GATEWATCHER

TRACKWATCH_

Data sheet

Détecter les intrusions ciblant vos infrastructures les plus *sensibles*

Votre entreprise est confrontée à de multiples défis :

Un temps de détection des menaces long, notamment pour les menaces persistantes avancées (APT).

Une évaluation et hiérarchisation complexe de la criticité des alertes remontées par les analystes.

Une surcharge récurrente des équipes d'experts cyber face au nombre de faux positifs.

Une protection de cyber sécurité complexe à adapter à un contexte de menaces très évolutif et sophistiqué.

1,8

nombre moyen d'attaques réussies par an, affectant les organisations françaises.

207

nombre moyen de jours nécessaires à une entreprise pour détecter une brèche de sécurité sur son SI.

53%

des intrusions réussies ne sont pas détectées par les outils de cyber détection déjà en place.

TRACKWATCH : une solution NDR *qualifiée*

VISA DE SECURITE – ANSSI

Conformité

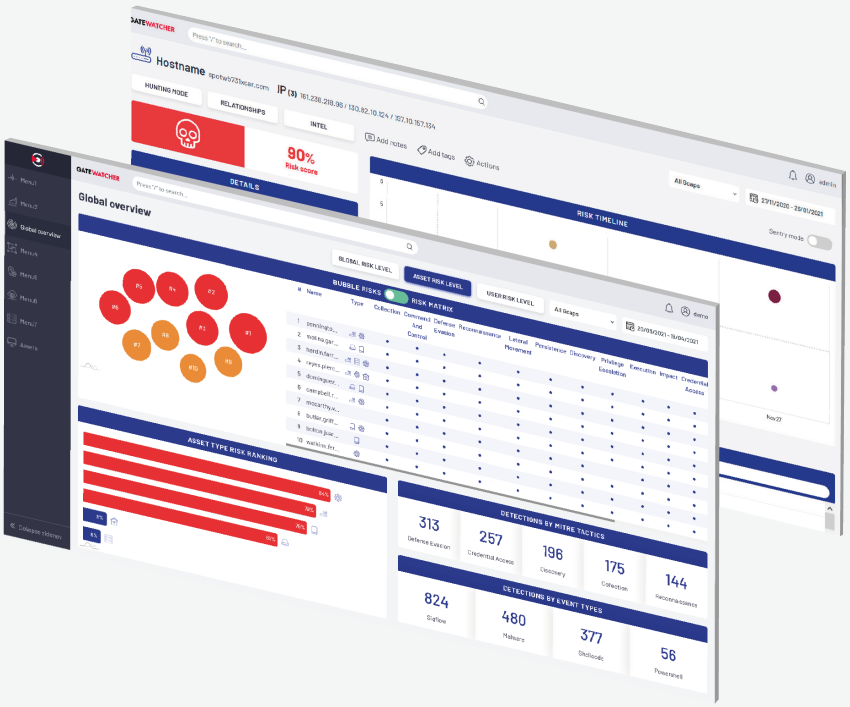
Une solution qualifiée et durcie permet-tant de répondre aux enjeux réglementaires, garantissant une détection efficace même dans le cadre de déploiements hors-ligne (air gap).

Rapidité

Une détection multi-vectorielle permettant une compréhension et remédiation au plus tôt des différentes tentatives d'intrusion grâce à l'analyse intelligente dès les premiers signaux faibles.

Contrôle

Une solution de détection sans impact business s'intégrant dans un écosystème existant afin de maximiser l'efficacité des analystes (SOC).



*easy as_*

NDR

Bénéfices utilisateur

Une *détection* des menaces, y compris en cas de flux chiffrés

Bénéficiez d'une meilleure visibilité sur les menaces dissimulées grâce à leur analyse par une combinaison de moteurs de détection (statique, heuristique, comportementale et contextuelle par machine learning).

Une *consolidation* et agrégation des menaces

Disposez de l'intégralité des métadonnées pour permettre à vos analystes SOC de gagner en rapidité dans la qualification et remédiation des incidents.

Une *maîtrise* de vos informations (air gap)

Basé sur une large gamme hardware, gagnez en flexibilité par un fonctionnement en mode connecté ou entièrement hors ligne pour les réseaux restreints et confidentiels. Vous restez maître de vos informations. La position en dérivation (TAP) garantit l'absence d'impact sur votre environnement de production.

Une *analyse* avancée des fichiers

Approfondissez votre détection de tous types de malwares par une analyse réalisée par plusieurs moteurs anti-virus. La plateforme peut examiner jusqu'à 6 millions de fichiers par 24 heures, et rétro-analyser des fichiers enregistrés comme suspects après leur passage.

Fonctionnalités

Priorisation globale des menaces_

Sur la base d'un score de risque évolutif en fonction de votre SI, triez rapidement les alertes agrégées et accélérez la prise de décision de vos experts SOC.

Interconnexion flexible avec l'écosystème_

Par le biais de développements spécifiques basés sur les API de notre NDR qualifié, ou par des connecteurs standardisés (EDR, XDR, SIEM,SOAR,NGFW), soyez certain d'être interconnecté avec l'ensemble de l'écosystème.

Plateforme logicielle résiliente face aux cyberattaques_

Renforcez votre résistance aux tentatives de corruption et réduisez votre surface d'attaque grâce à l'OS durci de notre NDR qualifié, développé dans une approche "Secure by design".

Contrôle des payloads même obfusquées_

Enrichissez votre analyse protocolaire et statique sur les paquets en les comparant à des signatures d'attaques connues par plusieurs sources de Threat Intelligence. Assurez une détection précise des shellcodes (y compris polymorphes) et de tous les payloads encodés.

Recherche et anticipation d'exploitations de vulnérabilités_

Facilitez les recherches proactives d'intrusions et le traitement des incidents de sécurité de vos experts SOC qui disposent, avec notre NDR qualifié, de l'intégralité des données et métadonnées issues de l'analyse des communications réseaux.

À propos

Leader dans la détection des cybermenaces, Gatewatcher protège depuis 2015 les réseaux critiques des grandes entreprises et des institutions publiques à travers le monde. Nos solutions de Network Detection and Response (NDR) et de Cyber Threat Intelligence (CTI) détectent les intrusions et répondent rapidement à toutes les techniques d'attaque. Grâce à l'association de l'IA à des techniques d'analyse dynamiques, Gatewatcher offre une vision à 360° et en temps réel des cybermenaces sur l'ensemble du réseau, dans le cloud et on premise.

Nous contacter

contact@gatewatcher.com
www.gatewatcher.com