NOZOMI NETWORKS

PRÉSENTATION DE SECTEUR

Fabrication : Amélioration de la résilience opérationnelle grâce à la sécurité et la visibilité OT et IoT

Table des matières

1. Introduction

Amélioration de la résilience opérationnelle grâce à la sécurité et la visibilité sur les ressources industrielles et de l'IoT

La pandémie de COVID-19 a accéléré la transformation digitale dans le secteur manufacturier. L'innovation et l'automatisation sont essentielles pour maximiser la croissance, mais les nouvelles technologies digitales augmentent également l'exposition aux cybermenaces qui peuvent perturber les activités.

Les solutions avancées qui offrent une cybersécurité et une visibilité en temps réel sur les réseaux industriels réduisent considérablement les risques et renforcent la résilience de la production.

L'arrivée de petits concurrents agiles dans le secteur de la fabrication pousse les acteurs établis à répondre aux attentes des consommateurs de l'ère digitale. Pour être compétitives, les entreprises doivent déployer de nouvelles technologies tirant parti des systèmes et des chaînes logistiques interconnectés, de l'intelligence artificielle pour la maintenance prédictive et des tendances à la personnalisation de masse.

La crise de l'emploi dans le domaine de la cybersécurité ne fait qu'aggraver le problème. Si l'automatisation réduit le nombre de postes peu qualifiés et accroît la productivité opérationnelle, l'augmentation de la connectivité au niveau de l'usine fait peser sur le réseau des menaces qui nécessitent un nouvel ensemble de compétences sur les technologies informatiques/industrielles.

Du point de vue de la cybersécurité, les fabricants sont traditionnellement restés sous le radar. Les pirates ont d'abord ciblé les infrastructures critiques, telles que l'énergie et les transports, puis la régulation de la sécurité par le secteur et les gouvernements a suivi.

Selon un rapport de 2018 sur la cybersécurité dans le secteur manufacturier, ce dernier est désormais le troisième secteur le plus ciblé, derrière le gouvernement et la finance[1]. Des pirates sponsorisés par des États et des cybercriminels profitent pleinement de cette opportunité. D'après le rapport de Verizon de 2019 sur les fuites de données, les attaques intentionnelles sur la fabrication par des personnes extérieures représentaient 70 % de toutes les failles de sécurité signalées[2].

Les menaces externes ne sont toutefois pas les seuls risques qui empêchent les dirigeants d'entreprise de dormir. Les cyberincidents accidentels et non intentionnels causés par des employés ou des fournisseurs peuvent également avoir un impact sur la productivité. Compte tenu du grand nombre de dispositifs vulnérables et de processus non sécurisés, le risque de faille de sécurité est bien réel. Malgré un manque historique de régulation de la part du secteur, des directives et des réglementations sont en cours d'élaboration.

VERS UNE RÉSILIENCE OPÉRATIONNELLE

Lisez ce document pour découvrir comment une solution unifiée de surveillance et de détection des menaces sur les ressources industrielles et de l'IoT peut être utilisée pour

obtenir une disponibilité, une sécurité et une visibilité opérationnelles.

Les fabricants, notamment dans les secteurs de l'alimentation et des boissons, de la chimie, de la pharmaceutique et de l'automobile, doivent prendre les devants. La première étape consiste à adopter un cadre de cybersécurité favorisant la collaboration des équipes informatiques/industrielles. Grâce à des meilleures pratiques de cybersécurité et la technologie appropriée, les entreprises peuvent protéger leur production, leur personnel et leur réputation, tout en préservant leurs résultats.

2. Principaux défis de l'industrie manufacturière

À mesure que les fabricants s'automatisent et adoptent des technologies digitales, ils sont confrontés aux défis suivants, qui les exposent à des risques commerciaux importants s'ils ne sont pas correctement traités.

2.1 Maintien de la résilience et de la disponibilité opérationnelles

L'interconnectivité entre les réseaux informatiques et industriels ouvre la porte aux cyberattaques. Il en va de même pour la connectivité externe, poussée par l'industrie 4.0 et l'Internet des objets industriels (IIoT). Cela signifie que lorsqu'une chaîne de production s'arrête, les entreprises peuvent perdre des millions en quelques minutes.

Même s'il s'agit du pire des scénarios, les fabricants sont très conscients de l'impact financier potentiel des temps d'arrêt. Pour ce secteur, le maintien d'une disponibilité 24 h/24 est essentiel.

En 2017 par exemple, l'entreprise britannique de biens de consommation Reckitt Benckiser Group a subi une perte estimée à 117 millions de dollars après une attaque de NotPetya. Le logiciel malveillant a entraîné une perturbation généralisée des activités, la perte d'informations et de revenus, et des dommages matériels dans de multiples pays[2]. Qualifiée par beaucoup de cyberattaque la plus dévastatrice de l'histoire, NotPetya a coûté à Reckitt Benckiser 1 % de son chiffre d'affaires annuel, et a infligé 10 milliards de dollars de dommages dans différents secteurs à travers le monde[3].

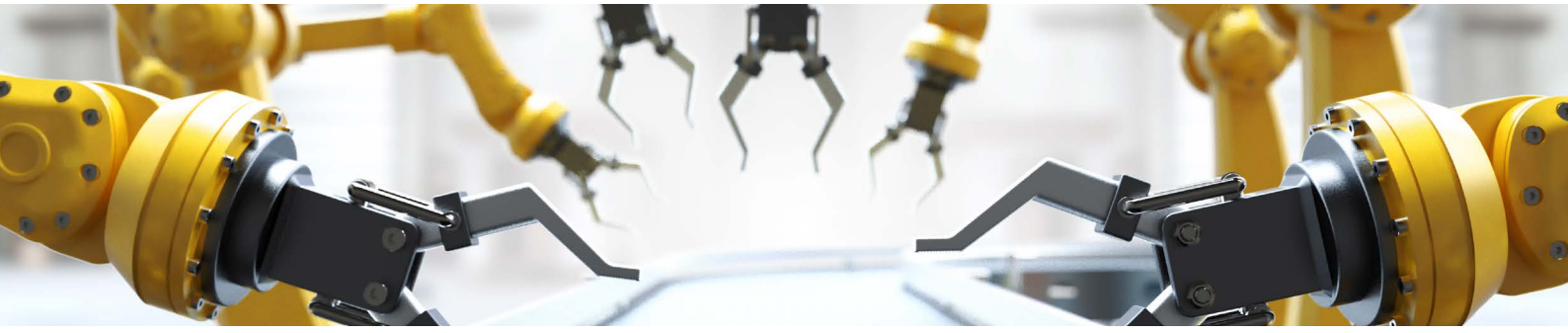
En raison de l'impact que les temps d'arrêt peuvent avoir sur la capacité des fabricants à mettre leurs produits sur le marché, beaucoup d'entre eux choisissent de conserver des stocks supplémentaires comme tactique d'atténuation des risques. Produire et stocker des produits supplémentaires pendant des jours, voire des semaines, est une proposition coûteuse. Elle empêche également les fabricants de recourir à la fabrication en juste-à-temps (JIT), une méthode idéale de contrôle des stocks qui augmente la productivité tout en réduisant les coûts. Au lieu de cela, les entreprises ont été contraintes de retarder la rotation de leurs stocks par crainte de cyberincidents susceptibles de perturber les activités.

LE LOURD FARDEAU DES TEMPS D'ARRÊT OPÉRATIONNELS

Pour l'industrie manufacturière, le maintien d'une disponibilité 24 h/24 est essentiel.

