GATEWATCHER
NDR PLATFORM

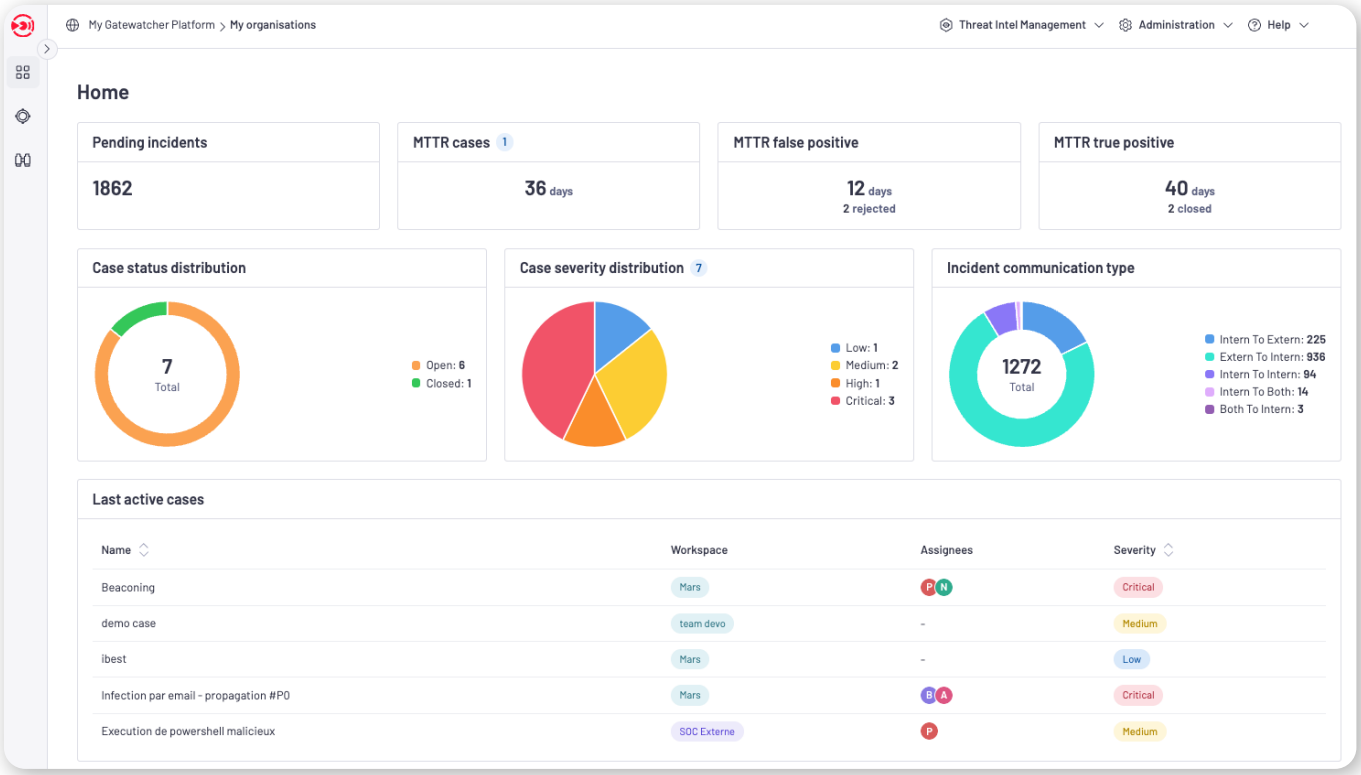
NDR : Le réseau *ne ment jamais*_

Le Network Detection and Response (NDR) fait du réseau *votre première ligne de défense.*

En analysant l'ensemble du trafic en temps réel, le NDR met en évidence les menaces qui échappent aux outils traditionnels : malwares dissimulés, mouvements latéraux et exploits zero-day.

Il fait du réseau le point central de visibilité et de contrôle du S.I. En surveillant et en analysant en continu l'intégralité des flux, il identifie les menaces connues et inconnues, révèle les comportements anormaux et détecte les indicateurs qu'aucune autre solution n'est en mesure d'identifier.

Pour les équipes de sécurité, le NDR offre une détection avancée, une priorisation optimisée des menaces et des investigations simplifiées, réduisant significativement le MTTD et le MTTR. Grâce à une qualification plus rapide, une réponse orchestrée et une intégration native avec les solutions EDR, SIEM, SOAR et au sein des écosystèmes existants, en s'adaptant de manière fluide à leurs évolutions, le NDR renforce la défense globale tout en préservant l'efficacité opérationnelle.



- **Visibilité à 360°_**
  Cartographiez et surveillez l'ensemble des actifs, des utilisateurs et des communications pour une connaissance complète du réseau.

