GATEWATCHER

DETECT AND TRACK

GATEWATCHER

GATEWATCHER

NOS SOLUTIONS

CAS D'USAGE

PARTENAIRES TECHNOLOGIQUES

Gatewatcher est le leader français de la détection d'intrusions et de menaces avancées. Depuis 2015, nous protégeons les différents réseaux critiques des plus grandes entreprises, des institutions publiques et des OIV.

Gatewatcher est un acteur industriel multiproduits apportant une amélioration immédiate aux enjeux de cyberdéfense. Sa gamme de solutions intelligentes répond aux besoins de détection des organisations.

2015

GATEWATCHER

Création de **Gatewatcher**.

2016

Obtention du label **France Cybersécurité**.

Gatewatcher gagne au **FIC** le **prix spécial du jury**.

2018

HEXATRUST
CLOUD CONFIDENCE & CYBERSECURITY

Gatewatcher rejoint **Hexatrust**.

2019

Qualification élémentaire de l'**ANSSI** pour nos produits **Trackwatch**.

Gatewatcher remporte avec Harfang Lab le prix **Com Cyber** organisé par le Ministère des Armées.

2020

Lancement de la plateforme **Gatewatcher NDR**.

LastInfoSec

Rachat du pur-player de **Threat Intelligence** LastInfoSec.

NOTRE ENGAGEMENT

Se défendre dans le cyber-espace n'est plus l'affaire de quelques grands groupes qui disposent de moyens importants. Les menaces se sont complexifiées, industrialisées et ont élargi leur périmètre de frappe. Il est crucial d'anticiper une attaque en détectant les premiers éléments de sa kill chain dans un contexte où les cybercriminels sont plus déterminés que jamais.

Gatewatcher propose des solutions de détection capables de repérer le plus grand nombre de techniques d'exploitation possible en un minimum de temps. Nos produits offrent à nos clients une Threat Intelligence de pointe et une capacité d'analyse réseau en profondeur, pour leur permettre d'éviter ce qui aurait pu arriver.

NOS SOLUTIONS

Les produits Gatewatcher proposent une **détection à 360° des cybermenaces**.Ils combinent des **algorithmes d'apprentissage automatique** avec différentes méthodes d'**analyse du trafic réseau**. Ils sont conçus pour être **scalables** et **immédiatement opérationnels**.

Les solutions de détection Trackwatch® et Gatewatcher NDR ont la **qualification élémentaire de l'ANSSI** et garantissent une forte résilience aux offensives dirigées contre elles. Ce visa de sécurité vous permet de mettre vos systèmes d'informations en **conformité à la LPM**.

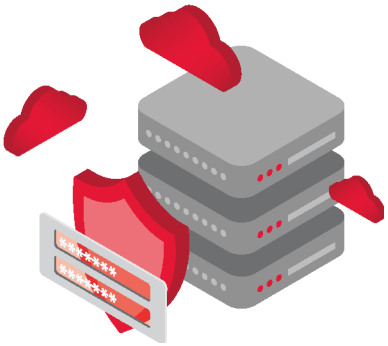
DUALWATCH

Gartner, 2019 « *IDPS / IDS offers the best detection efficacy and performance network security* ».

L'IDS next-gen Dualwatch se déploie en toute simplicité et diminue immédiatement le risque cyber au sein de votre organisation.

Il analyse statiquement et dynamiquement votre réseau et prévient d'un large panel d'attaques, des plus simples aux plus complexes. Dualwatch peut s'interconnecter avec un MISP et recevoir des sources extérieures de Threat Intelligence, vous apportant de la flexibilité face à l'évolution des menaces.

BÉNÉFICES



- Augmentation immédiate de la visibilité sur les réseaux surveillés.
- Intégration simple et rapide sur vos systèmes d'information. Importante granularité des appliances (de 10Mbps à 40Gbps stackables).
- Paramétrage simplifié.
- Gestion centralisée du parc d'IDS depuis une seule interface de management.
- Threat Intelligence extensible, connecteur MISP fonctionnel.
- Apport de données contextuelles pour chaque alerte.

