NOZOMI NETWORKS

GUIDE

Guide d'achat de solutions d'inventaire des ressources industrielles et des objets connectés destiné aux responsables de la sécurité

La visibilité sur les ressources est le fondement de la cybersécurité des technologies industrielle (OT) et des objets connectés (IoT). L'inventaire des actifs est donc le point de départ, quel que soit le cadre choisit : la norme CEI 62443, le cadre de cybersécurité NIST 2.0 ou les cinq contrôles critiques SANS pour ICS. Pourquoi ? Parce que vous ne pouvez pas protéger ce que vous ne pouvez pas voir.

Avant de pouvoir évaluer les risques, segmenter votre réseau, gérer les vulnérabilités et mettre en œuvre des plans efficaces de réponse aux incidents, vous devez avoir une visibilité sur les éléments de votre réseau et leurs communications.

Pour quelque chose d'aussi fondamental, il existe de grandes différences dans la définition de la « gestion de l'inventaire des ressources » chez les fournisseurs. Si vous faites l'impasse sur cette étape fondamentale, vous risquez de vous retrouver avec une simple base de données d'adresses IP au lieu d'une fondation utile pour votre programme de cybersécurité.

Lisez ce guide pour en savoir plus :

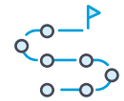
Principaux défis à relever pour réaliser un inventaire complet et fiable des ressources industrielles/ objets connectés

Les cinq piliers à rechercher dans une solution de sécurité de l'inventaire des ressources industrielles

Principales questions à poser lors de l'évaluation des solutions d'inventaire des ressources

Table des matières

Principaux défis d'un inventaire complet et fiable des ressources industrielles/objets connectés



La transformation numérique durant la dernière décennie a augmenté la complexité de l'inventaire des ressources industrielles. Pour améliorer l'efficacité, les environnements d'aujourd'hui connaissent une explosion du nombre et du type de ressources qui élargissent radicalement la surface d'attaque et introduisent de nouveaux défis.

Manque de visibilité

Sans visibilité centralisée sur les ressources dans les environnements industriels, IoT et informatiques, les angles morts vous exposent à des risques.

Différents environnements

Grande variété de fournisseurs, de protocoles et de types d'appareils (automates, unités terminales distantes, capteurs, interfaces hommes-machines, etc.).

Infrastructures et outils hérités

Les équipements plus anciens peuvent ne pas être compatibles avec les outils modernes de surveillance ou de découverte. Les versions de leur micrologiciel et de leur système d'exploitation peuvent être obsolètes ou ne pas pouvoir être corrigées.

Limites de la découverte

L'équilibrage des méthodes de découverte actives et passives permet d'identifier tous les appareils sans perturber les opérations.

Conformité et risques de sécurité

Difficulté de se conformer à des normes telles que NIST CSF 2.0, CEI 62443 ou NERC CIP en l'absence de données et de contexte fiable sur les ressources.

Environnements dynamiques

Les changements fréquents dans l'environnement (par ex. les prestataires qui ajoutent de nouveaux appareils, des ressources mobiles) entraînent une dérive de l'inventaire.