En 2017, l'entreprise britannique de biens de consommation Reckitt Benckiser Group a subi une perte estimée à 117 millions de dollars après une attaque de NotPetya.

Pour protéger les lignes de production, les fabricants peuvent profiter de solutions de détection et d'atténuation des risques industriels qui ne compromettent pas la production.



2.2 Utilisation des bonnes pratiques et d'un cadre de cybersécurité

Les cyberattaques dévastatrices et coûteuses dominent les médias, ce qui amène les fabricants à se demander : « Que se passerait-il si une attaque frappait notre entreprise ? » Qu'il s'agisse de NotPetya, de WannaCry[4] ou de Dragonfly 2[5], ces attaques de logiciels malveillants font des ravages sur la capacité des fabricants à produire, et provoquent des pertes financières massives.

Lorsque les entreprises examinent leur posture et leurs pratiques de sécurité, les cadres dirigeants et les conseils d'administration craignent que, si les fonctions informatiques semblent bien couvertes, aucune visibilité ou protection n'est en place pour l'exploitation. Les équipes industrielles sont poussées par les DSI ou les DSSI à veiller à ce que la propriété intellectuelle, la technologie et les processus de production soient protégés de manière adéquate.

Si le secteur manufacturier y a largement échappé jusqu'à présent, des cyber-réglementations sont désormais élaborées pour presque tous les secteurs industriels. Afin de prendre les devants sur les mandats gouvernementaux, les fabricants doivent travailler rapidement sur les mesures à prendre pour améliorer la cyber-résilience, voire déterminer par où commencer.

Les principaux fabricants étudient et sélectionnent un cadre de cybersécurité à suivre, notamment les normes CEI 62443, NIST ou NIS. Ces cadres offrent des directives pour adopter de bonnes pratiques de cybersécurité et des outils pour faciliter leur mise en œuvre.

LA MEILLEURE PRATIQUE CONSISTE À ÊTRE PROACTIF

Si le secteur manufacturier y a largement échappé jusqu'à présent,

des cyber-réglementations sont désormais élaborées pour presque tous les secteurs industriels.

Après avoir choisi un cadre de référence fiable, les fabricants peuvent identifier les personnes, les processus et les outils nécessaires à une bonne hygiène de cybersécurité. Qu'il s'agisse de constituer un inventaire précis des ressources ou d'identifier des menaces potentielles, les fabricants peuvent suivre les directives et les bonnes pratiques du secteur pour améliorer la résilience de la cybersécurité.

2.3 Obtenir une visibilité sur les réseaux OT et IoT (et les protéger)

Pendant des décennies, les fabricants d'automatismes ont défini leurs propres protocoles réseau propriétaires. Ces dernières années, cependant, l'industrie a pris conscience des avantages des plateformes de connectivité communes pour assurer la compatibilité entre les appareils et protéger correctement leurs systèmes.

ÉLIMINER LES ANGLES MORTS DU RÉSEAU

Pour transformer l'architecture système et obtenir la visibilité requise, les fabricants doivent utiliser les toutes dernières technologies et les bonnes pratiques.

À commencer par un inventaire de toutes les ressources sur le réseau.

Au fur et à mesure que le secteur se transforme, le mélange de nouvelles et d'anciennes infrastructures peut être un défi. Entre les systèmes industriels existants et les nouveaux objets connectés ajoutés sans documentation, de nombreuses équipes n'ont pas une visibilité précise sur ce qui se trouve dans leur réseau. Il n'est pas rare que les fabricants estime avoir 5 000 appareils, alors que leur nombre est plutôt de 10 000. Ce manque de visibilité rend presque impossible la sécurisation et la surveillance des réseaux industriels, et de nombreux fabricants ne savent pas par où commencer.

Pour transformer l'architecture système et obtenir la visibilité requise, les fabricants doivent utiliser les toutes dernières technologies et les bonnes pratiques. À commencer par un inventaire de toutes les ressources sur le réseau. Si l'équipe IT/OT n'a pas de visibilité sur ce qu'elle possède, elle ne peut pas protéger ses ressources ni segmenter le réseau pour améliorer la résilience.

La visibilité améliore également l'efficacité opérationnelle pour réaliser des économies potentielles. Par exemple, un lien réseau inefficace avec une utilisation inhabituellement élevée de la bande passante peut être facilement identifié. Et une fois que l'ensemble du réseau est visible, il peut être surveillé en permanence pour détecter les écarts. Les fabricants peuvent alors facilement repérer les zones vulnérables et les ressources qui ont besoin d'être protégées, et superviser un système efficace et résilient.

2.4 Intégration IT/OT pour empêcher les failles de sécurité

Les cadres dirigeants de l'industrie manufacturière poussent leurs DSSI et VP de l'exploitation à 1) protéger l'entreprise contre les risques et 2) transformer l'exploitation de l'usine en améliorant l'efficacité opérationnelle. Cette transformation ne peut être accomplie que si les technologies informatiques et industrielles travaillent ensemble.

En raison de leurs priorités divergentes, le rapprochement des équipes et des systèmes informatiques et industriels peut ressembler à une bataille difficile. Et comme de plus en plus de systèmes convergent, les points de vulnérabilité et les risques potentiels ne cessent d'augmenter. Les équipes doivent équilibrer leurs priorités concurrentes et tirer parti de l'expertise unique de chacune.

L'équipe informatique peut fournir des conseils sur les problèmes et les processus de cybersécurité. L'équipe industrielle maintien le fonctionnement des systèmes de

LA VALEUR DE LA COLLABORATION IT/OT

Les enseignements de la convergence IT/OT **peuvent optimiser le fonctionnement des usines, améliorer l'utilisation des équipements, permettre la maintenance prédictive et améliorer la cybersécurité.**

production en évitant les temps d'arrêt. Ensemble, ces fonctions permettent une surveillance globale des menaces et une sécurisation des flux de données, afin de réduire les angles morts et minimiser les risques pour la sécurité.

Les informations tirées de la convergence IT/OT peuvent optimiser le fonctionnement des usines, améliorer l'utilisation des équipements, permettre une maintenance prédictive et améliorer la cybersécurité. Et l'impact ne s'arrête pas là. Ces informations contribuent à créer un système plus évolutif, prêt à relever de nouveaux défis logistiques.

En fait, la transformation digitale d'une usine s'étend sur toute la chaîne de valeur, du développement des produits jusqu'à leur distribution (et au-delà). Grâce à une visibilité opérationnelle complète et en temps réel, les usines peuvent augmenter leur productivité et empêcher les failles de sécurité.

3. La solution Nozomi Networks

3.1 Comment la solution Nozomi Networks améliore la résilience opérationnelle

Nozomi Networks aide les fabricants à accélérer le rythme de la transformation digitale en unifiant la détection et la visibilité sur les menaces dans les systèmes OT, IoT, IT et cyber-physiques.

Nous aidons votre entreprise à faire face à l'escalade des cyber-risques sur les réseaux d'exploitation tout en la modernisant pour assurer sa réussite à l'avenir.

PROTECTION DES LEADERS MONDIAUX DE LA PRODUCTION

Nozomi Networks fournit une sécurité et une visibilité OT et IoT aux plus grands sites de fabrication et autres sites industriels dans le monde. Grâce à l'utilisation innovante de l'intelligence artificielle (IA), notre solution automatise le travail difficile d'inventaire, de visualisation et de surveillance des réseaux de contrôle industriel.

Les fabricants bénéficient de la détection et de la visibilité en temps réel sur les menaces, afin d'assurer une cyber-résilience et une fiabilité élevées.

