NOZOMI NETWORKS

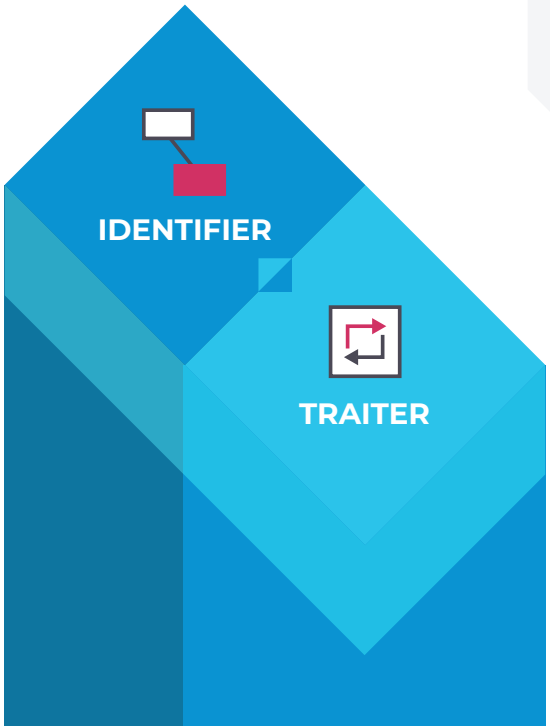
FICHE PRODUIT

Threat Intelligence

Détection des vulnérabilités émergentes et des menaces ciblant les systèmes industriels (OT) et de l'IoT

Nozomi Networks **Threat Intelligence**™ met continuellement à jour les capteurs **Guardian**™ avec des analyses et des données enrichies afin que vous puissiez détecter et traiter plus rapidement les menaces émergentes.

Guardian corrèle les informations sur les menaces avec le comportement de l'environnement afin de maximiser la sécurité.



Voir

Toutes les ressources et tous les comportements des systèmes industriels et de l'IoT sur vos réseaux pour une connaissance sans pareil

Détecter

Cybermenaces, vulnérabilités, risques et anomalies pour un traitement plus rapide

Unifier

Sécurité, visibilité et supervision sur l'ensemble de vos ressources pour une meilleure résilience

Détection

Des renseignements qui réduisent le délai moyen de détection (MTTD)

Détection rapide des menaces et identification des vulnérabilités

Renseignements actualisés sur les menaces

Fournit des renseignements actualisés en permanence sur les menaces et les vulnérabilités des systèmes OT et de l'IoT

Détecte les menaces avancées et les cyber-risques à un stade précoce et avancé

Identifie les ressources risquant d'être attaquées grâce à l'évaluation de la vulnérabilité des systèmes OT et de l'IoT

Indicateurs de menaces étendus

Fournit des informations détaillées sur les menaces :

- Règles de Yara :
- Règles de paquets
- Indicateurs STIX
- Définition des menaces
- Base de connaissances sur les menaces
- Signatures de vulnérabilités

