

Maîtrisez les cybermenaces avec < Sekoia Intelligence >

Obtenez des informations éclairées sur les cybermenaces et transformez les données brutes en renseignements exploitables à travers l'ensemble de votre écosystème.

Les organisations dépendent de leurs systèmes informatiques pour mener leurs opérations, ce qui entraîne une extension du périmètre à défendre. Pour faire face aux cybermenaces, les organisations ont besoin d'une connaissance approfondie des risques auxquels elles sont exposées, ainsi que des outils et des tactiques utilisés par les cybercriminels. C'est là que la Cyber Threat Intelligence (CTI) entre en jeu.

Sekoia.io est à l'avant-garde de la CTI en Europe. Notre équipe dédiée de chercheurs en cybersécurité, appelée Threat Detection & Research (TDR), est passionnée par la production de renseignement sur les cybermenaces, que nous mettons à disposition via notre plateforme SaaS.

POINTS FORTS

Sekoia.io propose un renseignement **stratégique et technique**, qui permet de comprendre les cybermenaces actives et les Indicateurs de Compromission (IoCs) qui leurs sont associés.

En se basant sur les **standards de l'industrie**, nous produisons du renseignement pouvant être utilisé par toute type d'organisation, quel que soit son secteur.

Nous produisons du renseignement opérationnel qui améliore les **capacités de détection** et offre un niveau élevé de **contexte sur la menace** ainsi que de connaissance de la situation.

CARACTÉRISTIQUES

01

Renseignement natif de qualité

Accédez au renseignement exclusif de nos analystes CTI - **Threat Detection & Research (TDR) Team** - et de sources tierces, avec de puissantes fonctionnalités de recherche, de filtrage et d'intégration.

02

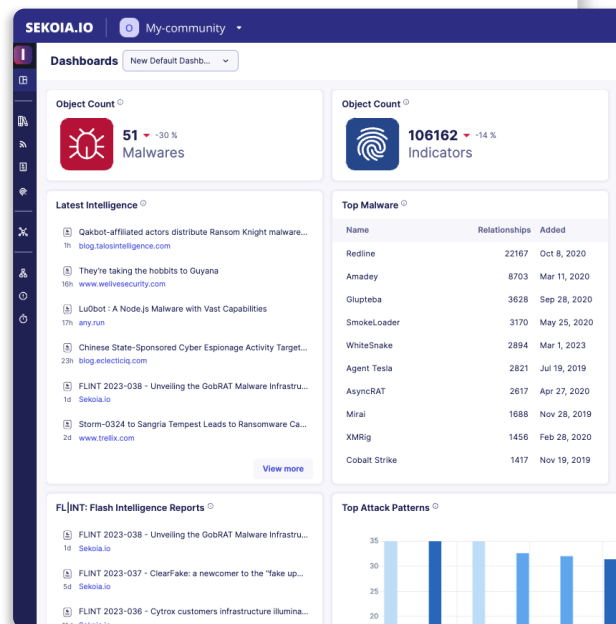
Sources de renseignement multiples

Nous agrégeons des informations provenant de sources exclusives, OSINT (Open Source Intelligence) et communautaires, en les reliant et les contextualisant systématiquement à l'aide de STIX 2.1.

03

Flux d'informations sur les cybermenaces

Notre plateforme est mise à jour en continu, avec l'ajout d'environ 150 000 nouveaux IoCs chaque mois. Elle comprend plus de 6 millions d'objets liés aux menaces, interconnectés à travers un million de relations.



04

Rapports CTI approfondis

Nous proposons environ 4 000 rapports de recherche, couvrant des rapports de renseignement exclusifs de **Sekoia.io** et de tiers.

05

Collecte de renseignements tiers

Regroupez vos flux de renseignements sur les menaces provenant de tiers au sein de la **plateforme SOC Sekoia** et importez vos listes personnalisées d'indicateurs de compromission (IoCs).

06

Diffusion facile du renseignement

Facilitez la distribution du renseignement vers des systèmes tiers, sur le cloud et en local, pour une détection et une contextualisation améliorées (SIEM, SOAR, TIP, EDR, pare-feu, etc.) grâce à nos intégrations natives, capacités API, TAXII et playbooks.

07

Explorations graphiques

Faites le lien entre les menaces pour des investigations efficaces.

08

Tableaux de bord

Créez des tableaux de bord personnalisés pour surveiller les tendances, les principales menaces et voir les rapports récents.

09

API REST publiques

Configurez la plateforme à l'aide des micro-services et API REST.

10

Cas d'usage possibles

Déployez la CTI pour divers cas d'usage, afin d'améliorer votre posture de sécurité :

- ▶ Dissémination d'IoCs vers des moteurs de détection EDR
- ▶ Diffusion d'IoCs vers les listes noires d'un firewall on-premise
- ▶ Hunting, retro-hunting, et télémétrie
- ▶ Contextualisation de la réponse aux incidents dans un SOAR
- ▶ Mise en détection des IoCs Sekoia.io sur votre SIEM

NOTRE OFFRE CTI

Possibilités offertes par Sekoia Intelligence

Accéder à notre base de données CTI



Configurer des flux CTI personnalisés



Lire nos rapports sur les menaces



Importer notre CTI dans vos systèmes



Importer et utiliser des IoCs externes



Importer notre CTI dans vos systèmes



Diffuser des IoCs via des APIs tiers



Automatiser les actions pour le hunting



CLIENTS & MENTIONS

Gartner

La CTI de **Sekoia.io** est mentionnée dans le rapport "Market Guide for Security Threat Intelligence Products and Services" **Gartner**, 2023

FROST & SULLIVAN

La CTI de **Sekoia.io** est citée dans le rapport "Global Threat Intelligence Platforms" - **Frost & Sullivan**, 2022



À propos de Sekoia.io

Sekoia.io est une entreprise européenne spécialisée dans la cybersécurité, experte dans les solutions de détection et réponse étendues, alimentées par du renseignement exclusif. La **plateforme SOC Sekoia** offre une vision unifiée et un contrôle total du périmètre à défendre. Notre mission est de donner aux équipes SOC un accès à une plateforme flexible et facile à utiliser. Nous protégeons plus de 150 entreprises, des administrations publiques et des partenaires MSSP de premier plan à travers le monde.

Des questions ? Un projet ?

www.sekoia.io
contact@sekoia.io