Vous trouverez ci-dessous une brève description de notre gamme de produits. Pour des informations complètes, consultez **notre site web**.

SAAS

Vantage

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 protège 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

Guardian

Guardian fournit une sécurité et une visibilité robuste sur les systèmes industriels 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.

PÉRIPHÉRIE OU CLOUD PUBLIC

Console d'administration centrale

La console d'administration centrale (CMC) consolide la visibilité et la surveillance des risques sur les systèmes industriels 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 workflows, et traiter les menaces et les anomalies plus rapidement.

ABONNEMENT

Threat Intelligence

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).

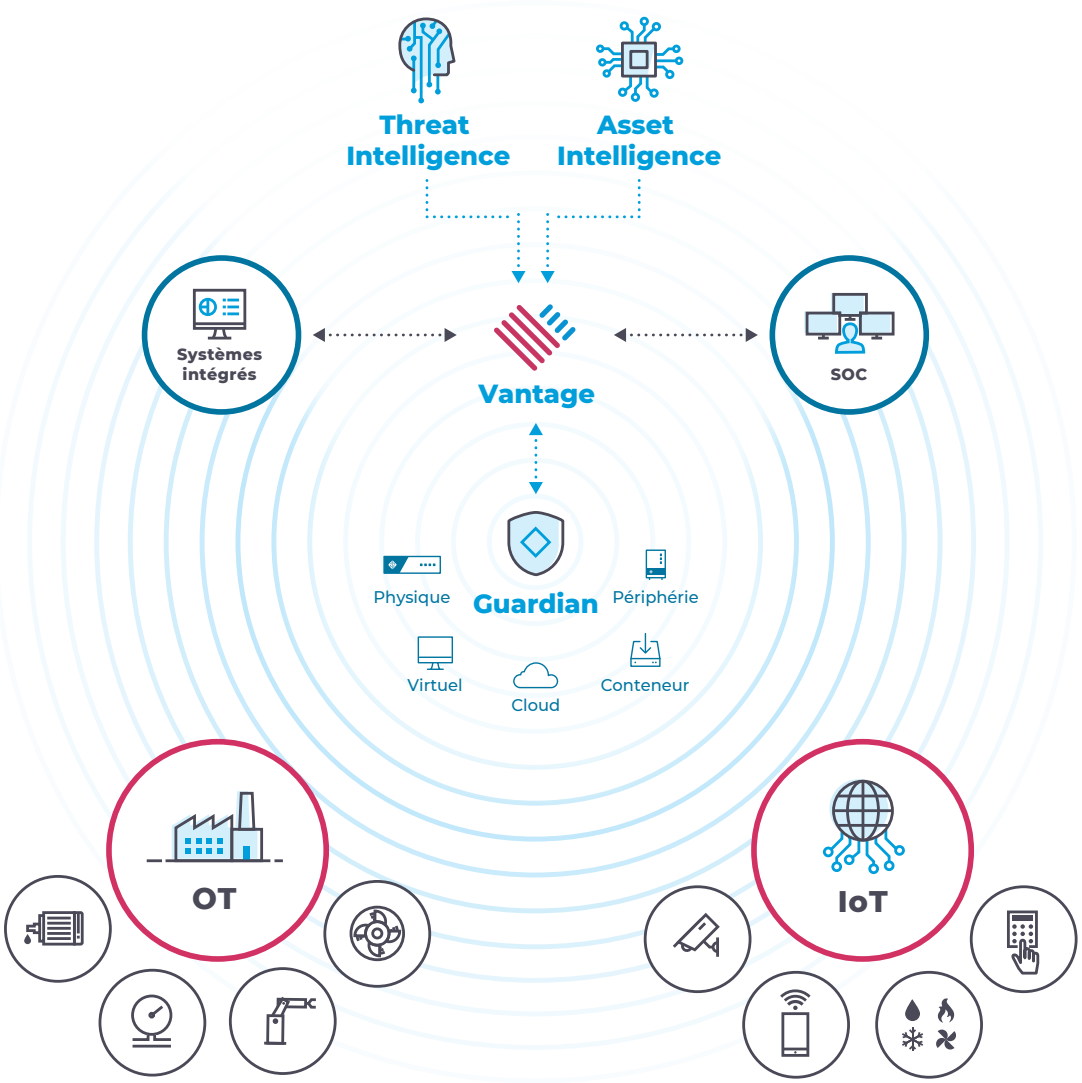
ABONNEMENT

Asset Intelligence

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).

3.2 Diagramme : Sécurité et visibilité OT et IoT

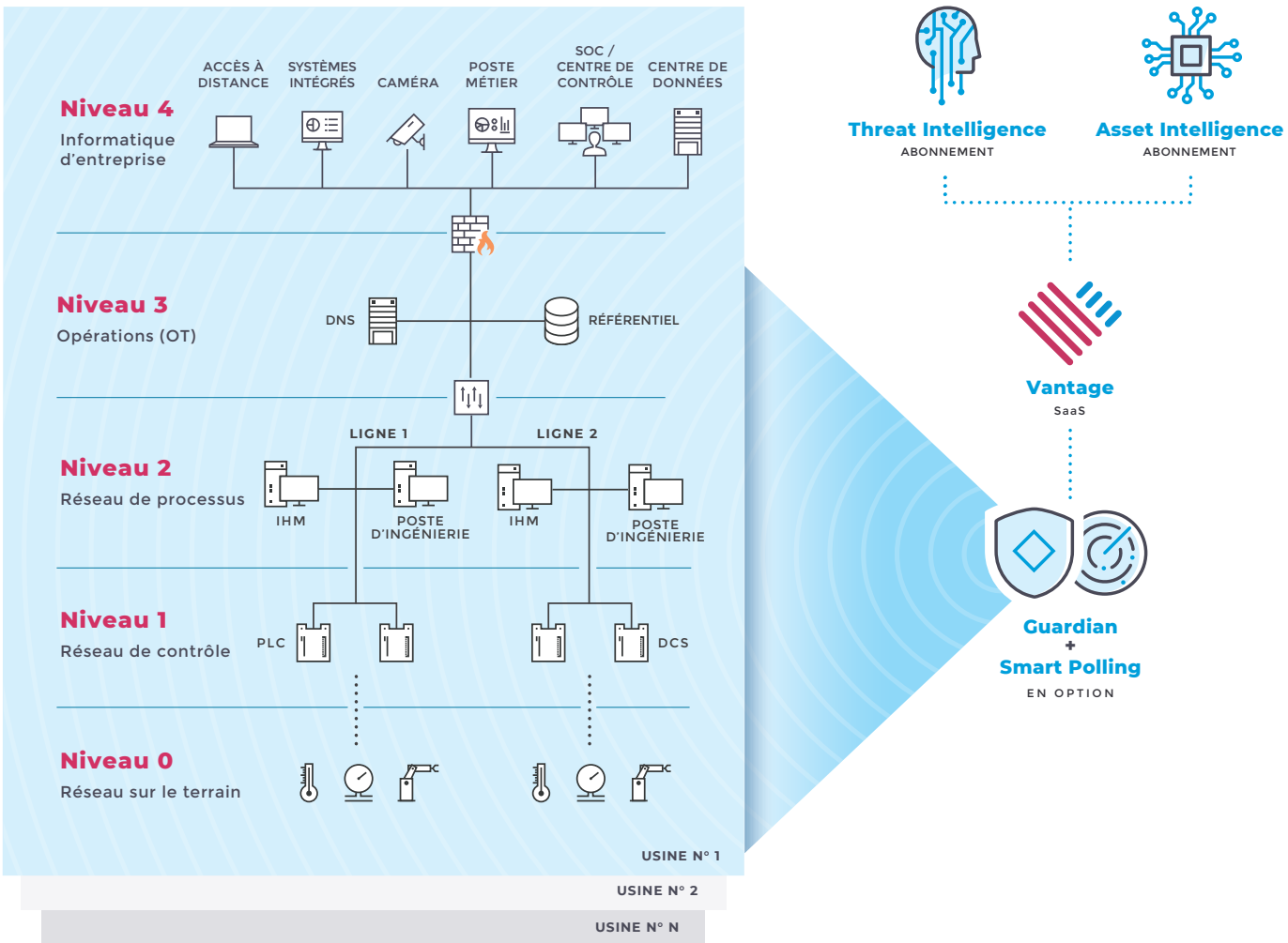
Vous pouvez protéger une grande variété d'environnements mixtes grâce à la découverte rapide des ressources, la visualisation du réseau en temps réel et des renseignements actualisés sur les menaces.



