

# Protection unifiée, sécurité simplifiée avec < Sekoia Defend >

**Pilotez votre sécurité à l'aide d'une plateforme SOC intuitive, alimentée par le renseignement, et dotée de performances exceptionnelles en matière de détection, d'investigation et de réponse.**

Dans le paysage actuel de la cybersécurité, les organisations dépendent de nombreux outils, mais ces configurations en silo manquent d'efficacité. Le processus de détection, d'isolement et de résolution des incidents de sécurité requiert des ressources et du temps, impliquant l'utilisation de plusieurs consoles.

Les analystes sont contraints d'explorer manuellement des sources de données disparates pour identifier l'origine des incidents, tandis que les acteurs malveillants exploitent habilement les failles de sécurité.

Pour renforcer la protection des environnements hybrides, cloud et on-premise, les organisations doivent consolider leurs capacités de détection des menaces, d'investigation, de hunting et de réponse aux incidents, en tirant parti de la technologie eXtended Detection and Response (XDR).

## POINTS FORTS

Maximisez la détection et la réponse **en temps réel** grâce à une plateforme SaaS conviviale et performante, basée sur une architecture ouverte, et alimentée par du renseignement exclusif sur les menaces.

Obtenez des **résultats instantanés** grâce à +200 connecteurs pour une intégration fluide dans votre écosystème et +900 règles de détection vérifiées qui entrent en action dès la réception des premiers logs.

Bénéficiez d'une **prévisibilité des coûts** avec notre tarification transparente, basée sur les actifs ou le volume, combinée à la **proximité de nos équipes** pour un accompagnement complet et une assistance rapide.

## CARACTÉRISTIQUES

01

### Plateforme SOC unifiée

**Sekoia Defend** intègre, de façon unifiée, des capacités de détection (SIEM Next-Gen), du renseignement sur les menaces (CTI) et des capacités d'orchestration et de réponse aux incidents (SOAR).

02

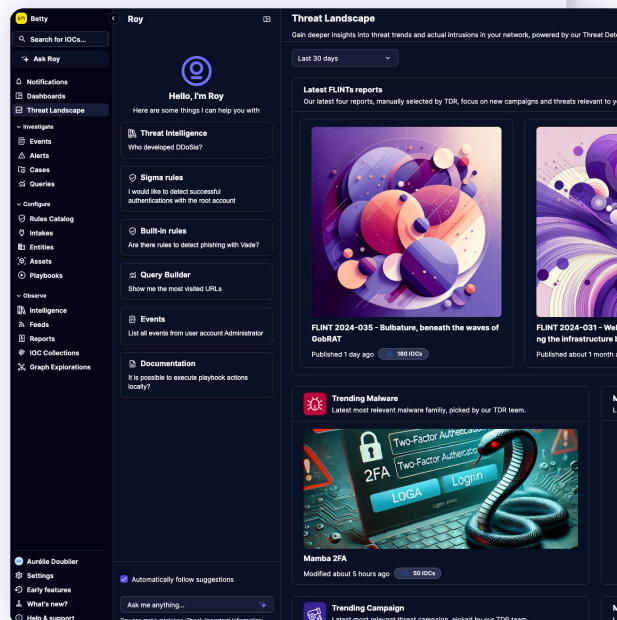
### Flexibilité et interopérabilité

L'approche agnostique de la plateforme lui permet de s'adapter à des technologies diverses, aussi bien on-premise que dans le cloud, via des connecteurs prêts à l'emploi et personnalisés.

03

### Accessibilité

En tant que solution SaaS, **Sekoia Defend** garantit une utilisation sécurisée et facile d'accès, permettant aux utilisateurs de se connecter de n'importe où et à tout moment via une URL dédiée.



04

## Collecte des événements

La plateforme prend en charge plusieurs méthodes de collecte, y compris les modes push et pull, et propose un catalogue de plus de 200 intégrations, facilitant la gestion des données de sécurité.

05

## Normalisation et enrichissement

Les événements sont normalisés à l'aide du schéma commun Elastic (ECS), facilitant l'utilisation transparente et vérifiable des données. Les enrichissements avec des observables CTI et des actifs organisationnels améliorent le contexte pour les analystes.

06

## Capacité de détection étendue en temps réel

**Sekoia Defend** utilise les règles basées sur la CTI avec retrohunt, l'analyse comportementale et la détection d'anomalies, pour offrir une défense proactive et en temps réel contre les cybermenaces.

07

## Règles de détection intégrées et vérifiées

La plateforme propose des règles catégorisées par menaces, techniques MITRE ATT&CK et sources de données, le tout organisé et contextualisé pour une analyse efficace des menaces.

08

## Gestion collaborative des incidents

La plateforme offre des fonctionnalités telles que la gestion du cycle de vie des alertes, la gestion des cas et des outils collaboratifs d'investigation, rationalisant la réponse aux incidents et améliorant l'efficacité de l'équipe.

09

## Automatisation et orchestration

**Sekoia Defend** intègre des capacités SOAR avec des playbooks faciles à utiliser, permettant aux utilisateurs d'automatiser les réponses, de rationaliser les flux de travail et d'exécuter des actions à grande échelle, améliorant l'efficacité des opérations.

10

## Intégration native de la CTI

Avec la CTI présente dans **Sekoia Intelligence**, la plateforme intègre automatiquement du renseignement sur les menaces dans l'analyse, fournissant des informations contextuelles riches pour une prise de décision rapide et éclairée lors de la détection de menaces et de la réponse aux incidents.

## NOTRE OFFRE XDR & SIEM

| Sekoia Defend                         | Core   | Prime & Flow |
|---------------------------------------|--------|--------------|
| Gérer plusieurs communautés           | ✓      | ✓            |
| Intégrer +200 sources de données      | ✓      | ✓            |
| Utiliser plus de 900 règles vérifiées | ✓      | ✓            |
| Avoir des alertes contextualisées     | ✓      | ✓            |
| Automatiser les tâches et la réponse  | ✓      | ✓            |
| Utiliser les Playbooks on-premises    | -      | ✓            |
| Configurer des rôles personnalisés    | -      | ✓            |
| Répondre aux exigences de conformité  | -      | ✓            |
| Accéder aux flux et aux rapports CTI  | OPTION | OPTION       |

## NOTRE BUSINESS MODEL

### Defend Core & Prime : Une offre adaptée à vos besoins, prévisible et optimisée !

Choisissez entre deux plans conçus pour répondre à vos besoins, avec une politique d'utilisation équitable (Fair Use Policy) : Defend Core (3 Go par mois et par actif) et Defend Prime (5 Go par mois et par actif). Suivez votre consommation directement sur la plateforme ; en cas d'approche de votre forfait, notre équipe est là pour vous aider à optimiser vos ressources. Assurez-vous d'une gestion budgétaire prévisible pour une planification financière simplifiée, sans jamais perdre vos données.

### Defend Flow : Toutes les fonctionnalités de Prime, avec un forfait au volume ajustable !

Optez pour Flow et bénéficiez de forfaits flexibles en Go par jour, avec une refacturation trimestrielle en cas de dépassement. Suivez votre consommation en temps réel et recevez des notifications lorsque vous atteignez 80% de votre quota. En cas de dépassement, notre équipe vous contactera pour réévaluer votre forfait et procéder à une refacturation sans tracas, avec un tarif convenu à l'avance. Grâce à plus de flexibilité et à des ajustements simples, gardez le contrôle sur vos coûts tout en optimisant votre utilisation.

Des questions ? Un projet ?

[www.sekoia.io](http://www.sekoia.io)
[contact@sekoia.io](mailto:contact@sekoia.io)