TRACKWATCH

Trackwatch® est la plateforme de détection on-premise qui vous alerte en temps réel des menaces les plus avancées.

La plateforme est opérationnelle dès sa mise en place. Elle combine des algorithmes d'apprentissage automatique identifiant les manœuvres inconnues avec plusieurs méthodes d'analyse du trafic réseau (statique, dynamique et heuristique). Trackwatch® offre une visibilité accrue sur les actions malicieuses en cours et contextualise chaque alerte par la reconstitution de nombreuses métadonnées sur les protocoles.

Deux versions produit :

Critical Infrastructure Edition
Conformité & Détection

Full Edition
Détection avancée des menaces

BÉNÉFICES

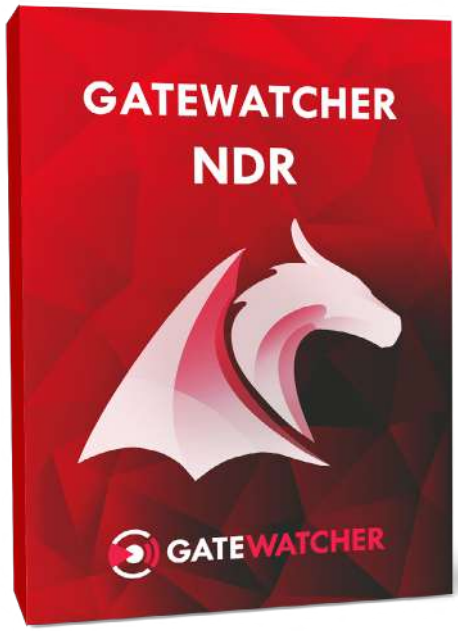
Capacité de prédétection sur l'ensemble de la kill chain d'une attaque :

- Reconstitution et analyse exhaustive des payloads et des fichiers.
- Alerting dès les premiers signes de compromission (Nmap, shellcode, one-liner).
- Identification et contextualisation des menaces de type ransomware, malware, botnet...
- Détection d'attaques complexes par ML : script powershell malicieux, communication de malware par DGA.

Efficience du SOC optimisée :

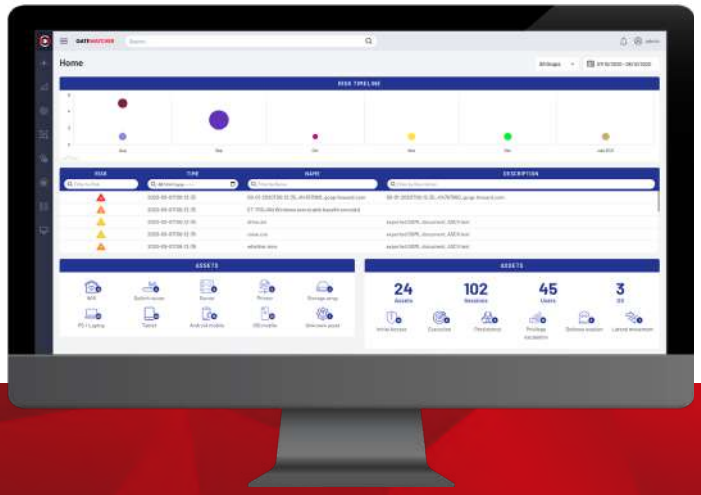
- Génération de métadonnées contextuelles facilitant le travail d'investigation des analystes.
- Raccourcissement du temps de remédiation.
- Interopérabilité avec des EDR et d'autres technologies bloquantes.
- Réduction des coûts d'exploitation du SOC.

GATEWATCHER NDR



Gatewatcher NDR est la nouvelle solution proposée par Gatewatcher pour détecter les menaces les plus récentes et les actions internes malicieuses. Cette nouvelle plateforme Network Detection and Response vous permet, à l'aide d'un seul et même produit, de découvrir les anomalies et comportements suspects au sein de votre infrastructure.