3.3 Architecture de déploiement : Exemple de modèle Purdue

Vous pouvez adapter la solution Nozomi Networks à vos besoins en utilisant son architecture flexible et ses intégrations avec d'autres systèmes.

Des **Remote Collectors™** peuvent être ajoutés aux capteurs Guardian pour capturer des données à partir de sites distants.



4. Amélioration de la visibilité sur le réseau et l'exploitation

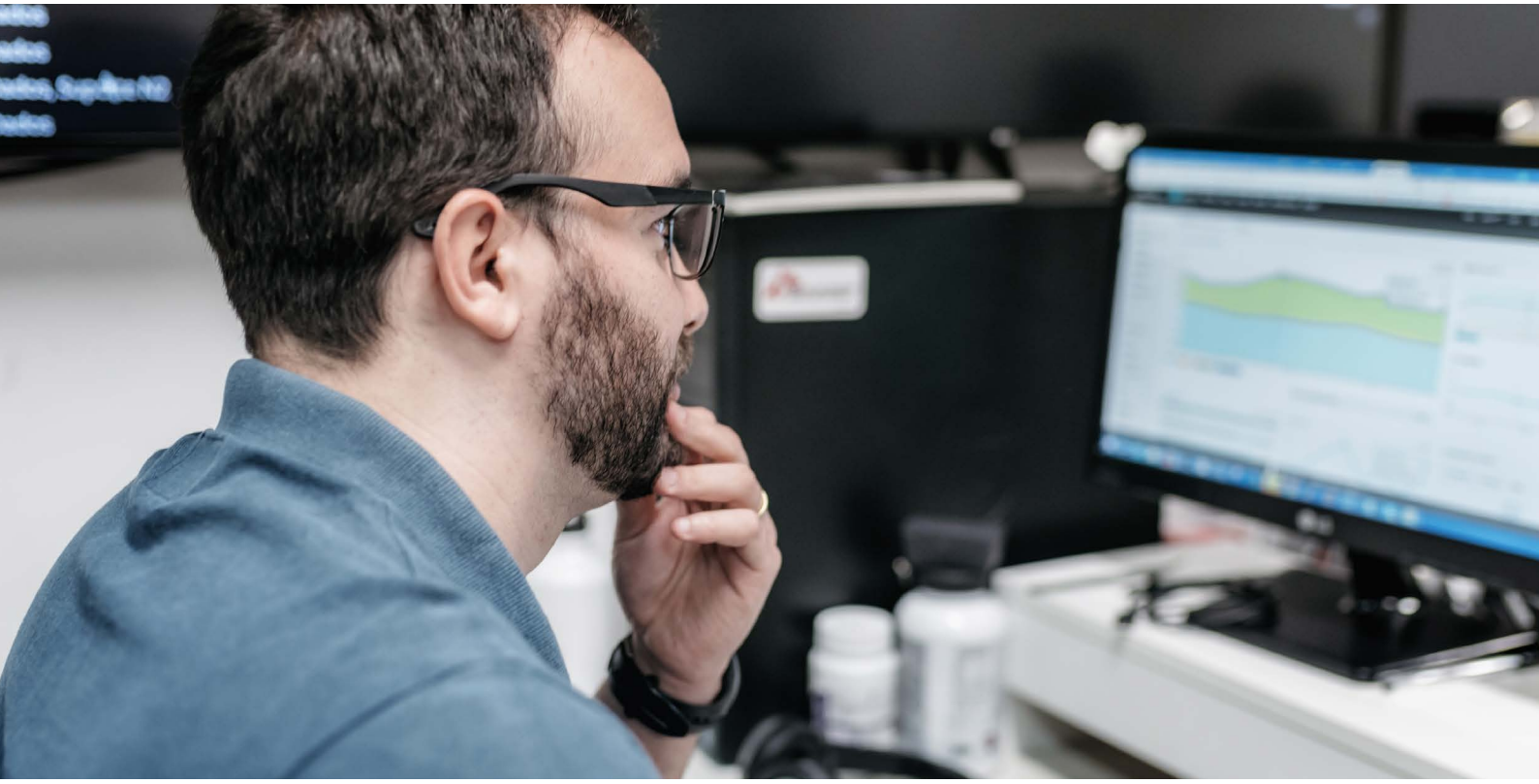
4.1 Cas d'utilisation : Supervision efficace du réseau ICS

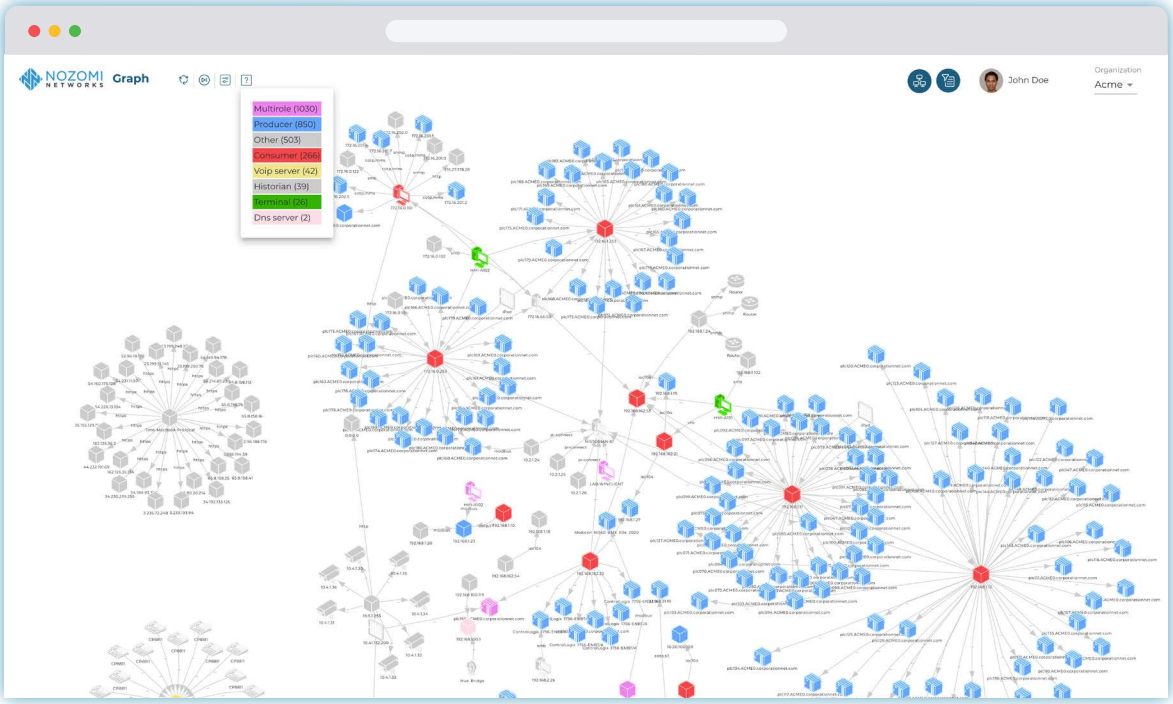
Dans le monde de la fabrication, un petit changement ou un problème de connectivité peut avoir un effet significatif sur la qualité des produits, la disponibilité de la production et même la sécurité de l'usine. Il est essentiel de comprendre ce qui se passe dans le réseau de contrôle industriel et de réagir rapidement aux changements.