Équipes et outils cloisonnés

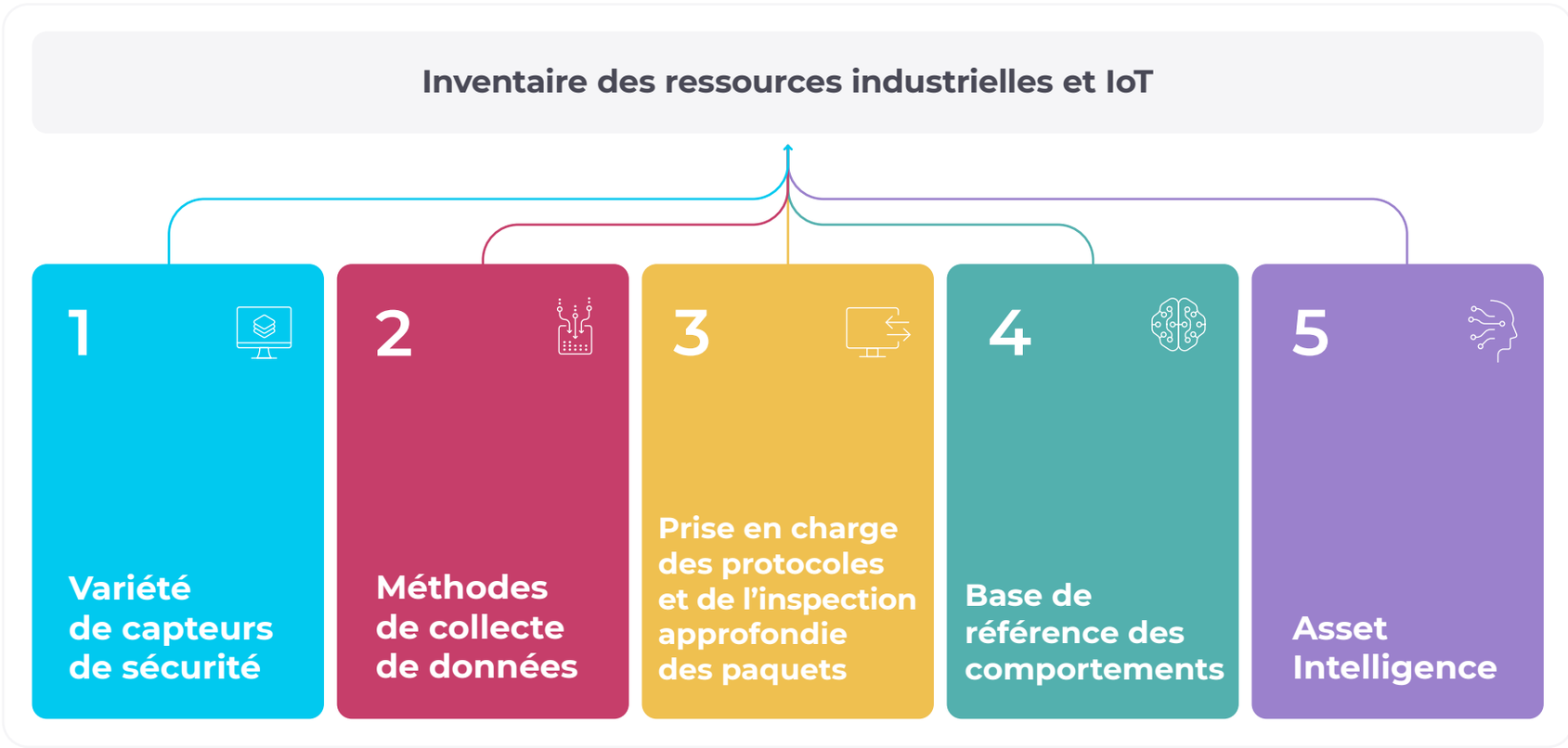
Les équipes informatiques utilisent souvent des outils différents, ont une compréhension limitée des environnements industriels et peuvent ne pas collaborer efficacement.

Contexte incomplet

Les outils de gestion des ressources peuvent ne pas fournir de contexte opérationnel tel que la version du micrologiciel, les schémas de communication ou la pertinence des processus.

5 piliers à rechercher dans une solution d'inventaire des ressources industrielles et des objets connectés

Pour servir de fondation à votre programme de cybersécurité, une solution d'inventaire des ressources doit faire bien plus que découvrir et identifier les ressources. Elle doit également pouvoir fournir des informations approfondies sur le comportement et les communications des appareils. Voici les cinq piliers à évaluer.



1. Variété de capteurs de sécurité

La découverte et l'identification de chaque ressources de votre environnement nécessitent une variété de capteurs au-delà des capteurs réseau traditionnels. Chacun de ces types de capteurs doit être spécialement conçu pour les environnements industriels/ICS afin de lire les protocoles industriels sans perturber les activités.