Renforcez considérablement votre posture de sécurité

Informations sur les menaces ciblant les systèmes OT et de l'IoT

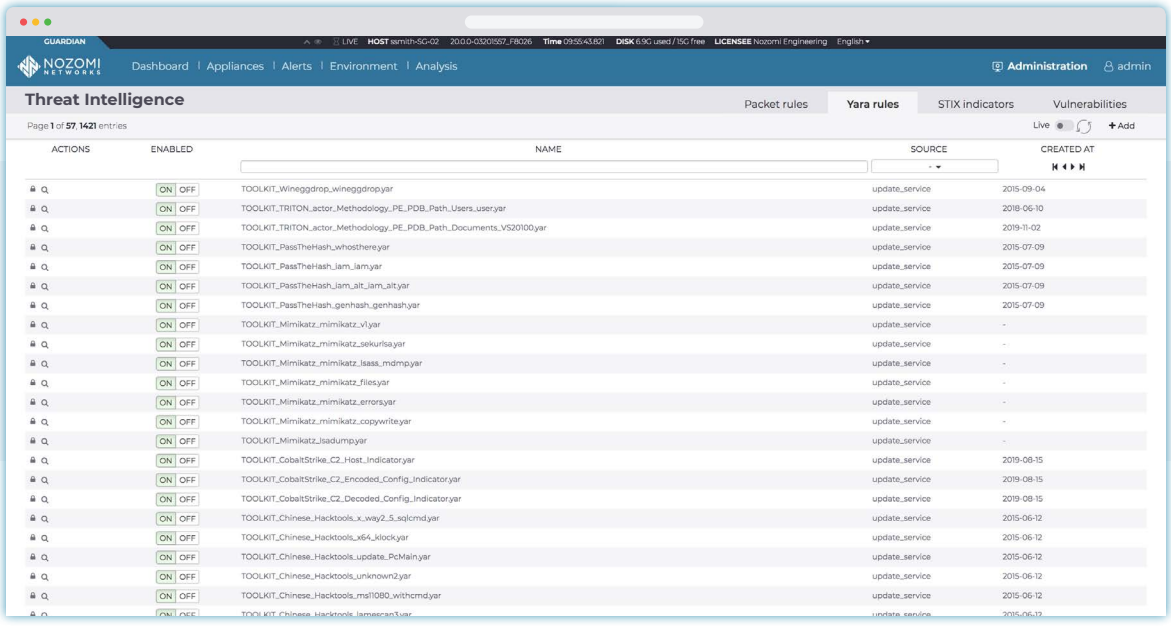
Fournit une évaluation précise de l'état de votre sécurité grâce à une visibilité totale sur le réseau, et des renseignements intégrés sur les menaces

Fournit les informations dont vous avez besoin pour gérer efficacement les risques sur les systèmes OT et de l'IoT

Haute performance pour réduire le MTTD

Analyse des capteurs Guardian pour une détection accélérée des menaces

Transmet des alertes immédiates et fiables regroupées en incidents pour accélérer le traitement



Threat Intelligence fournit continuellement des informations détaillées et à jour sur les menaces.

Traitement

Alertes détaillées et outils d'investigation pour un traitement rapide

Intervenez rapidement grâce à des informations détaillées et fiables

Renseignements fiables sur les menaces

Garantit des informations valides sur les menaces en s'appuyant sur l'expertise de Nozomi Networks Labs, une équipe de chercheurs spécialisés en sécurité

Fournit des règles fiables soumises à des tests rigoureux avant leur diffusion afin de minimiser les faux positifs

Des alertes détaillées et utiles

Fournit des alertes détaillées qui précisent ce qui s'est produit

Regroupe les alertes en incidents, offrant ainsi au personnel chargé de la sécurité et de l'exploitation une visibilité simple, claire et consolidée sur ce qui se passe dans leur réseau

Analysez rapidement les incidents et simplifiez les processus IT/OT

Processus de sécurité informatiques/industriels simplifiés

Réduit les coûts grâce à une évaluation unique et complète des vulnérabilités et de la détection des menaces sur les systèmes OT et de l'IoT

S'intègre à l'infrastructure de sécurité informatique pour optimiser les processus de sécurité, voir : **nozominetworks.com/intégrations**

Harmonise les données de sécurité sur l'ensemble des outils de l'entreprise pour un traitement cohérent