Mais les opérateurs industriels ne peuvent pas surveiller et gérer ce qui n'est ni visible ni documenté. Par exemple, lors d'une récente preuve de concept, une entreprise de fabrication a déclaré avoir 3 000 appareils sur son réseau. Lorsque la solution de Nozomi Networks a été déployée, 15 000 appareils sont apparus ! La solution a permis de découvrir des appareils qui étaient censés ne plus être utilisés, d'anciens prestataires qui avaient toujours accès au système, et d'autres informations surprenantes.

Savez-vous vraiment quels types d'appareils sont sur votre réseau, et combien il y en a ? Lesquels communiquent activement et quels protocoles ils utilisent ? Sauriez-vous si quelqu'un a intentionnellement ou accidentellement modifié la configuration d'un automate, ou supprimé un fichier journal ?

Pour repérer et résoudre les problèmes de réseau et de communication qui menacent la fiabilité, vous avez besoin d'une visibilité en temps réel sur les ressources, les connexions, les communications, les protocoles et autres.





La solution Nozomi Networks : Vue graphique du réseau
Cette visualisation affiche toutes les ressources de votre réseau en temps réel.

PROBLÉMATIQUE

- Maîtriser l'état et les changements apportés au réseau.

LA SOLUTION

Utilisation de la visibilité OT et IoT en temps réel pour améliorer la connaissance de la situation.

- La solution Nozomi Networks analyse le trafic réseau, et utilise les données pour une visualisation interactive du système, révélant souvent des aspects inconnus des systèmes industriels et de l'IoT.
- Les fabricants peuvent superviser efficacement les réseaux industriels et résoudre facilement les problèmes avant qu'ils n'aient un impact sur la production.

RÉSULTATS

Connaissance de la situation du réseau

Dépannage plus rapide des problèmes et des changements apportés au système

Meilleure compréhension des vulnérabilités et des risques

Plus grande fiabilité opérationnelle

4.2 Cas d'utilisation : Assurer le fonctionnement des lignes de production

Les temps d'arrêt imprévus ont de multiples causes : un composant tombe en panne alors qu'il fonctionnait 24 h/24, un changement apporté au réseau affecte les lignes de production ou un cyberincident perturbe la communication.

Non seulement il faut du temps pour comprendre et résoudre le problème, mais les précieuses capacités de production sont perdues. Pour atténuer ce type de risques, certains fabricants disposent d'un stock supplémentaire, juste pour couvrir les temps d'arrêt potentiels.

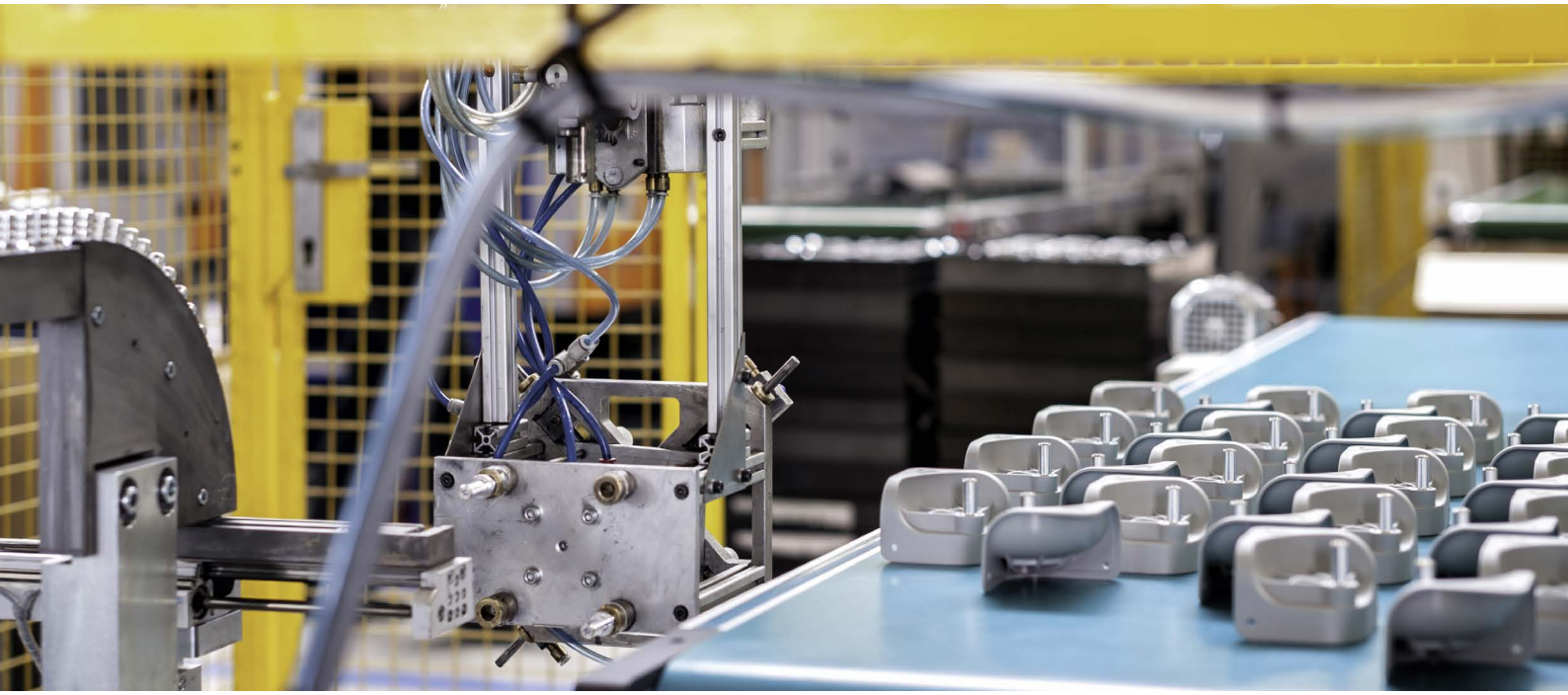
Mais dans le secteur de la fabrication, le temps c'est de l'argent, et les temps d'arrêt planifiés et non planifiés, ainsi que les stocks excédentaires, peuvent avoir un impact considérable sur les résultats. Selon Gartner, le coût des temps d'arrêt se situe entre 300 000 et 500 000 dollars par heure[6].