Capteurs réseau et collecteurs à distance

Les capteurs réseau et les collecteurs à distance extraient passivement, analysent et présentent les données du réseau pour en effectuer la surveillance en continu et détecter toute menace ou anomalie. Les capteurs réseau Guardian observent le trafic local sans agent ni interrogation pour identifier les appareils et surveiller l'activité. Ils comprennent du matériel monté en rack et du matériel durci, ainsi que des formats virtuels, portables et conteneurisés.

De petits collecteurs à distance à faibles besoins en ressources travaillent avec les capteurs Guardian pour extraire des données dans des endroits difficiles d'accès ou sans personnel, tels qu'en pleine nature, en milieu marin et dans des endroits distribués où les capteurs réseau ne sont pas rentables ou pratiques.

Capteurs sans fil

L'explosion des dispositifs connectés sans fil dans les environnements industriels et les infrastructures critiques a considérablement augmenté la surface d'attaque. Les réseaux de contrôle des processus s'appuient sur Wifi, Bluetooth et d'autres protocoles sans fil spécialisés, conçus pour faciliter une communication fiable entre les capteurs et les

Nozomi Networks offre la gamme de capteurs la plus complète du marché avec des capteurs réseau, sans fil et sur terminaux.

CAPTEURS RÉSEAU

GUARDIAN

CERTIFIÉ PAR L'ANSSI

CONFORME À FIPS

REMOTE COLLECTOR

CAPTEURS SANS FIL

GUARDIAN AIR

CAPTEURS DE PROTECTION SUR TERMINAUX

ARC

ARC EMBEDDED

contrôleurs avec une faible consommation d'énergie. Nozomi Guardian Air est le premier capteur sans fil conçu pour détecter non seulement les protocoles Wifi et Bluetooth, mais également Zigbee, LoRaWAN, Drone RF et d'autres protocoles sans fil fréquemment utilisés dans les environnements industriels/IoT.

Capteurs sur terminaux

Dans le domaine de la sécurité informatique, les agents sur terminaux sont omniprésents pour la protection antivirus et l'application de correctifs. Malheureusement, les conséquences négatives du déploiement d'agents informatiques sur des dispositifs industriels ont conduit à une faible adoption de la surveillance des terminaux dans les environnements industriels, qui en ont pourtant bien besoin. C'est tout aussi risqué.

Les solutions traditionnelles de surveillance du réseau ICS surveillent le trafic nord-sud entre les niveaux Purdue ou les pare-feu, mais les communications est-ouest entre les dispositifs au sein d'une zone, en particulier aux niveaux inférieurs de Purdue, ont longtemps été un angle mort. La surveillance des terminaux est le seul moyen de corréler les événements et l'activité des utilisateurs afin de détecter les menaces internes.

Nozomi Arc est un agent de sécurité léger et non perturbateur pour Windows, Linux et MacOS qui comprend les protocoles industriels/IoT sans fonctionner au niveau du noyau du système d'exploitation hôte.

Capteurs intégrés aux terminaux

La visibilité sur le trafic est-ouest aux niveaux 1 et 0 de Purdue est généralement inexistante, y compris sur les contrôleurs industriels et leurs communications. Pourtant, toute perturbation aux niveaux inférieurs de Purdue pourrait avoir un impact direct sur la production.

La première version d'Arc Embedded, développée en collaboration avec Mitsubishi Electric, est disponible pour la famille d'automates MELSEC iQ-R, et d'autres dispositifs OEM sont en cours de développement. Arc Embedded offre une visibilité sans précédent sur les contrôleurs et les équipements de terrain qu'ils contrôlent, jusqu'au niveau 0 de Purdue.

2. Méthodes de collecte de données

Le second élément à rechercher dans une solution d'inventaire des ressources industrielles est une variété de techniques de collecte de données. S'appuyer sur la découverte passive ne suffit pas pour faire face à la sophistication et la fréquence croissantes des menaces industrielles. Vous avez besoin d'une combinaison de techniques de découverte passives et actives, avec la possibilité d'intégrer des données stockées dans d'autres parties de votre système de sécurité.

