# LASTINFOSEC ®

**Enriched streams analysis for Smarter Detection**

GATEWATCHER

## La détection des cybermenaces avancées : Nouveau défi des organisations

Les conséquences financières d'une cyberattaque peuvent fragiliser durablement votre organisation.

L'augmentation du volume des menaces complique l'évaluation de la criticité des alertes traitées par vos analystes.

La persistance d'une attaque ciblée sur votre SI non détectée peut aggraver le préjudice occasionné.

La complexité et la furtivité des dernières cyberattaques augmentent les risques de compromission de votre S.I.

**3,86M$**

est le coût global moyen d'une violation de la sécurité des données en 2020. [1]

**255%**

est la progression du nombre d'attaques par rançongiciels en France entre 2019 et 2020. [2]

**207 jours**

est le délai moyen nécessaire à une entreprise pour détecter une brèche de sécurité. [3]

**53%**

des intrusions réussies ne sont pas détectées par les outils de cyberdétection déja en place. [4]

## La solution Lastinfosec : Un flux de Threat Intelligence compatible avec toute solution de cybersécurité et offrant une amélioration immédiate de votre protection

LastInfoSec® est une plateforme complete de Threat Intelligence permettant de faciliter la détection des menaces internes et externes susceptibles de cibler votre système d'information. Avec une bibliotheque de 6 millions d'IoCs, plus de 5000 nouveaux marqueurs qualifiés par jour et plus de 3000 différentes sources de donnée, l'infrastructure LastInfoSec® fournie des indices de compromissions enrichis et contextualisés à votre activité dans le but de réduire le temps d'analyse d'une menace lors de sa détection.

LastInfoSec® facilite la prise de décision de vos équipes de sécurité opérationnelles et réduit fortement leurs temps d'analyse et de réaction en cas d'incident sans modification de leurs processus internes.

Les moteurs automatisés de collecte, d'analyse et de corrélation de LastInfoSec® permettent de rendre accessibles les informations sur les menaces 24 heures en moyenne avant la concurrence.

L'intégration de LastInfoSec® se fait simplement et rapidement grâce à des exports standardisés aux dernières normes CTI (Stix v2, Stix v2.1, JSON..) et des connecteurs disponibles pour les principaux outils d'analyse du marché (Splunk, OpenCTI...)

La plateforme de LastInfoSec® inventorie et évalue en permanence les sources de données accessibles sur de multiples canaux : réseaux sociaux, sites spécialisés, darknet et deep web...

## Bénéfices utilisateurs

**Couverture de la menace** : Une meilleure connaissance du paysage des menaces et une augmentation de la couverture de celles-ci sont apportées par les flux de LastInfoSec.

**Prise de décision plus fiables, plus rapides, et mieux documentée** sur les suites à donner aux événements de sécurité, sur les actions à prendre en urgence et sur l'évolution des moyens techniques et humains de cyber-défense.

**Efficacité des experts** : Les temps d'analyse des experts en cyber-défense, et les délais de détection et de réaction, sont réduits. Ce gain d'efficacité permet d'augmenter la couverture des événements pris en compte et analysés. La satisfaction des équipes de cyber-défense est améliorée.

**Capacités évolutives** : Plus de 5000 nouveaux marqueurs sont diffusés par jour. En cas d'attaque à grande échelle, la plateforme de LastInfoSec n'est pas limitée dans ses capacités de collecte et de traitement et ne sera pas saturée de par son intégration technologique poussée.

**Réduction du bruit et des faux-positifs :** Les données fournies ne génèrent que des alertes significatives et apportent toute l'information nécessaire à leur compréhension. La réduction des faux positifs issus d'autres sources de Threat Intel ou de vos solutions est facilitée par corrélation avec les données de LastInfoSec.

**Gains de temps :** Par sa diffusion des marqueurs 24 h en avance sur la moyenne du marché, le flux LastInfoSec permet une détection précoce des incidents, une analyse plus rapide des événements et une prise de décision accélérées par les équipes SOC.