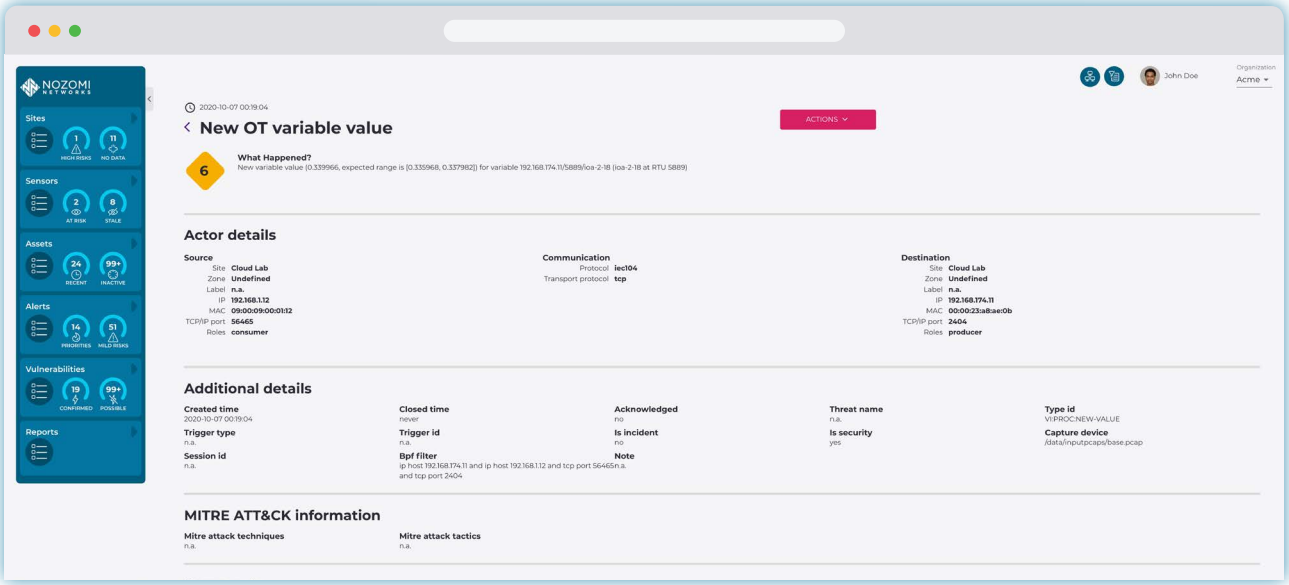
Prenons un exemple de temps d'arrêt :

En 2019, l'un des plus grands producteurs d'aluminium au monde, dont le siège est en Norvège, a déclaré avoir été touché par un logiciel rançonneur qui a affecté ses systèmes informatiques et de production. L'unité Extruded Solutions, qui fabrique des composants pour la construction automobile, la construction et d'autres secteur, a réduit sa production de 50 %.

Les systèmes administratifs, tels que la création de rapports et la facturation, ont subi des retards. Plusieurs semaines ont été nécessaires pour une reprise normale des activités. Les marges perdues et les faibles volumes de production ont été estimés à 70 millions de dollars[7].

Imaginez quels seraient les avantages de l'identification proactive des problèmes d'équipement potentiels, des cybermenaces et de la réduction de 50 % ou plus de votre stock courant ?





La solution Nozomi Networks : Alerte sur des variables d'exploitation
Le comportement inhabituel d'un équipement ou d'un système peut entraîner une interruption de l'exploitation et de graves incidents de sécurité.

PROBLÉMATIQUE

- Empêcher la perte des capacités de production.

LA SOLUTION

Détection des anomalies pour identifier les équipements et les processus à risque avant une défaillance

- La solution de Nozomi Networks protège contre les perturbations opérationnelles en détectant lorsqu'un dispositif spécifique ou une activité automatisée s'écarte de ses valeurs de référence et se dirige vers un état susceptible de perturber les services. Elle permet également de savoir si le travail du prestataire a été effectué ou non, afin de garantir que la maintenance soit effectuée à temps.
- Les opérateurs bénéficient d'une visibilité simple et consolidée sur ce qui se passe, et reçoivent des alertes qui les incitent à agir avant la défaillance d'un équipement ou d'une activité automatisée.

RÉSULTATS

Détection proactive des défaillances potentielles des équipements

Réduction du dépannage et des analyses

Résolution plus rapide des problèmes

Maximisation de la disponibilité de la ligne de production

5. Détection des cyber-risques et amélioration de la cyber-résilience

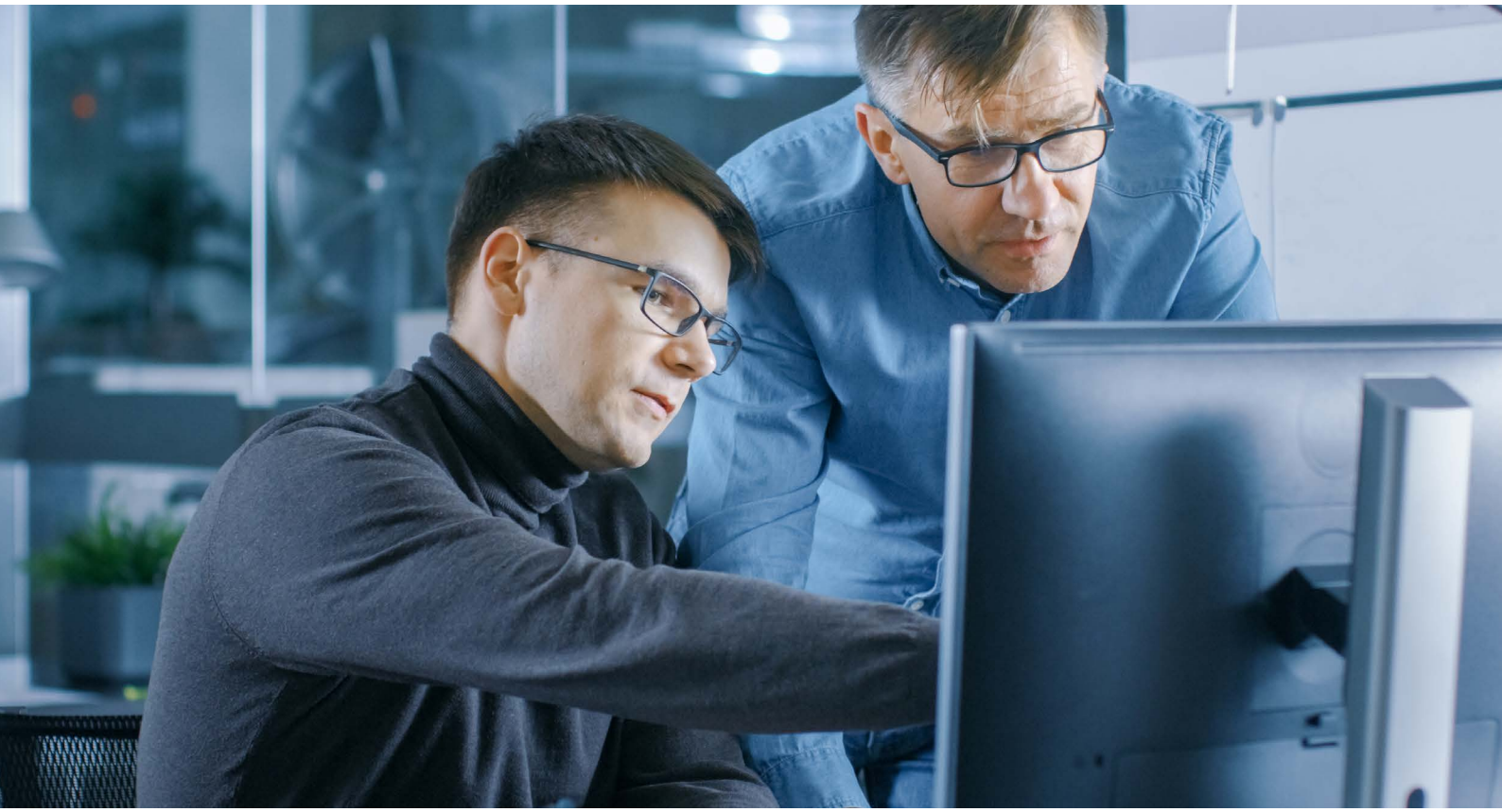
5.1 Cas d'utilisation : Intégration de la sécurité informatique/industrielle