Découverte passive

La découverte passive via des capteurs réseau est depuis longtemps la norme pour la découverte de ressources industrielles/ICS lorsque les techniques actives de recherche et de sondage ne sont pas appropriées. Elle surveille le trafic réseau sans interagir directement avec les appareils. Imaginez un commutateur réseau observant les schémas de communication : il peut voir quels appareils communiquent, à quelle fréquence et avec quels protocoles. Les capteurs réseau Guardian de Nozomi Networks, associés à des collecteurs distants, sont des outils de découverte passive. Ils surveillent en permanence le réseau pour découvrir les nouvelles ressources connectées.

Découverte active

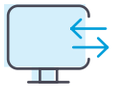
La découverte passive a fait ses preuves, mais elle a ses limites. Elle n'est pas en mesure de détecter les appareils silencieux ou ceux qui ne transmettent pas de données activement. Cela signifie que des risques cachés peuvent passer inaperçus, tels que des dispositifs dormants, des ressources malveillantes ou des terminaux mal configurés, qui ne génèrent pas de trafic réseau mais qui constituent néanmoins une menace pour la sécurité.

La découverte active permet de combler ces lacunes. Il est de plus en plus accepté qu'une visibilité totale est essentielle à la résilience. Elle devient donc une norme dans les réseaux industriels.

Appelée Smart Polling dans la plateforme Nozomi Networks, la découverte active sonde le réseau en envoyant aux appareils des requêtes soigneusement élaborées, telles que des pings réseau ou des requêtes spécifiques à un protocole. Exactement comme si un administrateur système interrogeait activement les ressources connectées pour leur demander de quel type d'appareil il s'agit et les services qu'il propose. L'interrogation active révèle plus de détails sur les appareils, même ceux qui ne communiquent pas, mais elle doit être effectuée avec précaution pour éviter de perturber les opérations critiques.

Intégrations avec des tiers

La plupart des environnements industriels/ICS s'appuient sur des dizaines de solutions technologiques, dont beaucoup capturent de précieuses données qui peuvent ensuite enrichir les inventaires de ressources. La plateforme Nozomi Networks dispose d'une bibliothèque croissante de connecteurs tiers capables d'extraire des données structurées sur les ressources là où elles existent déjà, notamment Microsoft Active Directory, Microsoft Defender, les routeurs et les commutateurs Cisco, CrowdStrike, ServiceNow et d'autres grandes solutions de sécurité informatique.



3. Prise en charge des protocoles et de l’inspection approfondie des paquets

Le troisième élément à évaluer dans une solution d'inventaire des ressources est l’utilité des données collectées pour les opérateurs et les analystes de sécurité. Afin de diagnostiquer les environnements industriels/IoT, vous avez besoin d’une inspection approfondie des paquets et d'une prise en charge complète des protocoles. Cela fournit une visibilité sur toutes vos ressources et vous permet de comprendre ce qu'elles font et avec qui elles communiquent.

Inspection approfondie des paquets

La visibilité sur les variables et les flux des processus est essentielle pour la détection précoce des anomalies. Cela n'est possible avec l’inspection approfondie des paquets pour analyser soigneusement les protocoles industriels propriétaires tels que Modbus ou Profibus. Recherchez des capteurs passifs spécifiques aux réseaux industriels qui utilisent l'inspection approfondie des paquets pour découvrir automatiquement les composants, les connexions et la topologie du réseau, et révéler les menaces.

Prise en charge des protocoles industriels

Les systèmes informatiques communiquent à l'aide de protocoles standard, tandis que les systèmes industriels utilisent un large éventail de protocoles, dont beaucoup sont propriétaires et spécifiques au secteur industriel.

Les profils des appareils seront toujours incomplets si la solution ne peut analyser le trafic réseau et les communications entre les appareils, qui sont des indicateurs clés pour signaler les problèmes potentiels dans votre environnement. Étant donné que les ressources communiquent via leurs protocoles, la maîtrise d'un large éventail de protocoles est essentielle pour comprendre le comportement des ressources. Lorsque votre outil ne prend pas en charge un protocole, vous êtes aveugle aux comportements associés.