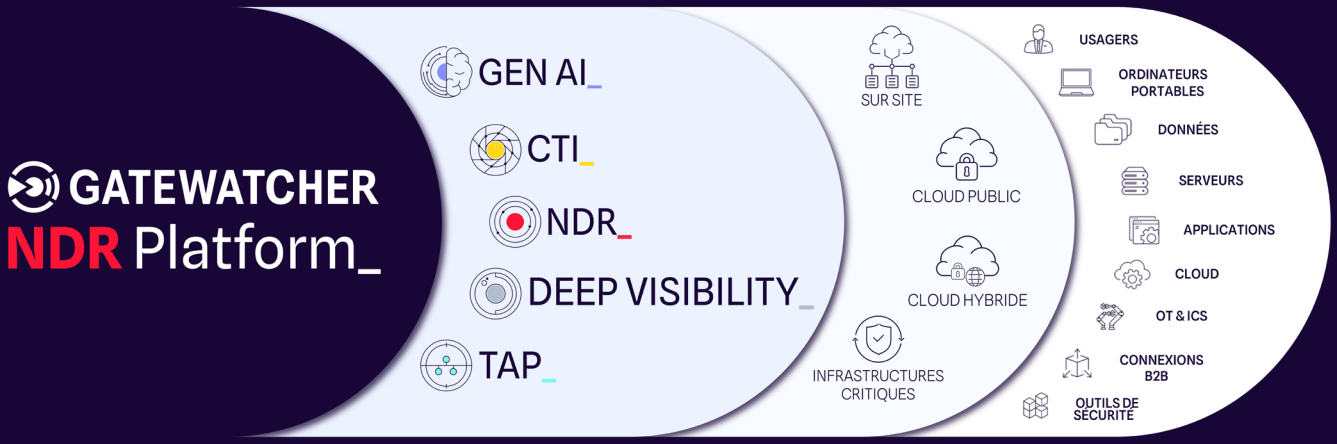
- **Détection multi-vecteurs_**
  Identifiez les menaces avancées grâce à l'analyse intelligente des signaux faibles, qu'il s'agisse de mouvements latéraux ou d'exploits zero-day.

- **Évaluation contextuelle des risques_**
  Hiérarchisez dynamiquement les alertes en fonction du contexte métier et de leur gravité, afin de réduire le bruit et les faux positifs.

- **Intégration transparente à l'écosystème_**
  Interopérez nativement ou via API avec les solutions EDR, SIEM, SOAR, NGFW et bien d'autres, afin de renforcer l'ensemble de votre dispositif de sécurité.

GATEWATCHER
NDR PLATFORM

Gatewatcher propose un écosystème Network Detection & Response complet, conçu pour offrir aux organisations une visibilité totale, une détection accélérée et une réponse décisive face aux menaces avancées.



VISIBILITÉ INTÉGRALE

Assurez une visibilité complète sur l'ensemble du trafic et des actifs réseau, avec un inventaire et une supervision continue sur les environnements IT, OT et cloud pour un contrôle précis et unifié.

DÉTECTION AVANCÉE DES MENACES

Identifiez plus rapidement les menaces avancées et émergentes grâce à un renseignement enrichi qui réduit les faux positifs et renforce la prise de décision.

RÉPONSE ORCHESTRÉE

Coordonnez des actions de remédiation cohérentes et efficaces à travers l'ensemble de l'écosystème de sécurité, en minimisant l'impact et en réduisant les temps de réponse.

EFFICACITÉ OPÉRATIONNELLE ACCRUE

Le SOC autonome de Gatewatcher s'appuie sur l'IA générative pour fluidifier les opérations, réduire la charge des analystes et recentrer leur expertise sur les investigations stratégiques.

UNE PLATEFORME UNIFIÉE : chaque signal devient *clarté*, *contexte*, et *réponse*_

GEN AI : votre assistant cyber basé sur *l'IA générative*_

Les attaquants exploitent déjà l'IA, GAIA en fait une force pour la défense.
Développé par Gatewatcher, cet assistant d'IA générative apporte aux équipes SOC, aux RSSI et aux décideurs un nouveau niveau d'efficacité et de visibilité. Plug-and-play et entièrement interopérable, GAIA s'intègre à votre écosystème pour automatiser les tâches répétitives et permettre aux analystes de se concentrer sur l'essentiel : neutraliser les menaces.

NDR : de la détection à la *remédiation*_

COCKPIT est la tour de contrôle de la plateforme Gatewatcher. Les incidents y sont consolidés, contextualisés et hiérarchisés en alertes exploitables. Les équipes de sécurité gagnent ainsi en clarté et en maîtrise, en se concentrant sur ce qui compte vraiment.
Cependant, visibilité et détection ne suffisent pas : une défense efficace exige aussi une réponse intelligente.