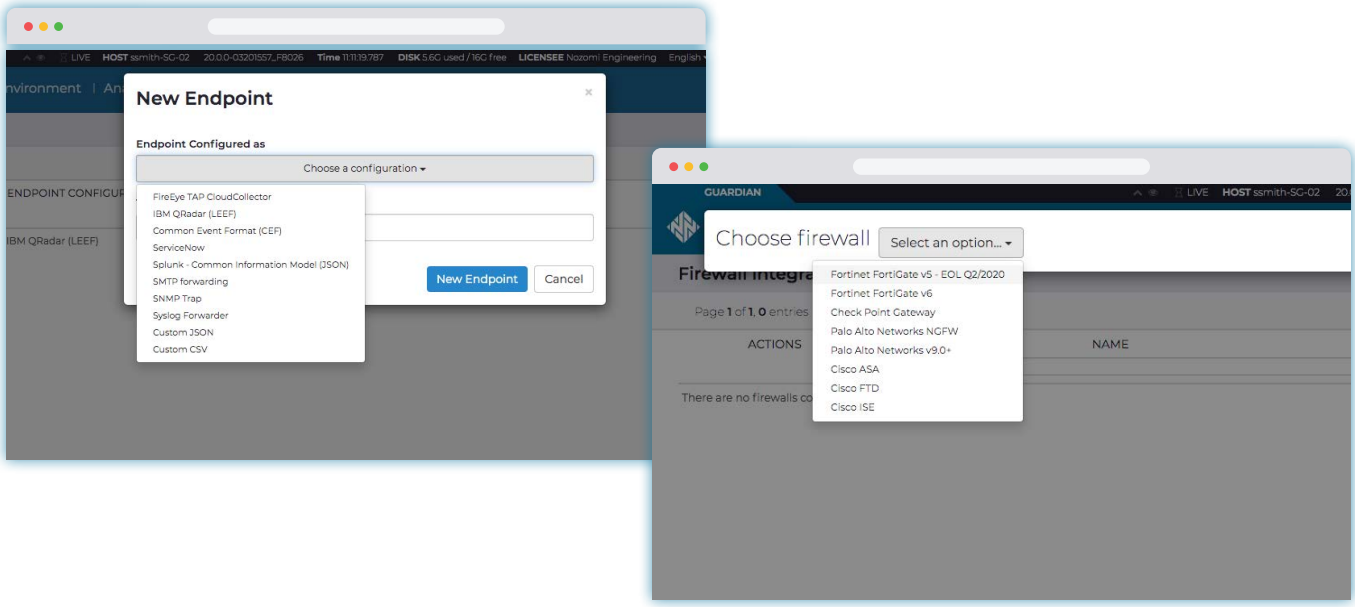
L'équipe industrielle sait comment atteindre les objectifs de production et faire fonctionner l'usine. L'équipe informatique dispose de l'expertise nécessaire pour traiter les problèmes de réseau et de cybersécurité auxquels l'équipe industrielle n'est pas familière. Ne serait-il pas formidable que les équipes informatiques et industrielles travaillent ensemble pour renforcer la résilience opérationnelle ?

Malheureusement, la surveillance de la sécurité industrielle peut être très fragmentée. Un rapport d'Automation World a révélé que moins de 8 % des entreprises interrogées ont combiné les deux départements, tandis que 24 % ne voient pratiquement aucune interaction entre eux[8].

Parfois, la sécurité industrielle est gérée par le groupe de technologie d'ingénierie, dans d'autres cas par un directeur d'usine. Parfois, un membre de l'équipe informatique passe dans l'équipe technique pour s'en occuper, d'autres fois, il y a peu ou pas d'interaction entre les équipes informatiques et industrielles

Pourtant, la collaboration entre ces équipes est essentielle pour réduire les angles morts et les risques qui entourent les systèmes de contrôle industriel hautement connectés. À mesure que les usines « intelligentes » exploitent davantage la technologie IIoT et que les réseaux industriels sont de plus en plus connectés aux réseaux d'entreprise et au Cloud, le fossé IT/OT met les entreprises en danger.





La solution Nozomi Networks : Intégration IT/OT facile

La prise en charge intégrée de nombreux systèmes de gestion des ressources et des identités, de pare-feux, de SIEM et autres, facilite l'intégration et le partage des informations des systèmes OT et IoT dans les environnements IT/OT.

PROBLÉMATIQUE

- Combiner l'expertise informatique et le savoir-faire industriel pour améliorer la résilience

LA SOLUTION

Alignement IT/OT grâce à une solution unique.

- La solution sans risque de Nozomi Networks offre aux équipes informatiques et industrielles une visibilité approfondie sur les ressources ICS, et une surveillance continue des risques qui pourraient avoir un impact sur la fiabilité ou la cybersécurité. Elle fournit une plateforme commune pour la convergence informatique/industrielle.
- Les fabricants peuvent facilement intégrer la surveillance des ressources industrielles en temps réel dans l'infrastructure de sécurité globale pour améliorer la résilience et la fiabilité opérationnelles.

RÉSULTATS

Réduction des angles morts de la sécurité industrielle

Suivi en continu pour une meilleure surveillance des menaces, des infractions et des risques

Dépannage plus rapide

Surveillance des menaces industrielles totalement intégrée dans le mandat de sécurité global

5.2 Cas d'utilisation : Application des bonnes pratiques de cybersécurité

Le risque opérationnel provient de multiples sources, notamment des personnes, des processus et de la technologie. D'après le rapport de Verizon de 2019 sur les fuites de données, les attaques intentionnelles sur la fabrication par des personnes extérieures représentaient 70 % de toutes les failles de sécurité signalées[2].

Tandis que les logiciels malveillants et autres cyberattaques très médiatisées retiennent l'attention, le SANS Institute rapporte que 28 % des professionnels de l'ICS considèrent les incidents internes (et souvent accidentels) comme le principal vecteur de menace. L'enquête sur la cybersécurité OT/ICS récemment publiée par l'entreprise révèle que 62 % des personnes interrogées considèrent les « personnes » comme étant le pilier le plus risqué pour la sécurité, loin derrière la technologie et les processus[9].

Parmi les exemples de risques opérationnels d'origine humaine, la mauvaise configuration des équipements, les ports ouverts, l'utilisation de mots de passe faibles et la continuité de l'accès des prestataires après leur départ de l'entreprise.

Compte tenu du risque important pour les activités, il n'est pas surprenant que les responsables industriels veuillent améliorer leur sécurité. Mais comment mettre en œuvre un cadre de cybersécurité et améliorer la cyber-résilience ?

La solution Nozomi Networks : Affichage des ressources
Cet affichage résume l'état des ressources sur l'ensemble des sites pour une connaissance de la situation et une évaluation des risques en temps réel.

PROBLÉMATIQUE

- Renforcement de la maturité de la sécurité sur l'ensemble de l'entreprise

LA SOLUTION

Détection des anomalies pour identifier les équipements à risque avant leur défaillance.