La plateforme Nozomi Networks comprend des centaines de protocoles industriels, IoT et informatiques, des plus courants jusqu’aux plus obscurs, et nous en ajoutons constamment. Grâce à notre kit de développement logiciel (SDK), nous pouvons rapidement créer de nouveaux protocoles à la demande.

4. Base de référence des comportements

L'IA et l'apprentissage machine sont essentiels pour établir une base de référence des comportements des ressources et détecter les anomalies. Recherchez un système qui utilise l'IA pour apprendre de votre environnement et établir une base de référence des comportements « normaux », et qui utilise l'analyse des comportements pour surveiller le réseau et alerter en cas d'événements suspects.

Détection automatique grâce à l'IA

Dès son déploiement dans votre environnement, la plateforme Nozomi Networks commence à surveiller les communications des appareils en mode « apprentissage », y compris les variables des processus. Elle utilise l'IA pour créer des profils détaillés du comportement attendu de chaque appareil à chaque étape d'un processus afin d'établir une base de référence du comportement « normal ».

En mode « protection », la plateforme utilise l'analyse comportementale pour surveiller l'environnement et alerter lors des événements suspects qui s'écartent de cette base de référence, tout en filtrant les activités anormales bénignes en deçà des seuils établis. Le comportement devient ainsi un élément essentiel du profil de chaque ressource.

5. Enrichissement par l'IA à partir de l'Asset Intelligence

L'abonnement à un ou plusieurs services de renseignement sur les menaces ciblées (Threat Intelligence) est le meilleur moyen de détecter les menaces connues susceptibles de se trouver dans votre environnement.

De même, un flux de renseignements sur les ressources (Asset Intelligence), qui enrichit les profils des capteurs en complétant les informations manquantes, est le meilleur moyen de disposer de toutes les données disponibles sur vos ressources pour constituer l'inventaire le plus solide et fiable possible.

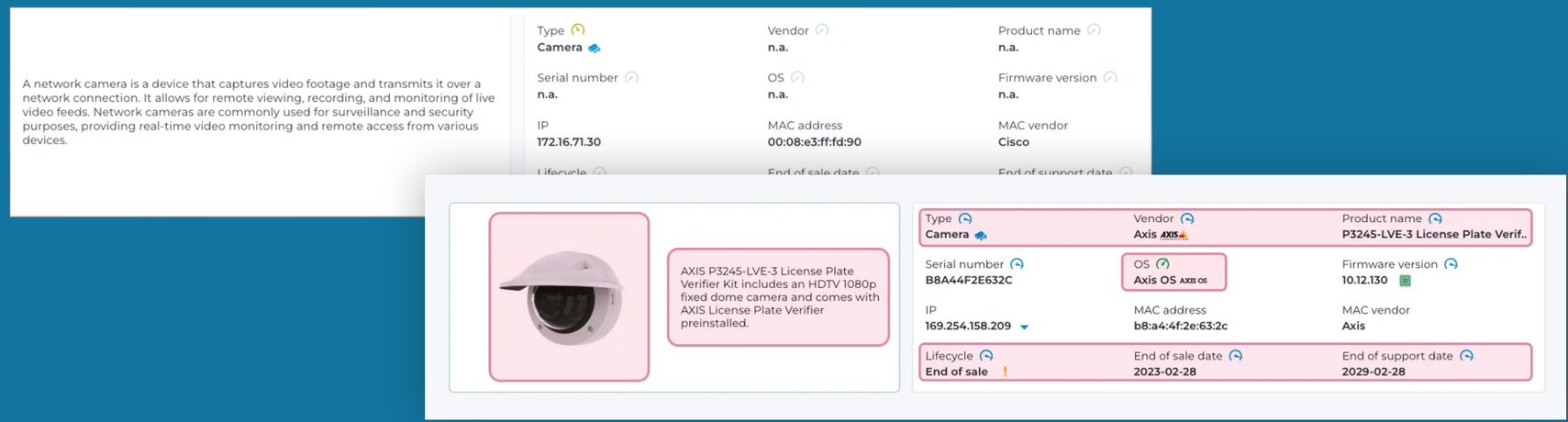
Recherchez un fournisseur qui utilise des données anonymisées sur les ressources de ses clients pour établir une base de profils de ressources, et qui travaille avec un nombre suffisamment important de clients comme vous pour que cela apporte une valeur ajoutée à votre environnement.