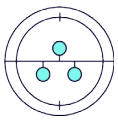
C'est là qu'intervient REFLEX. Intégré nativement à COCKPIT, REFLEX transforme la détection en remédiation en orchestrant des playbooks automatisés et manuels sur les endpoints, les firewalls, les annuaires et les flux réseau. Résultat : une maîtrise plus rapide des incidents, une remédiation cohérente et une posture de sécurité renforcée.

CTI : détecter *avant d'être ciblé*_

Gatewatcher CTI regroupe un ensemble complet de technologies pour vous donner l'avantage du renseignement. Des premiers IoCs aux investigations approfondies et à la protection de l'identité numérique, il fournit un contexte exploitable qui renforce les capacités de détection du NDR, accélère la prise de décision des équipes SOC et maintient l'avance de votre organisation sur ses attaquants.

DEEP VISIBILITY : il est impossible de sécuriser *ce qu'on ne voit pas*_

DEEP VISIBILITY assure une inspection complète du trafic réseau (DPI), offrant une visibilité totale sur les protocoles, les applications, les actifs et les comportements des utilisateurs. Il met en évidence les erreurs de configuration, les problèmes de performance et les connexions non autorisées, aidant les équipes à comprendre qui fait quoi sur le réseau et quels actifs nécessitent une protection renforcée.



TAP : visibilité réseau *continue*_

Les Gatewatcher TAPs capturent 100 % du trafic réseau sans perturbation. Déployés aux points stratégiques, ils transmettent des données en temps réel et infalsifiables au NDR pour une analyse approfondie. Non-intrusifs, plug-and-play et conçus en fail-safe, nos TAPs garantissent une visibilité continue et une sécurité totale sur les infrastructures IT, OT et cloud.

Piloter la cybersécurité avec *Cockpit_*

COCKPIT est la tour de contrôle du NDR de Gatewatcher. Il fournit une visibilité complète et transforme des milliers d'alertes brutes en informations claires et exploitables. Grâce à l'analyse continue du trafic et à une évaluation contextuelle des risques, il permet aux équipes de sécurité de détecter plus rapidement les menaces avancées, de réduire les faux positifs et de se concentrer sur les priorités.

- **Réponse accélérée_**
  Réduisez le délai moyen de détection (MTTD) et le délai moyen de réponse (MTTR) grâce à des flux de travail intégrés et à l'automatisation.
- **Visibilité intégrale_**
  Surveillez et analysez l'ensemble du trafic réseau, y compris les flux chiffrés, avec une clarté totale.
- **Évaluation contextuelle des risques_**
  Hiérarchisez les incidents selon leur gravité et leur impact afin de concentrer vos efforts sur les menaces les plus critiques.
- **Intelligence unifiée NDR & CTI_**
  Corrélez les détections réseau avec le renseignement sur les menaces pour des investigations plus riches et plus précises.
- **Consolidation intelligente des alertes_**
  Transformez des milliers d'alertes brutes en incidents clairs et exploitables, afin de réduire le bruit et les faux positifs.
- **Collaboration fluide_**
  Partagez des informations entre les équipes SOC, les MSSP et les clients grâce à une interface SaaS intuitive et flexible.

SOC AUTONOME DE GATEWATCHER
*l'IA au coeur de la défense_*

Gatewatcher autonomous SOC représente une évolution majeure dans la conduite des opérations de sécurité. Renforcé par l'IA agentique et l'automatisation, il élimine les tâches à faible valeur ajoutée telles que la gestion des faux positifs, le whitelisting récurrent, le reporting et le triage initial.

Son efficacité repose sur la qualité des données. Chaque signal est enrichi, corrélé aux événements passés et futurs, analysé de manière croisée entre protocoles et complété par des sources externes de renseignement, puis validé par plusieurs modèles d'IA pour garantir des verdicts cohérents et fiables.

Cette approche fournit une chronologie complète de l'attaque, permettant une qualification plus rapide et plus précise des incidents, tout en réduisant significativement le MTTD et le MTTR. En automatisant la classification, la corrélation et la remédiation, le SOC autonome libère les analystes des tâches répétitives et leur permet de se concentrer sur l'investigation, la stratégie et la traque proactive aux menaces.

Gatewatcher autonomous SOC renforce la détection, accélère la remédiation et offre un cadre robuste et évolutif adapté a la lutte contre les futurs menaces.

gatewatcher.com

Ahead of *threats*_

Explorer nos solutions...

contact@gatewatcher.com

+33 (0)1 44 51 03 93

Campus Cyber • Puteaux, France

GATEWATCHER

GATEWATCHER Official

@GATEW4TCHER