sekoia

ÉTUDE DE CAS

Comment un MSSP valorise son expertise et la CTI grâce à Sekoia.io ?

CLIENT
Partenaire MSSP depuis 2022

POSTE
Responsable de l'équipe XDR (30 personnes)

SOLUTION RETENUE
Sekoia SOC Platform (XDR+CTI)

NOMBRE D'ACTIFS SUPERVISÉS
Plus de 100 000 en 2024

OBJECTIF DE CROISSANCE
+25% en 2024

Pourquoi Sekoia.io XDR ?

Nous avons choisi la plateforme SOC Sekoia pour plusieurs raisons. Tout d'abord, la diversité des technologies intégrées par Sekoia nous permet de **réduire nos efforts d'interconnexion et d'intégration**, ce qui est un avantage significatif pour un MSSP. De plus, la solution offre une **prédictibilité de prix** grâce à une facturation basée sur le nombre d'actifs plutôt que sur la volumétrie des logs, facilitant la gestion des coûts pour nos clients. Enfin, **l'intégration native de la CTI** dans Sekoia nous permet de bénéficier d'une détection avancée des menaces, ce qui a déjà prouvé sa valeur à plusieurs reprises pour nos clients.

Ainsi, la plateforme SOC Sekoia se distingue par sa capacité à répondre aux défis spécifiques suivants :

- **Catalogue d'intégrations prêtes à l'emploi**
  Nous pouvons intégrer rapidement de multiples sources de données et démontrer la valeur de notre offre dès le POC.
- **Intégration native de la CTI**
  Les règles de détection intégrant la CTI Sekoia nous permettent de détecter des signaux faibles et d'anticiper les menaces de manière proactive.
- **Modèle de facturation transparent basé sur les actifs**
  Ce modèle prévisible est un vrai différenciant, en particulier pour attirer de nouveaux clients moins matures.
- **Approche MDR hybride**
  L'équilibre entre standardisation et personnalisation répond parfaitement à nos attentes (Services à 80% mutualisés, 20% sur-mesure).
- **SIEM souverain**
  Pour les administrations, nous proposons systématiquement Sekoia en tant que solution SIEM souveraine, un atout majeur sur le marché.

CONTEXTE & ENJEUX

En tant que fournisseur de services de sécurité managés, notre principal défi réside dans l'interconnexion efficace des outils et des processus de nos clients, via une solution XDR co-managée par notre équipe de 30 personnes.

Nous avons besoin de disposer d'un catalogue riche d'intégrations pour limiter les efforts d'intégration et de nous concentrer sur la valeur ajoutée pour nos clients.

Un autre enjeu majeur est la rentabilisation de notre investissement dans la Threat Intelligence (CTI). Comment offrir une réelle valeur ajoutée à nos clients tout en maîtrisant nos coûts ? La capacité à fournir des analyses de sécurité avancées tout en minimisant les frais opérationnels est cruciale.

Enfin, la facturation basée sur la volumétrie des logs est problématique, en particulier pour les clients les moins matures ne pouvant pas évaluer leur volume (EPS). Cela complique la gestion budgétaire et peut devenir un frein à l'adoption de solutions de sécurité robustes.

Bénéfices

La plateforme SOC Sekoia nous permet d'améliorer considérablement la gestion de la sécurité de nos clients :

- Optimisation de la qualification et de la gestion des alertes
- Vue d'ensemble complète avec le SIEM et la CTI intégrés
- Réactivité et efficacité opérationnelle renforcées
- Prédictibilité des coûts pour nos clients

Les **formations certifiantes** Sekoia permettent à nos équipes de mieux accompagner nos clients dans l'utilisation de la plateforme et de valoriser notre expertise de MSSP.

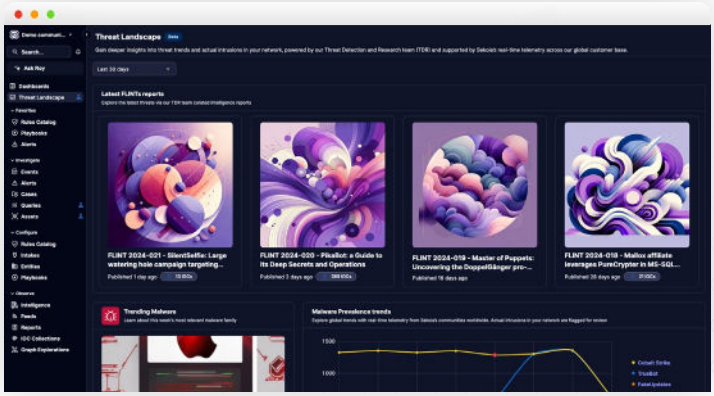
Nous pouvons également proposer des **services à valeur ajoutée** comme la création de parseurs et de règles contextualisées pour répondre aux besoins spécifiques de chaque client.

Cas d'usage

Nos principaux cas d'usage incluent la surveillance continue, la gestion des alertes, l'ajustement des règles de détection et l'accompagnement de nos clients dans la réponse aux incidents.

Nous priorisons les sujets ayant un **impact visible** chez le client, en utilisant les règles Sigma et STIX de la communauté ainsi que les playbooks pour optimiser nos interventions.

La capacité à adapter rapidement les stratégies de défense aux nouvelles menaces est essentielle pour garantir la sécurité de nos clients.



Prenez le temps de tester la plateforme SOC Sekoia par vous-même !

Voir la démo

TÉMOIGNAGE

Notre collaboration avec Sekoia nous a permis d'élever le niveau de sécurité de nos clients tout en valorisant notre expertise.

La CTI intégrée de Sekoia nous a beaucoup plu dès le début !

La fiabilité de la plateforme et la réactivité des équipes sont des atouts majeurs pour notre succès

MSSP
Responsables
des équipes XDR

SATISFACTION

9/10

★★★★★ Produit très fiable
★★★★★ Intégrations rapides
★★★★★ Support client réactif

Notre collaboration avec Sekoia.io peut être résumée en un mot : Satisfait !

Sekoia.io est un partenaire de choix pour toute organisation cherchant à consolider sa posture de sécurité grâce à une approche flexible, une intégration transparente et un support client exceptionnel.

www.sekoia.io

sekoia
One view. Total control.