Gatewatcher NDR augmente les capacités de détection comportementale de Trackwatch® par l'ajout d'un UEBA ouvrant un nouvel horizon de possibilités : mise en avant de la relation USER-Entity pour cartographier la totalité des assets, visibilité totale de la kill chain d'une attaque, réduction drastique des faux-positifs etc...



BÉNÉFICES

- Détection d'anomalies sur le réseau y compris dans les flux chiffrés (TLS).
- Détection de ransomware de nouvelle génération et d'exfiltration de certains fichiers.
- Détection avancée des C&C : analyse détaillée des flux utilisés pour le beaconing.
- Gestion des assets et des users, vision agrégée par risque, réduction du bruit.
- Modélisation des risques par une matrice MITRE.
- Automatisation de la capacité de réponse : interopérabilité avec des SOAR.

GBOX

La GBox est notre réponse aux analystes en SOC et CERT qui veulent prendre rapidement la bonne décision grâce à une analyse avancée d'échantillons.

La Gbox est plus qu'une simple sandbox : elle regroupe 4 analyseurs et 16 moteurs anti-malwares pour investiguer à 360° des échantillons qui lui sont soumis. L'ensemble des actions est tracé puis reporté. L'analyste peut valider l'interprétation fournie pour évaluer la gravité de l'attaque. La GBox est interopérable avec nos solutions Trackwatch® et Gatewatcher NDR.

- Inspection rapide et complète des échantillons facilitant l'analyse forensic.
- Génération rapide d'IOC pertinents pour alimenter votre Threat Intel.

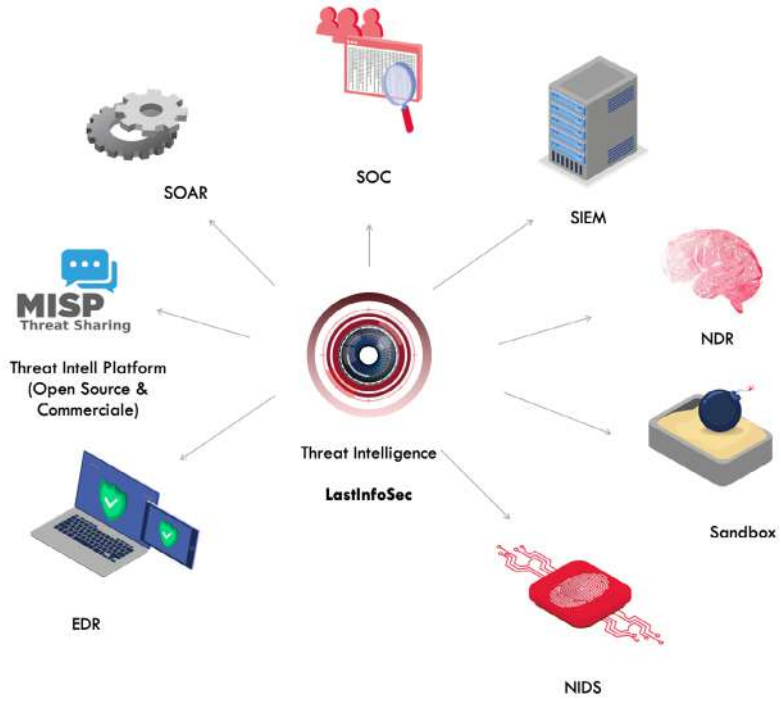
LASTINFOSEC

LastInfoSec est une offre de flux de Threat Intelligence de Gatewatcher améliorant immédiatement la cybersécurité des organisations.

Les données qualifiées et enrichies de LastInfoSec sont déployables dans toute infrastructure critique et augmentent l'efficacité des solutions en place et des équipes cyber.