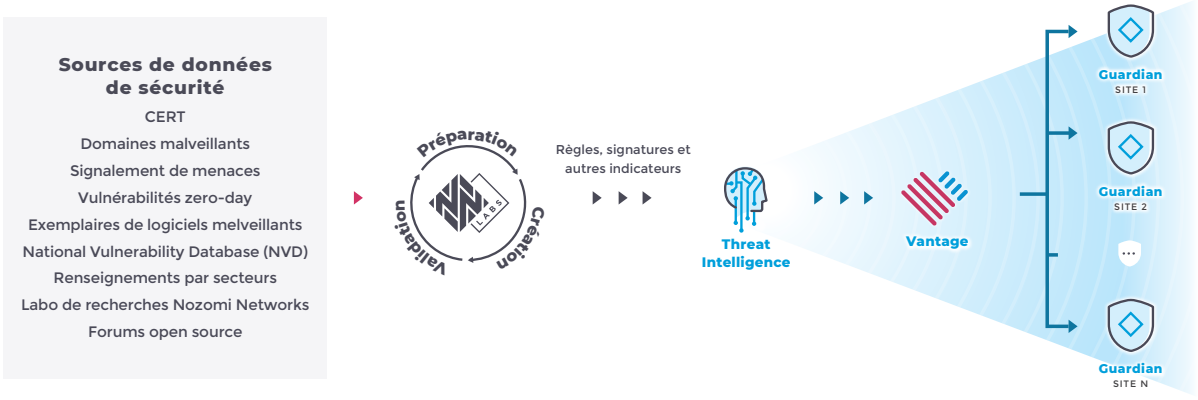
Analyses rapides

Concentre les efforts avec Smart Incidents™ qui :

- Corrèle et consolide les alertes
- Fournit un contexte opérationnel et de sécurité
- Capture automatiquement les paquets

Décode les incidents avec Time Machin™ avant et après les instantanés système

Fournit des réponses rapidement grâce à un puissant outil d'interrogation ad hoc



La **recherche de menaces en continu** réduit le temps nécessaire à la détection des menaces et des vulnérabilités actives.

Produits et services

SAAS

Vantage accélère la transformation digitale grâce à une sécurité et une visibilité sans pareil sur vos réseaux industriels, informatiques, et l'IoT. Sa plateforme SaaS évolutive vous permet de protéger un nombre illimité de ressources en tout lieu. Vous pouvez réagir plus rapidement et plus efficacement aux cybermenaces, ce qui garantit la résilience opérationnelle.

Requiert les capteurs Guardian.

PÉRIPHÉRIE OU CLOUD PUBLIC

La **console d'administration centrale** (CMC) consolide la visibilité et la surveillance des risques sur les systèmes OT et de l'IoT de vos sites distribués, à la périphérie ou dans le Cloud public. Elle s'intègre à votre infrastructure de sécurité informatique pour optimiser les workflow, et traiter les menaces et les anomalies plus rapidement.

ABONNEMENT

Le service **Threat Intelligence** fournit des renseignements en continu sur les menaces et les vulnérabilités des systèmes industriels et de l'IoT. Il vous aide à devancer les menaces émergentes et les nouvelles vulnérabilités, et réduire le délai moyen de détection (MTTD).

PÉRIPHÉRIE OU CLOUD PUBLIC

Guardian fournit une sécurité et une visibilité robuste sur les systèmes OT et de l'IoT. Il combine la découverte des ressources, la visualisation du réseau, l'évaluation des vulnérabilités, la surveillance des risques et la détection des menaces en une seule application. Guardian partage ses données avec Vantage et la CMC.

ABONNEMENT

Le service **Asset Intelligence** fournit des mises à jour régulières des profils pour une détection plus rapide et plus fiable des anomalies. Il vous aide à concentrer vos efforts et réduire le délai moyen de réponse (MTTR).

OPTION POUR GUARDIAN

Smart Polling ajoute une interrogation active de faible volume à la découverte passive des ressources de Guardian, améliorant ainsi le suivi des ressources, l'évaluation des vulnérabilités et la supervision de la sécurité.

OPTION POUR GUARDIAN

Les **Remote Collectors** sont des capteurs nécessitant peu de ressources, qui collectent des données de vos sites distribués et les envoient à Guardian pour analyse. Ils améliorent la visibilité tout en réduisant les coûts de déploiement.

Nozomi Networks

La solution leader de sécurité et de visibilité OT et IoT

Nozomi Networks accélère la transformation digitale en protégeant les infrastructures critiques, les entreprises industrielles et les gouvernements du monde entier contre les cybermenaces. Notre solution offre une visibilité exceptionnelle sur le réseau et les ressources, une détection des menaces et des informations pour les environnements industriels et l'IoT. Les clients comptent sur nous pour minimiser les risques et la complexité tout en maximisant la résilience.

DS-TI-FR-A4-006

nozominetworks.com