Bénéficiez d’une classification fiable à près de 100 % des appareils grâce à des profils enrichis par l'IA

Disponible sous forme d'abonnement, le flux Nozomi Asset Intelligence utilise l'intelligence artificielle élaborée par les ingénieurs de données de Nozomi Networks Labs pour enrichir les profils des appareils avec des informations manquantes, notamment les mises à jour du système d'exploitation et du micrologiciel, les rappels de produits, le statut du cycle de vie et les vulnérabilités connues, ainsi que les codes des fonctions attendues pour comprendre le comportement normal et détecter les anomalies. Ces profils actualisés en continu vous permettent de prendre des décisions éclairées sur la maintenance et la sécurité de vos appareils industriels et vos objets connectés.

Notre moteur d'IA est formé à partir de millions de ressources que nous surveillons dans les environnements de nos clients dans tous les secteurs d'activité à travers le monde.

Ces données sont utilisées pour combler les lacunes d’appareils identiques utilisés dans différents environnements. Lorsqu'une correspondance est trouvée, ces attributs et comportements sont ajoutés au profil de votre appareil. L'équipe de Nozomi Networks Labs ajoute des images et des descriptions de produits à la base de données, ainsi que des énumérations de plateformes communes (CPE), qui sont des identifiants essentiels pour établir une correspondance précise entre les vulnérabilités et les ressources dans votre environnement, et déterminer lesquelles sont importantes. Ces données sont également utilisées pour déterminer les comportements connus, ce qui permet de réduire le nombre d'alertes bénignes et de comprendre quelles « nouveautés » ou « différences » ne sont pas un risque.



Profil des ressources avant et après l'enrichissement par Asset Intelligence

Ne faites pas l’impasse sur l'inventaire des ressources, qui sert de fondement à la cybersécurité

Les réseaux industriels et d'infrastructures critiques contiennent généralement des milliers d'appareils industriels provenant de centaines de fournisseurs, ainsi que des objets connectés, qui surveillent et contrôlent les processus. La création d'un inventaire précis et actualisé de ces ressources et leur suivi, ainsi que les informations contextuelles importantes, sont essentiels à la résilience opérationnelle. Cela ne peut pas être fait manuellement.

À l’aide de capteurs sur terminaux, de la collecte de données passive et active, de la prise en charge des protocoles industriels/IoT et de données sur les ressources informatiques, la plateforme Nozomi Networks fournit un inventaire complet des ressources, dynamisé par des renseignements utiles et enrichis par l'IA. Lorsque vous recherchez une solution d'inventaire des ressources industrielles pour vous aider à progresser sur la courbe de maturité de la cybersécurité, considérez Nozomi Networks comme la référence absolue.

Questions à poser aux fournisseurs

1

Quels types de capteurs sont utilisés sur votre plateforme pour la découverte et la surveillance des ressources ?

2

Quelles méthodes de collecte de données sont utilisées par votre plateforme ?