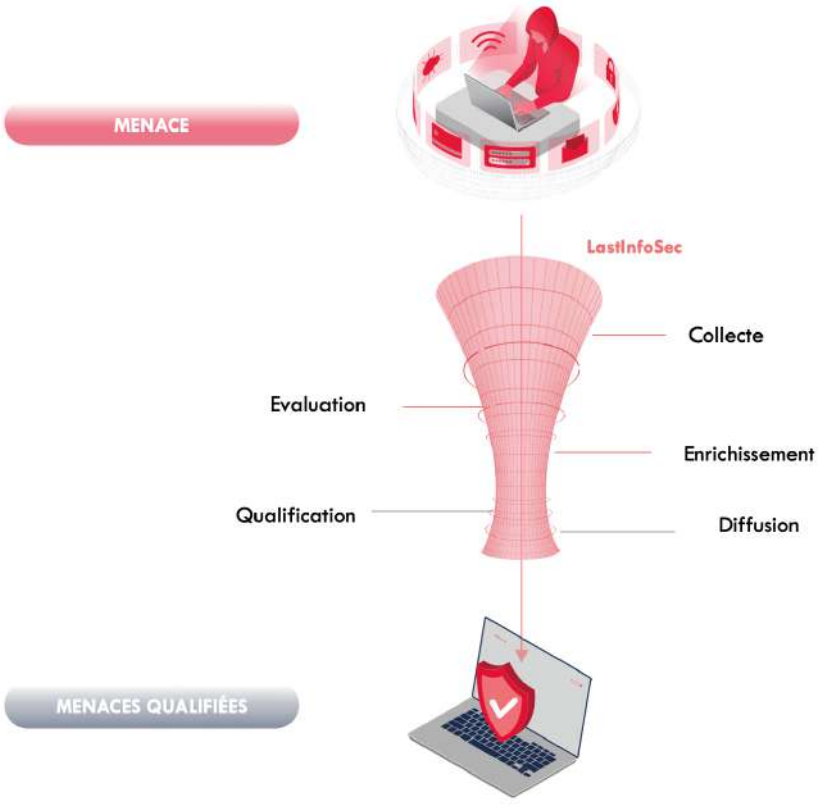
LastInfoSec possède une bibliothèque de plus de 2 millions d'IOC et garantit une mise à disposition 24H avant ses concurrents. L'automatisation est au cœur de la R&D de LastInfoSec.

La Threat Intelligence LIS est disponible aux formats standards (JSON, CSV, STIXV1, STIXV2, MISP, Suricata) et est compatible avec toutes les solutions existantes.



BÉNÉFICES

- Connaissance et couverture de la menace.
- Réduction des délais de détection.
- Réduction des faux-positifs.
- Gain de temps dans l'analyse des événements cyber.
- Prises de décisions fiables et documentées.
- Facilité de déploiement et amélioration immédiate du niveau de sécurité.



CAS D'USAGE

Identifier en temps réel une attaque par ransomware

Les attaques par ransomware font exécuter à la victime un logiciel chiffrant les données et demandant une rançon. Si reconnaître un ransomware est aisé lorsqu'il est passé à l'action, le déceler en amont est bien plus difficile. Les pirates camouflent systématiquement les différents composants de leur attaque afin de contourner les défenses en place.

Les modules au sein de Trackwatch® sont capables de détecter des éléments propres à ces attaques : récupération de la clé sur un C&C, identification de flux SMB suspicieux ou détection de pièces jointes malicieuses dans un email. La plateforme vous donne l'avantage pour réagir le plus tôt possible.

- Détection des mouvements silencieux sur le SI et des techniques d'exploitation obfusquées.
- Détection des ransomwares avant leur exécution.
- Évite une perte de contrôle de votre SI et les dommages financiers / de réputation.

Réagir aux premiers signes d'une attaque

Votre société est attaquée : vous subissez une demande de rançon, des coupures de production, vos informations confidentielles circulent publiquement... Cette situation est souvent le résultat d'une opération malveillante débutée des semaines plus tôt à votre insu. Pour éviter un scénario catastrophe, il faut anticiper : cela passe par une bonne visibilité sur votre réseau.

Trackwatch® est la seule solution du marché qui couvre l'ensemble du déroulement d'une cyberattaque avancée et repère les techniques d'exploitation utilisées tout au long de celle-ci.

- Identification d'un attaquant dès son passage sur le réseau.
- Niveau de détail avancé sur l'attaque : utilisateur cible, ouverture de socket, détail en profondeur dans le code...
- Gain de temps pour prendre les mesures de rétention.

