

Showcasing our MSSP expertise with CTI and Sekoia SOC Platform

COMPANY

MSSP Partner since 2022

JOB TITLE

SOC Team Lead
(30 members)

CHOSEN SOLUTION

Sekoia SOC Platform (XDR+CTI)

ASSETS UNDER SUPERVISION

Over 100,000 in 2024

GROWTH OBJECTIVE

+25% in 2024

▶ Why Sekoia.io?

We chose Sekoia SOC platform for several reasons. Firstly, the diversity of technologies integrated by Sekoia enables us to **reduce our inter-connection and integration efforts**, which is a significant advantage for an MSSP. In addition, the solution offers **price predictability** thanks to billing based on the number of assets rather than the volume of logs, making it easier for our customers to manage costs. Finally, the **native integration of CTI** in Sekoia enables us to benefit from advanced threat detection, which has already proved its value on several occasions for our customers.

Sekoia SOC platform stands out for its ability to meet the following specific challenges:

- ◆ **Ready-to-use integration catalog:**
We can quickly integrate multiple data sources and demonstrate the value of our offering from the Proof of Concept (POC) stage.
- ◆ **Native CTI integration:**
Detection rules incorporating CTI enable us to detect weak signals and anticipate threats proactively.
- ◆ **Transparent asset-based billing model:**
This predictable model is a true differentiator, especially for attracting new, less mature clients.
- ◆ **Hybrid MDR approach:**
The balance between standardization and customization perfectly meets our expectations (80% shared services, 20% bespoke).
- ◆ **Trusted SIEM approach:**
We systematically propose Sekoia.io to governmental clients. Having this European SIEM solution is a major asset to offer trusted services.

CONTEXT & CHALLENGES

As a Managed Security Service Provider (MSSP), our 30-member team specializes in monitoring our clients' information systems using **XDR technology**.

Our primary challenge lies in efficiently **interconnecting tools and processes** to provide optimal protection to our clients. We require a large catalog of integrations to minimize integration efforts and focus on **delivering value** to our clients.

Another significant challenge is maximizing the return on our investment in **Threat Intelligence (CTI)**. How can we provide real added value to our clients while managing our costs effectively?

In addition, volume-based log **billing** offered by some vendors is problematic, especially for **less mature customers** who are unable to estimate their volume (EPS). This complicates budget management and can become a barrier to the adoption of robust security solutions.

▶ Benefits

The Sekoia SOC Platform enables us to significantly enhance our clients' security management:

- ◇ Optimization of alert qualification and management
- ◇ Comprehensive overview with integrated SIEM and CTI
- ◇ Strengthened operational reactivity and efficiency
- ◇ Cost predictability for our clients

Certified Sekoia.io training empowers our teams to better support our clients in platform usage and showcase our MSSP expertise.

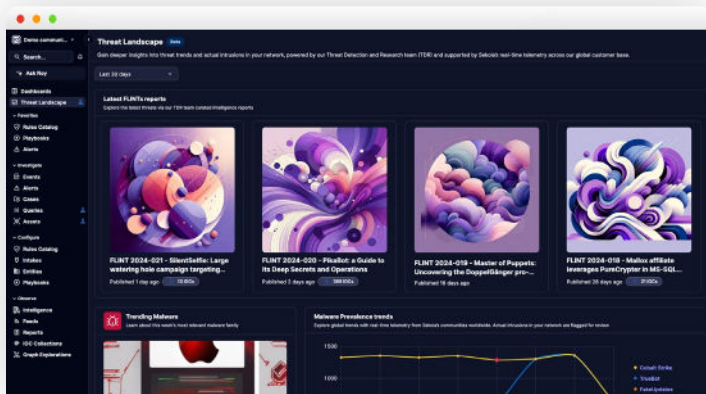
We can also offer **value-added services** such as creating parsers and contextual rules to meet each client's specific needs.

▶ Use cases

Our primary use cases include continuous monitoring, alert management, detection rule adjustment, and guiding our clients in incident response.

We prioritize topics with **visible impacts** on the client, leveraging community Sigma and STIX rules and playbooks to optimize our interventions.

The ability to rapidly adapt defense strategies to new threats is essential to guarantee our customers' security.



Take the time to test the SOC Sekoia platform by yourself !

Take a tour

66 TESTIMONIAL

Our collaboration with Sekoia has elevated our clients' security level while showcasing our expertise.

Sekoia's integrated CTI impressed us from the start!

The platform's reliability and the team's responsiveness are major assets for our success



MSSP
SOC Team Lead,
France

★ SATISFACTION ^{1/3}

9/10

- ★★★★★ Very reliable product
- ★★★★★ Rapid integration
- ★★★★★ Responsive customer support

Our collaboration with Sekoia.io can be summed up in one word: **Great!**

Sekoia.io is a preferred partner for any organization looking to strengthen its security posture through a flexible approach, seamless integration, and exceptional customer support.



www.sekoia.io

io sekoia
One view. Total control.