Comparer les offres « Sekoia Defend »

Sekoia Defend Core – XDR reloaded

Le **plan Core** est conçu pour les équipes SOC qui cherchent à améliorer leurs capacités de détection et de réponse dans un environnement cloud. Il offre des caractéristiques essentielles, une intégration transparente dans leur environnement, des fonctionnalités conviviales, le tout à un prix abordable.

Sekoia Defend Prime – SIEM reloaded

Le **plan Prime** est conçu pour les équipes SOC à la recherche d'outils avancés et répondant aux exigences de conformité. Ses capacités de détection et de réponse étendues dans des environnements hybrides, offent à la fois un déploiement rapide et des fonctionnalités conviviales.

Outils	Vos besoins	Comment Sekoia Defend peut vous aider	Core	Prime & Flow
MODE MULTI-TENANT "BY DESIGN"	Gestion de plusieurs communautés à partir d'une seule plateforme	Notre solution utilise une architecture multi-tenant, permettant une utilisation par les entreprises et les fournisseurs de services de sécurité managés (MSSP) par le biais d'un accès délégué.	✓	✓
LARGE CATALOGUE D'INTÉGRATIONS*	Connexion instantanée avec des technologies tierces afin d'ingérer facilement des données externes	En tant que solution XDR agnostique, nous fournissons un catalogue complet, étendu et flexible d'intégrations tierces. Plus de 200 connecteurs sont disponibles, y compris des fournisseurs de cybersécurité de premier plan tels que Microsoft, SentinelOne, Fortinet, CrowdStrike et d'autres. Voir toutes les intégrations	✓	✓
API	Communication avec tous les systèmes logiciels via API	Grâce aux API, vous pouvez améliorer l'interopérabilité et le partage des données entre les outils de sécurité pour une meilleure détection des menaces et une meilleure réponse.	✓	✓
SEKOIA ENDPOINT AGENT	Collecte des événements de sécurité sur les postes de travail (sur Windows, Linux, MacOs)	Notre agent pour postes de travail simplifie la collecte d'événements avec une configuration minimale, transmettant automatiquement les événements à la plateforme SOC Sekoia tout en préservant l'intégrité du journal des événements.	✓	✓
RÈGLES DE DÉTECTION CTI	Détection améliorée avec identification précise des menaces et de leur contexte	Nous incluons plus de 900 règles de détection prédéfinies, créées, vérifiées et maintenues par notre équipe d'analystes CTI, afin de minimiser les faux positifs et de garantir que vos efforts opérationnels se concentrent sur les menaces crédibles.	✓	✓
RETROHUNT	Découverte et traitement rétroactif de menaces non détectées	Nos capacités de retrohunt analysent automatiquement tous vos événements passés à la recherche d'IOCs qui ont été récemment ajoutés à la plateforme. Lorsqu'un nouvel IOC est ajouté à la base de données CTI, la plateforme le recherche dans vos journaux actuels et historiques.	✓	✓
DÉTECTION D'ANOMALIES	Identification d'activités inhabituelles ou suspectes à un stade précoce	Utilisez les règles de détection d'anomalies pour l'analyse automatisée des données de séries temporelles, l'identification des schémas anormaux et le déclenchement d'alertes à différents niveaux de criticité, le tout basé sur le machine-learning.	✓	✓
CORRÉLATION SIGMA	Amélioration de la détection des menaces grâce aux corrélations Sigma	Sigma est intégré directement dans notre moteur de détection en temps réel pour une détection et une réponse plus rapides aux cybermenaces, en utilisant des champs normalisés du format ECS dans les règles.	✓	✓
CONTEXT CTI DANS LES ALERTES	Des informations exploitables sur les alertes pour améliorer la réponse aux incidents	Nos renseignements internes sur les menaces enrichissent le contexte des menaces, élevant le processus de détection et fournissant des informations précieuses aux analystes en cybersécurité.	✓	✓

* Le plan Core donne accès aux fonctionnalités essentielles, avec un forfait mensuel de 3 Go par asset. Vous pouvez installer Sekoia Endpoint Agent pour recueillir la télémétrie des postes de travail. Le plan Prime, donne un accès complet à toutes les fonctionnalités, avec un forfait mensuel de 5 Go par asset. Pour obtenir la liste détaillée des connecteurs, veuillez consulter notre catalogue d'intégrations sur le site sekoia.io.