Remplacer votre parc IDPS par une plateforme Trackwatch

Trackwatch® garantit une qualité de détection supérieure à celle de vos IDPS en vous épargnant les faux positifs et des paramétrages chronophages. Elle allie Threat Intelligence de qualité et machine learning pour une détection pertinente. Notre plateforme analyse exhaustivement votre trafic et vous alerte des vraies attaques, grâce à la génération de métadonnées qui permettent de les contextualiser et de réduire le bruit.

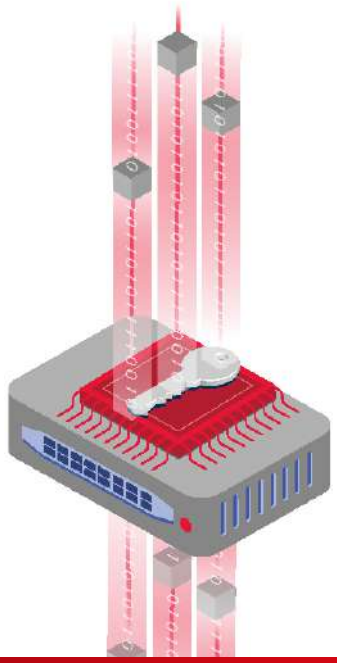
- Trackwatch® conduit une analyse statique et dynamique des binaires et des fichiers pour traquer toutes les techniques d'exploitation.
- Connecteur MISP donnant l'accès à toute la Threat Intelligence du marché.
- Trackwatch® a la qualification élémentaire de l'ANSSI qui garantit une base logicielle durcie, l'absence de backdoors et la maîtrise de vos données.

Détection de méthodes d'exploitation dans un environnement de flux chiffrés

Le chiffrement des flux est en augmentation, face à ce changement se pose la question de la détection des menaces. Trackwatch® est efficace au sein de ce type d'environnement.

La solution vous permet de traquer toutes les actions trahissant la présence d'un attaquant à couvert derrière des flux chiffrés : scans, payloads d'exploitation, tentatives de connexion, fingerprints (empreintes réseau), communications vers les C&C (DGA).

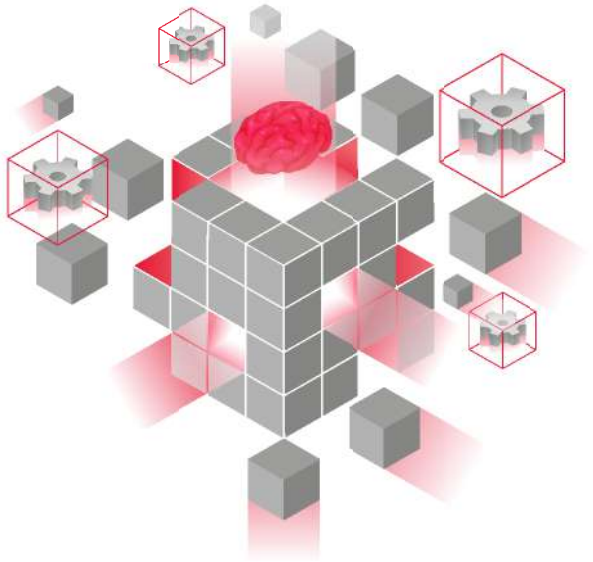
Même si vos flux applicatifs sont chiffrés, ces liens ne sont pas tous utilisables tels quels pour mener une attaque. Pour se propager, l'attaquant devra rechercher de nouvelles machines, trouver des services ouverts et tenter d'exploiter des vulnérabilités. La plupart de ses agissements se fera en clair : ils pourront donc être distingués des flux légitimes.



Optimiser vos solutions de cybersécurité avec LastInfoSec

Le flux de Threat Intelligence 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.