- La solution de Nozomi Networks facilite la compréhension et l'adoption de bonnes pratiques de cybersécurité, telles que celles décrites dans le NIST Cybersecurity Framework Manufacturing Profile, CEI 62443 et ISO 27000.

  Par exemple, le NIST décrit cinq fonctions du cadre de sécurité, l'identification, la protection, la détection, le traitement et la reprise, qui devraient être intégrées dans vos processus opérationnels pour faire face au cyber-risque. L'identification comprend la gestion des ressources et l'évaluation des risques, tandis que la détection inclut la recherche des anomalies et des événements en continu, entre autres fonctions.
- Avec l'adoption d'une solution de visibilité industrielle, les fabricants peuvent automatiser la création d'un inventaire des ressources et surveiller en permanence leur réseau et leurs ICS. Ils peuvent également repérer rapidement les vulnérabilités et identifier de manière proactive les menaces pour la sécurité de leurs systèmes de contrôle industriel.

RÉSULTATS

Adoption de cadres et de bonnes pratiques de cybersécurité

Identification et atténuation proactives des risques opérationnels

Amélioration de la résilience opérationnelle

6. Conclusion

La cybersécurité et la visibilité opérationnelle renforcent la résilience pour le secteur manufacturier

Les fabricants adoptent la transformation digitale pour dégager des gains d'efficacité et augmenter leurs revenus. Ce faisant, ils devront inévitablement relever des défis opérationnels courants, tels que l'obtention d'une visibilité sur leurs réseaux industriels et IoT, et la fermeture des failles de sécurité.

PROTECTION DES LEADERS MONDIAUX DE LA PRODUCTION

Sans visibilité OT et IoT, il est difficile de comprendre ce qui se passe sur le réseau. Un problème ou un petit changement apporté au réseau peut avoir un impact sur la qualité des produits, la disponibilité de la production, la sécurité de l'usine et les revenus.

Une visibilité en temps réel est nécessaire pour repérer et résoudre les problèmes qui menacent la fiabilité. Malheureusement, de nombreux fabricants n'ont pas une visibilité claire sur leurs équipements, leurs connexions et leurs communications.

Les failles de sécurité liées aux personnes, aux processus et aux technologies peuvent également avoir un impact important sur la résilience opérationnelle. Par exemple, la séparation IT/OT, combinée à des systèmes de contrôle industriels de plus en plus connectés, peut entraîner des angles morts pour la cybersécurité. Mais avec la bonne technologie et en se concentrant sur les meilleures pratiques, les fabricants peuvent améliorer leur résilience opérationnelle.

Avec la solution de Nozomi Networks, la visibilité et la cybersécurité sont faciles à implémenter. Elle offre une meilleure visibilité sur les ressources industrielles et de l'IoT en créant automatiquement un inventaire à jour de toutes les ressources sur le réseau. Elle surveille ensuite leur comportement pour détecter les anomalies et avertit les opérateurs des changements qui pourraient indiquer des problèmes potentiels. La solution offre également une détection avancée des vulnérabilités et des menaces, ainsi qu'un aperçu détaillé pour établir plus rapidement les priorités et les mesures correctives.

Conçue pour répondre aux défis uniques de l'industrie manufacturière, la solution de Nozomi Networks aide les opérateurs à bénéficier d'une meilleure visibilité opérationnelle, appliquer les bonnes pratiques de sécurité et aligner les technologies informatiques et industrielles.

Elle contribue nettement à surveiller les réseaux OT/IoT, maintenir le fonctionnement des lignes de production, intégrer la sécurité IT/OT et appliquer les bonnes pratiques de cybersécurité.

EN SAVOIR PLUS

Les fabricants ont tout à gagner à investir dans une solution de visibilité, de surveillance et de sécurité réseau.

Découvrez à quelle vitesse la solution Nozomi Networks peut renforcer votre résilience opérationnelle.

Contactez-nous via **nozominetworks.com/contact**

7. Avis des clients

Les clients du secteur de la fabrication accordent le meilleur score à Nozomi Networks

★★★★★

Attentes dépassées. Visibilité plus approfondie que prévu.

Nous faisons comprendre à chaque fournisseur avec lequel nous nous engageons que nous ne sommes pas faits pour une solution standard. Honnêtement, je m'attendais à ce que ce soit un problème pour la plupart des fournisseurs, sinon tous. Et j'avais raison, Nozomi est la seule exception. Non seulement sa solution fait ce qu'elle annonce, mais elle le fait même mieux.

Responsable senior de la sécurité industrielle

Une fois que vous aurez essayé Nozomi et ses fonctionnalités enrichies, vous ne pourrez plus vous en passer !

Nous l'avons comparé à d'autres produits similaires ; la plateforme Nozomi a été capable d'identifier et de classer correctement plus d'appareils L2 que tout autre outil sur le marché au moment du test.

Analyste de sécurité

D'excellentes solutions ICS.

La solution dispose encore de nombreuses fonctionnalités pour gérer l'environnement industriel, telles que l'inventaire et l'analyse des vulnérabilités. Point supplémentaire pour la solution : la carte des flux de communication du réseau neuronal, qui contient des informations d'une grande pertinence pour le traitement des incidents.

Analyste informatique

Pour plus d'avis, consultez notre site web.

Voir tous les avis

Prérequis d'une solution de sécurité et de visibilité OT et IoT

Les avancées technologiques, telles que celles de la solution Nozomi Networks, peuvent améliorer considérablement la sécurité et la fiabilité.

Lorsque vous choisissez une solution, recherchez les fonctionnalités suivantes :

- **Visibilité complète sur l'ensemble de votre réseau**
- **Détection avancée des menaces**
- **Alertes fiables sur les anomalies**
- **Évolutivité éprouvée**
- **Intégration IT/OT facile**
- **Écosystème mondial de partenaires**
- **Engagement et support client exceptionnels**

Voir la solution Nozomi Networks en action

Si vous souhaitez évaluer notre solution et constater à quel point il est facile de travailler avec Nozomi Networks, veuillez nous contacter via **nozominetworks.com/contact**

Contactez-nous

Vous voulez en savoir plus ?

PRÉSENTATION DE LA SOLUTION
Nozomi Networks

TÉLÉCHARGEZ

PAGE WEB
Fabrication

CONSULTEZ

FICHE PRODUIT
Vantage

TÉLÉCHARGEZ

FICHE PRODUIT
Threat Intelligence

TÉLÉCHARGEZ

8. Références

1. **« Cybersecurity for Manufacturing »,** Make UK (anciennement EEF), 2019.
2. **« 2019 Data Breach Investigations Report »,** 11e édition, Verizon, 2019.
3. **« How Much Did a Cyberattack Cost Reckitt Benckiser? Try $117 Million »,** AdAge, 2017.
4. **« WannaCry: A Wake-up Call to Revisit ICS Cybersecurity Measures »,** Nozomi Networks, 2017.
5. **« Russian Cyberattacks on Critical Infrastructure – What You Need to Know »,** Nozomi Networks, 2018.
6. **« The Cost of Downtime »,** Gartner, 2014.
7. **« First Quarter 2019 Report »,** Hydro, 2019.
8. **« Bridging the IT and OT Divide »,** Automation World, 2017.
9. **« SANS 2019 State of OT/ICS Cybersecurity Survey »,** SANS, 2019.
10. **« Cybersecurity Framework Manufacturing Profile »,** NIST, 2017.

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.

© 2021 Nozomi Networks, Inc.
Tous droits réservés.

IB-MANU-FR-A4-004

nozominetworks.com