Comparer les offres « Sekoia Defend »

Conservation des données et Sekoia Intelligence

Sekoia Defend inclut par défaut 30 jours de stockage à chaud, qui peuvent être étendus ou complétés par des archives jusqu'à 1 an. L'option **Sekoia Intelligence** offre un accès complet à notre Cyber Threat Intelligence (base de données CTI, rapports, flux et API).

Tarifs prévisibles et flexibles

Nous proposons deux plans basés sur le nombre d'actifs : **Defend Core** et **Defend Prime**, garantissant une tarification prévisible et un usage conforme à notre 'Fair Use Policy'. Si vous préférez un forfait au volume, **Defend Flow** est une solution flexible et ajustable, incluant toutes les fonctionnalités de Prime.

Outils	Vos besoins	Comment Sekoia Defend peut vous aider	Core	Prime & Flow
ASSET DISCOVERY	Une vue d'ensemble de votre infrastructure informatique	Notre fonction de gestion des actifs permet à votre équipe SOC de disposer d'une image claire de votre infrastructure informatique, de hiérarchiser les risques, d'aider à la détection des menaces et de faciliter les enquêtes sur les incidents.	✓	✓
CASE MANAGEMENT	Analyse et résolution des incidents de manière structurée et efficace	Permet de consolider et de partager les résultats des investigations provenant de diverses sources, incluant différents périmètres, alertes et analystes. Vous pouvez ouvrir un case à partir d'une alerte ou incorporer des alertes dans un case existant.	✓	✓
PLAYBOOKS	Automatisation des tâches et de la réponse dans le cloud pour une meilleure efficacité	Les fonctions d'automatisation vous permettent de vous concentrer sur les alertes prioritaires. Grâce aux Playbooks, vous pouvez créer des flux de travail pour améliorer la détection et enrichir les informations. Vous pouvez exécuter automatiquement les différentes actions de vos réponses : isolement, investigation et remédiation.	✓	✓
TABLEAUX DE BORD	Personnalisation des tableaux de bord, y compris avec vos requêtes issues du Query Builder	Nos tableaux de bord prédéfinis et personnalisables soutiennent le processus d'investigation, vous assurant que vous disposez de toutes les informations nécessaires pour prendre des décisions sur la pertinence des alertes, distinguer les faux positifs des vrais positifs et protéger les données critiques de votre entreprise.	✓	✓
QUERY BUILDER	Création de requêtes avancées et agrégation d'événements ou d'alertes	Le Query Builder vous permet de créer facilement des requêtes avancées et d'agréger des événements ou des alertes pour l'établissement de rapports, la corrélation d'événements et le hunting, y compris en utilisant des requêtes préconstruites. Vous pouvez également utiliser vos requêtes dans des tableaux de bord personnalisés.	✓	✓
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 Collections (import de fichiers et de textes).	–	✓
RÔLES PERSONNALISÉS & RESTREINTS	Configuration personnalisée des droits des utilisateurs de la plateforme	Ces rôles viennent s'ajouter aux rôles prédéfinis (lecteur, analyste, administrateur) et permettent aux administrateurs de définir précisément les droits des utilisateurs sur la plateforme, incluant l'accès aux fonctionnalités, les permissions et la ségrégation des données par intake.	–	✓
PLAYBOOKS ON-PREMISES	Automatisation des tâches et réponse efficace sur votre réseau local	Exécutez des workflows de réponse et d'orchestration via des playbooks dans des environnements SaaS et sur site à l'aide d'une interface unifiée, en répondant efficacement aux besoins de sécurité de votre réseau local.	–	✓
SÉCURITÉ ET CONFORMITÉ**	Atteinte des normes les plus élevées en matière de sécurité et de conformité	Nos fonctions de sécurité vous aident à respecter la conformité et comprennent l'application du 2FA, la désactivation du compte en cas d'inactivité, la déconnexion automatique après 15 minutes et des pistes d'audit complètes.	–	✓

** La plateforme SOC Sekoia offre de multiples possibilités d'hébergement pour répondre à vos besoins partout dans le monde. Que vous recherchiez une solution conforme aux normes PCI/DSS, un hébergement en France, en Europe ou au Moyen-Orient, Sekoia.io a une solution adaptée à vos besoins. **Pour plus de détails, visitez cette page.**