Identifier les violations des politiques de sécurité

Trackwatch® est l'outil idéal pour la mise en application et le contrôle de votre politique de sécurité de façon rigoureuse et déterministe. Trackwatch® vous apporte une cartographie et un inventaire de l'ensemble de votre trafic réseau. A partir de ces informations, votre équipe SSI peut établir les événements redoutés et mettre au point la politique de sécurité.

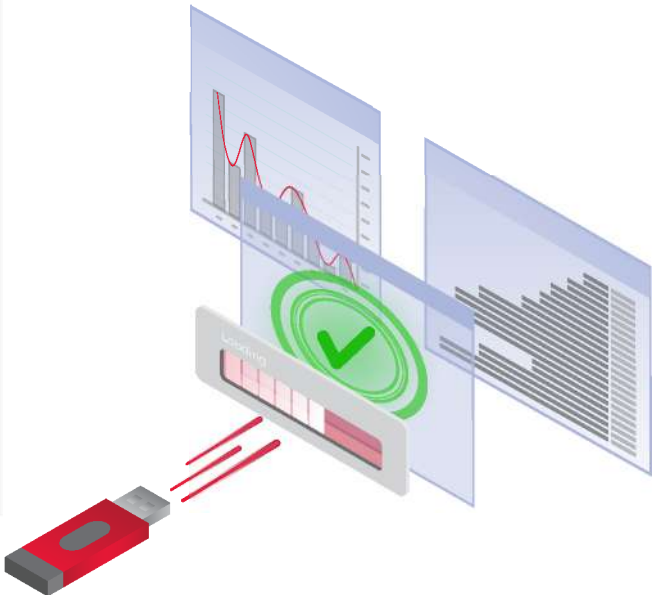
L'implémentation dans Trackwatch® de votre politique se réalise par la rédaction d'un ensemble de règles issues de la cartographie. La mise en place est immédiate et permet un contrôle également immédiat.

- Le résultat opérationnel est un contrôle exhaustif et sans aléas de votre trafic.
- Toute tentative de violation de votre politique de sécurité sera immédiatement remontée par une alerte.

Sécuriser vos supports mémoires et vérifier vos binaires avant utilisation

Les fichiers rentrent dans votre infrastructure de bien des manières. Il est recommandé de faire analyser le contenu d'une clé USB, d'un disque, d'un téléchargement chiffré avant de l'ouvrir.

La solution Trackwatch® permet à tout utilisateur de faire analyser de tels fichiers par un simple glisser/déposer. Et ainsi d'avoir accès à la puissance de détection de nos 16 moteurs antivirus et de notre moteur de détection de shellcodes encodés.



PARTENAIRES TECHNOLOGIQUES

SIEM

IBM Radar, RSA, splunk>

Des technologies SIEM pour corréler nos métadonnées et nos alertes avec d'autres solutions pour créer des scénarii d'attaques et de défense.

FIREWALL

FORTINET, websense, paloalto, f5

Des technologies firewall. Ces équipements interrogent nos moteurs de détection en cas de doute. L'information est renvoyée à ces équipements pour bloquer le plus rapidement possible les menaces les plus obfusquées.

EDR

HARFANGLAB

Des technologies EDR pour garantir une visibilité du réseau et des systèmes en apportant automatiquement des données contextuelles enrichies.

MONITOR

Nagios, centreon

Des technologies de monitoring pour enrichir les écrans de supervision réseau et de sécurité.

MICRO-SEGM.

illumio

Des technologies de micro-segmentation pour analyser des flux applicatifs.

IoT & OT

NOZOMI NETWORKS

GATEWATCHER et NOZOMI ont développé ensemble une solution unique pour créer une vision unifiée de la cybersécurité de l'IT et de l'OT.

VISIBILITE ET CAPTURE CLOUD

ixia, Gigamon

Des technologies « support » à TRACKWATCH® comme des agrégateurs, des solutions de déchiffrement des flux et de capture dans le cloud (AWS, Azure, GCP, Alibaba Cloud).

GATEWATCHER

75, Boulevard Haussmann
75008 PARIS
www.gatewatcher.com

@GATEW4TCHER
GATEWATCHER
contact@gatewatcher.com
+33 1 44 51 03 93