

Aperçu de Sekoia Intelligence

Sekoia Intelligence – CTI reloaded

Sekoia Intelligence permet aux équipes CERT et SOC d'accéder à la base de données exclusive de Sekoia Cyber Threat Intelligence, les dotant ainsi d'informations précieuses pour une surveillance et une réponse efficaces en matière de cybersécurité.

Les équipes CERT et SOC peuvent également utiliser la **plateforme SOC Sekoia** comme centre de collecte et d'opérationnalisation des indicateurs de compromission au sein de leur écosystème de cybersécurité, en rationalisant la gestion des informations sur les menaces et en améliorant les capacités de réponse aux incidents.

Outils	Vos besoins	Comment Sekoia Intelligence peut vous aider
TABLEAUX DE BORD	Personnalisation des tableaux de bord	Nous proposons des tableaux de bord personnalisables avec des widgets flexibles. Le tableau de bord par défaut donne une vue synthétique de l'activité actuelle de la communauté, tant du point de vue de la sécurité opérationnelle (niveau de risque, nombre d'alertes, etc.), que du point de vue de l'activité (liste des derniers commentaires postés, des dernières alertes créées, etc.)
BASE DE DONNÉES CTI	Accès à notre base de données CTI exclusive	Notre base de données CTI, continuellement mise à jour à partir de plus de 450 sources qualifiées, produit des renseignements qui sont enrichis par les recherches et analyses quotidiennes effectuées par nos analystes. Elle contient plus de 7 millions d'IOCs qualifiés et maintenus à jour.
RAPPORTS	Accès aux rapports sur les menaces des analystes CTI	Accédez à une analyse complète des menaces rédigée par notre équipe Threat Detection & Research (TDR).
FLUX SORTANTS	Accès à un flux CTI personnalisé depuis l'extérieur	Configurez des flux personnalisés pour recevoir et lire les dernières nouvelles directement dans votre application. Adaptez et personnalisez vos flux en fonction de vos besoins. Pour obtenir plus d'informations sur un secteur, une activité, une source ou une zone géographique, vous pouvez utiliser les filtres.
API	Collecte automatique de la CTI dans vos systèmes	Incorporez nos IOCs dans votre système sans avoir besoin d'accéder à la plateforme.
IOC COLLECTION	Import et utilisation d'IOCs externes	Les IOCs sont cruciaux pour la détection et sont partagés entre les équipes et les prestataires. Nous proposons nos propres IOCs et vous permettons d'en importer d'autres sources via IOC Collection (import de fichiers et de textes).
PLAYBOOKS	Automatisation de tâches	Les fonctions d'automatisation facilitent les tâches des analystes et permettent d'importer et de diffuser les flux d'IOCs, ainsi que de mettre en place des flux de travail personnalisés.
SUPPORT PREMIUM OPTION	Services d'assistance premium, en plus des services CSM existants.	Notre support premium comprend un SLA robuste garantissant un temps de disponibilité de 99,9 %, un accès étendu à nos ressources de support, telles que la messagerie instantanée in-app, des temps de réponse garantis, un Solution Advisor dédié (anciennement TAM), un canal Slack dédié.

Quels sont les principaux avantages de Sekoia Intelligence ?

- **Sekoia Intelligence** excelle dans la détection précise des menaces et la production de rapports de qualité, fournissant des informations exploitables pour une prise de décision éclairée.
- Le renseignement est organisé en paquets STIX, ce qui permet de comprendre l'ensemble du paysage des menaces. Cette approche favorise **l'interopérabilité et la normalisation**, assurant une intégration transparente avec d'autres outils et systèmes de sécurité, tout en mettant en évidence le contexte nécessaire à une compréhension approfondie de la menace.
- **Sekoia Intelligence** va au-delà du simple affinage des sources en intégrant des informations provenant de canaux multiples, y compris des sources privées et des enquêtes exclusives. Cette approche unique garantit une **vision complète et nuancée** des menaces potentielles.
- L'intégration de la télémétrie des clients XDR accroît la profondeur des renseignements sur les menaces grâce à des **données réelles**.
- La plateforme est alimentée par une équipe multidisciplinaire d'analystes CTI, connue sous le nom **Threat Detection & Research (TDR)**, qui couvre l'ensemble du paysage des menaces à partir de multiples perspectives (d'un point de vue stratégique et technique), y compris multi-régions, industries, étatiques, cybercriminalité et plus encore.