3

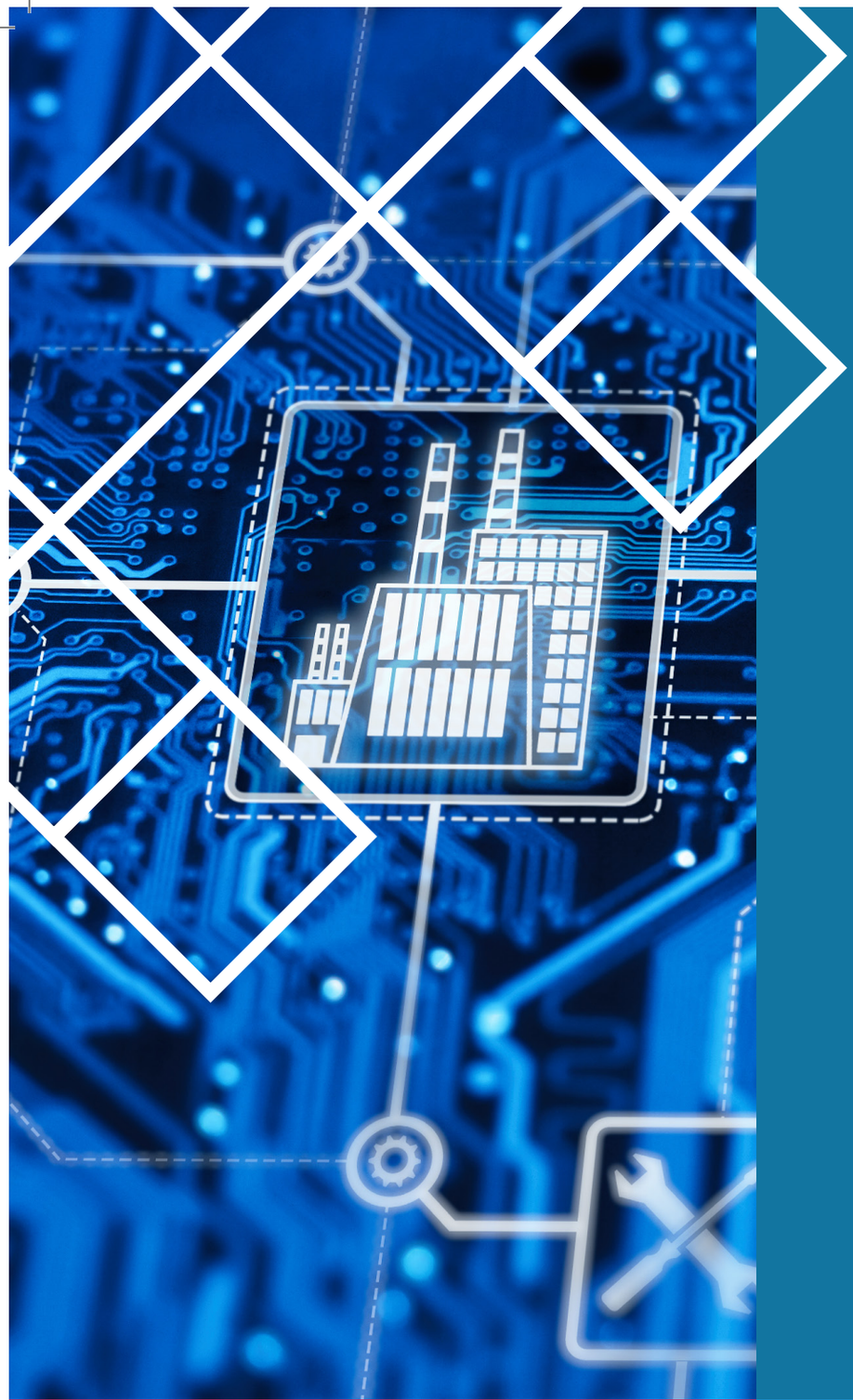
Votre solution utilise-t-elle l’inspection approfondie des paquets pour comprendre le trafic réseau ?

4

Quels protocoles industriels, IoT et informatiques sont pris en charge par votre solution ?

5

Comment utilisez-vous l'IA et **l'apprentissage machine** ?



NOZOMI NETWORKS

ÉTAPES SUIVANTES

Pour en savoir plus sur la façon dont Nozomi Networks peut vous aider à protéger vos systèmes industriels/IoT, rendez-vous sur :

nozominetworks.com

NOZOMI NETWORKS

Cybersécurité pour les technologies industrielles, l'IoT et les infrastructures critiques

Nozomi Networks protège les infrastructures critiques du monde entier contre les cybermenaces. Notre plateforme combine de manière unique une visibilité sur le réseau et les postes, la détection des menaces et l'analyse reposant sur l'IA pour une réponse aux incidents plus rapide et plus efficace. Les clients comptent sur nous pour minimiser les risques et la complexité tout en maximisant la résilience.