TRACKWATCH®

Machine capability enhanced by human insight 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.

La solution Trackwatch : Une plateforme intelligente pour détecter et analyser en temps réel les menaces et intrusions les plus avancées

Analyse en profondeur des fichiers
Trackwatch® détecte tout type de malwares par une analyse procédée par plusieurs moteurs anti-virus. La plateforme peut analyser jusqu'à 6 millions de fichiers par 24 heures.

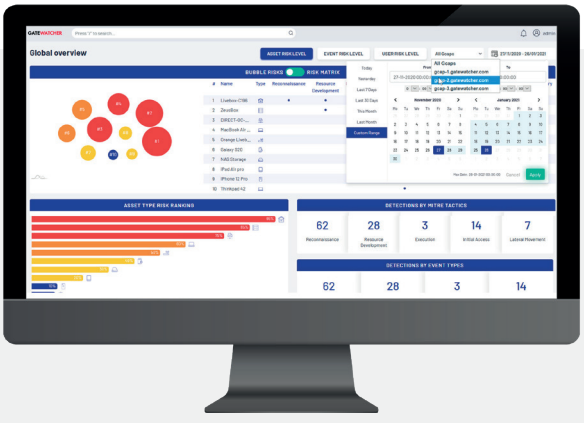
Contrôle des payloads
Trackwatch® conduit une analyse protocolaire poussée sur les paquets afin de les comparer aux signatures d'attaques connues et permet la détection des shellcodes polymorphes, et de tous payloads encodés.

Meilleure visibilité sur les menaces dissimulées
Trackwatch® embarque des algorithmes d'IA permettant la détection d'attaques complexes à repérer (scripts PowerShell malicieux, attaques par DGA, flux SMB dans des scénarios d'attaques par ransomware…).

Alerte dès les premiers signes d'une attaque
Trackwatch® détecte les signaux faibles des attaques fileless et des menaces avancées non encore repertoriées, grâce à une analyse multi-vectorielle des flux réseaux : statique, dynamique et par machine learning.

Trackwatch® allie une analyse poussée des flux à des méthodes novatrices de détection des comportements anormaux sur le réseau. Sa combinaison de plusieurs technologies de détection permet à la plateforme de s'adapter en permanence aux menaces polymorphes, garantissant une très forte pertinence face à la sophistication croissante des attaques persistantes avancées (APTs).

Opérationnel dès sa mise en place, Trackwatch® associe des algorithmes d'apprentissage automatique identifiant les manœuvres inconnues avec plusieurs méthodes d'analyse du trafic réseau (statique, dynamique et heuristique). Cette approche offre une visibilité accrue sur les actions malicieuses en cours et contextualise chaque alerte.



Bénéfices utilisateurs

UNE DÉTECTION QUALIFIÉE PAR L'ANSSI

Trackwatch® a reçu la qualification élémentaire de l'ANSSI en 2019. Ce visa certifie la résilience logicielle et matérielle de la gamme, et permet son utilisation par les OIV dans leur mise en conformité à la LPM.

UNE PROTECTION IMMÉDIATEMENT OPÉRATIONNELLE

Trackwatch® n'implique pas d'équipements supplémentaires ou de coûts cachés. La solution se paramètre simplement et détecte immédiatement les intrusions.

UNE FORTE INTEROPÉRABILITÉ AVEC VOS ÉQUIPEMENTS

Trackwatch® propose des possibilités d'interconnexions avec tous les SIEM du marché, ainsi qu'avec un MISP, des EDR, des proxys....

UNE PLATEFORME ALLIANT SCALABILITÉ ET PERFORMANCES

Trackwatch® propose une vaste gamme d'appliances offrant des débits de 10MBPS à 40 GBPS sans aucun compromis sur les performances avec jusqu'a 27000 EPS traitables en burst contre 1200 en moyenne sur le marché.

UNE SOLUTION FLEXIBLE

Trackwatch® peut fonctionner en mode connecté ou entièrement hors ligne pour les réseaux restreints et confidentiels. Vous restez mettre de vos informations. Sa position en dérivation TAP garantie l'absence d'impact sur votre environnement de production.

UNE EFFICIENCE OPTIMISÉE DE VOTRE SOC

Trackwatch®, par sa génération de métadonnées contextuelles, facilite le travail d'investigation des analystes SOC et la gestion de la criticité des alertes en contribuant au raccourcissement du temps de remédiation.

Cas d'usages

Repérer en temps réel une attaque par ransomware :
Trackwatch® est capable de détecter les 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 courriel. 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 d'éventuels dommages financiers ou de réputation

Réagir aux premiers signes d'une attaque ciblée :
Trackwatch® est la seule solution du marché en mesure de couvrir l'intégralité de la Kill Chain d'une cyberattaque avancée et de reperer les technique d'exploitation utilisées tout au long de son déroulement.

- Niveau de détail avancé sur l'attaque : utilisateur cible, ouverture de sockets, analyse en profondeur du code
- Identification d'un attaquant dès son passage sur le réseau

Mettre en conformité ses SIIV avec la loi de programmation militaire :
Intégrant des impératifs de durcissement logiciel et matériel dans sa conception même, Trackwatch® possède la qualification élémentaire de l'ANSSI et vous permet une mise en conformité LPM avec un déploiement simple dans une architecture de type PDIS.

- Une conformité à la LPM simple et performante sur le plan de la détection
- Des produits qualifiés sur le long terme

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. Il offre une cartographie et un inventaire de l'ensemble de votre trafic réseau utiles à votre équipe SSI qui peut établir les événements redoutés et mettre au point la politique de sécurité.

- Toute tentative de violation de votre politique de sécurité sera immédiatement remontée par une alerte
- Un contrôle exhaustif et sans aléas de votre trafic.

Sources : [1] Ponemon, [2] Intitute, [3] Anssi, [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