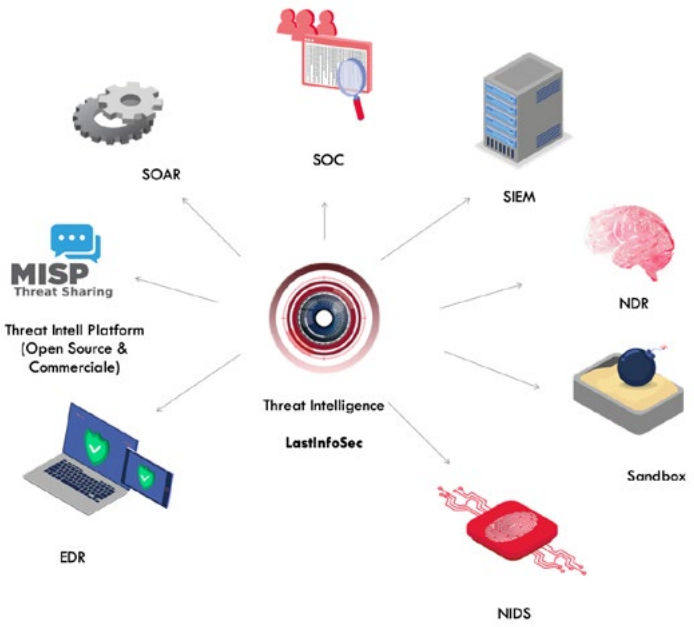
**Optimisation de l'exploitation des solutions en place :** Les informations de LastInfoSec sont connectables avec vos technologies de sécurité existantes. Elles augmentent l'efficacité des EDR, IPS, IDS, NGFW, NDR, BDS, Sandbox,SIEM et SOAR.

**Amélioration immédiate** : Intégrables en quelques clics dans votre dispositif actuel, les flux de LastInfoSec apportent une amélioration immédiate de votre niveau de cyber-défense.

## Cas d'usages

Les informations de LIS s'utilisent de manière globale sur toute une organisation, ou de façon circonscrite sur un périmètre donné. Les offres de services proposées portent sur des déploiements sur une partie des technologies de détection, par exemple sur les IDS ou les EDR, sur des outils au sein du SOC ou du CERT, ou sur toute l'organisation via des plateformes de Threat Intel. Le flux de LastInfoSec vous permet d'augmenter simplement l'efficacité de vos solutions de sécurité en améliorant la connaissance du paysage des menaces et en réduisant le bruit. Vous pouvez également automatiser votre hunting afin de réduire le temps de détection d'incidents.

- Intégration simple sans modification de vos process.
- Flux de données entièrement qualifiées et validées pour réduire les faux positifs..
- Enrichissement de vos alertes pour une meilleure réactivité de vos équipes
- Format d'export utilisable par les solutions de cybersécurité sans interaction humaine
- Contextualisation des informations facilitant le travail des équipes SOC




## Déploiement

Les informations de LastInfoSec s'utilisent de manière globale sur toute une organisation, ou de façon circonscrite sur un périmètre donné.Les offres de services proposées portent sur des déploiements sur une partie des technologies de détection, par exemple sur les IDS ou les EDR, sur des outils au sein du SOC ou du CERT, ou sur toute l'organisation via des plateformes de Threat Intel.

- Format standard et compatible avec les solutions existantes.
- Déploiement en quelques clics.
- Intégration du flux aux plateformes tierces de Threat Intel, aux solutions de sécurité réseaux existantes (IDS, IPS, NGFW, BDS, Sandbox, NDR), aux solutions de sécurité des Endpoint (EDR) et aux outils d'analyse SOC (SIEM, SOAR)

Sources : [1] Ponemon Institute, [2] ANSSI, [3] IBM, [4] FireEye Mandiant

## A propos

Gatewatcher est un éditeur européen spécialisés dans la détection des cybermenaces et intrusions les plus avancées. Son modèle associe plusieurs technologies à l'I.A pour vous offrir une protection optimale.


## Nous contacter

contact@gatewatcher.com
www.gatewatcher.com