easier and stronger in no time.

We ensure **cost predictability** through transparent, asset-based pricing, coupled with **responsive support** from our dedicated team, offering comprehensive guidance and timely assistance worldwide.

KEY BENEFITS

01 Unified security platform

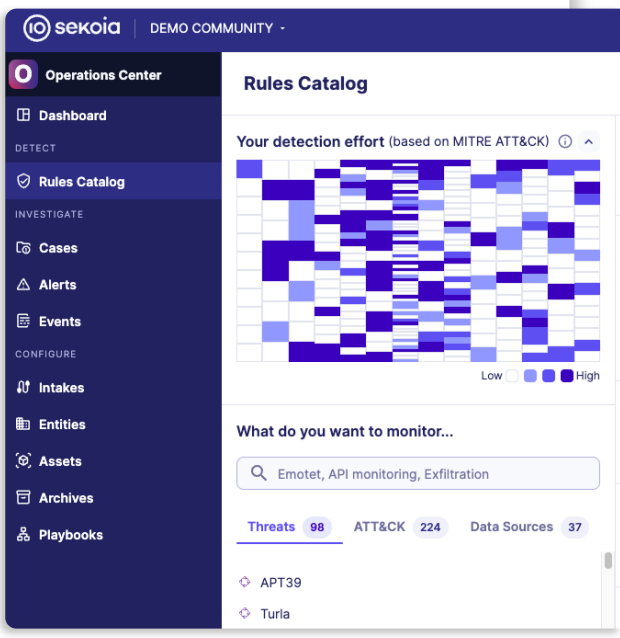
Sekoia Defend integrates Next-Gen SIEM, orchestration, incident response, and CTI into a unified platform, providing a centralized and comprehensive solution for cybersecurity.

02 Flexibility and openness

The platform's agnostic approach allows it to adapt to various technologies, both on-premises and in the cloud, with an expanding integration catalog and the ability to create custom integrations.

03 Global accessibility

As a SaaS solution, **Sekoia Defend** ensures secure and accessible global use, enabling users to connect from anywhere at any time via a dedicated URL.



04 Efficient event collection

The platform supports multiple methods of event collection, including push and pull modes, with a vast catalog of integrations, making it easy to collect and manage security data.

05 Normalization and enrichment

Events are normalized using Elastic Common Schema (ECS), facilitating transparent and auditable data handling. Enrichments with CTI observables and organizational assets enhance the context for analysts.

06 Real-time threat detection

Sekoia Defend employs behavioral, CTI-based, and anomaly detection in real-time, providing a proactive defense against a wide range of cyber threats.

07 Extensive catalog of verified detection rules

The platform offers a rich catalog of rules categorized by threats, MITRE ATT&CK techniques, and data sources, all organized and contextualized for efficient threat analysis.

08 Collaborative incident management

The platform provides features such as alert lifecycle management, case management, and collaborative investigation tools, streamlining incident response and improving team efficiency.

09 Automation and orchestration

Sekoia Defend incorporates SOAR capabilities with easy-to-use playbooks, allowing users to automate responses, streamline workflows, and execute actions at scale, enhancing the efficiency of cybersecurity operations.

10 Threat intelligence integration

With access to **Sekoia Intelligence**, the platform automatically infuses threat intelligence into the analysis, providing rich contextual information for quick and informed decision-making during threat detection and incident response.

OUR XDR & SIEM OFFERINGS

Sekoia Defend	Core	Prime
Manage multiple communities	✓	✓
Ingest data from third-party sources	✓ LIMITED	✓
Use 750+ verified detection rules	✓	✓
Get actionable insights from alerts	✓	✓
Automate tasks and remediation	✓	✓
Use our Playbooks on-premises	-	✓
Set up custom roles for users	-	✓
Security features to meet compliance	-	✓
Access to Sekoia CTI feeds & reports	OPTION	OPTION

RECOGNITIONS & CLIENTS

Gartner

Sekoia.io XDR mentioned in **Gartner** research paper: Emerging Tech: Security - Adoption Growth Insights for Extended Detection & Response.

FROST & SULLIVAN

Sekoia.io XDR named a leader in the latest Frost RadarTM for Extended Detection & Response providers.

stoïk Avril MIRAKL manche numer:que

PREMIER MINISTRE · COUNCIL OF EUROPE · angers loire métropole · MARLINK ABOVE AND BEYOND

About Sekoia.io

Sekoia.io is a European Cybertech, expert in intelligence-based eXtended Detection and Response solutions. Our **Sekoia SOC platform** provides a unified view and full control of the perimeter to be defended. Our mission is to empower security operations teams with a flexible and easy-to-use platform. We protect more than 150 Fortune 1000 companies, technology scaleups, governments, and Tier One MSSP partners worldwide.

Learn more & Contact us!

www.sekoia.io

contact@sekoia.io