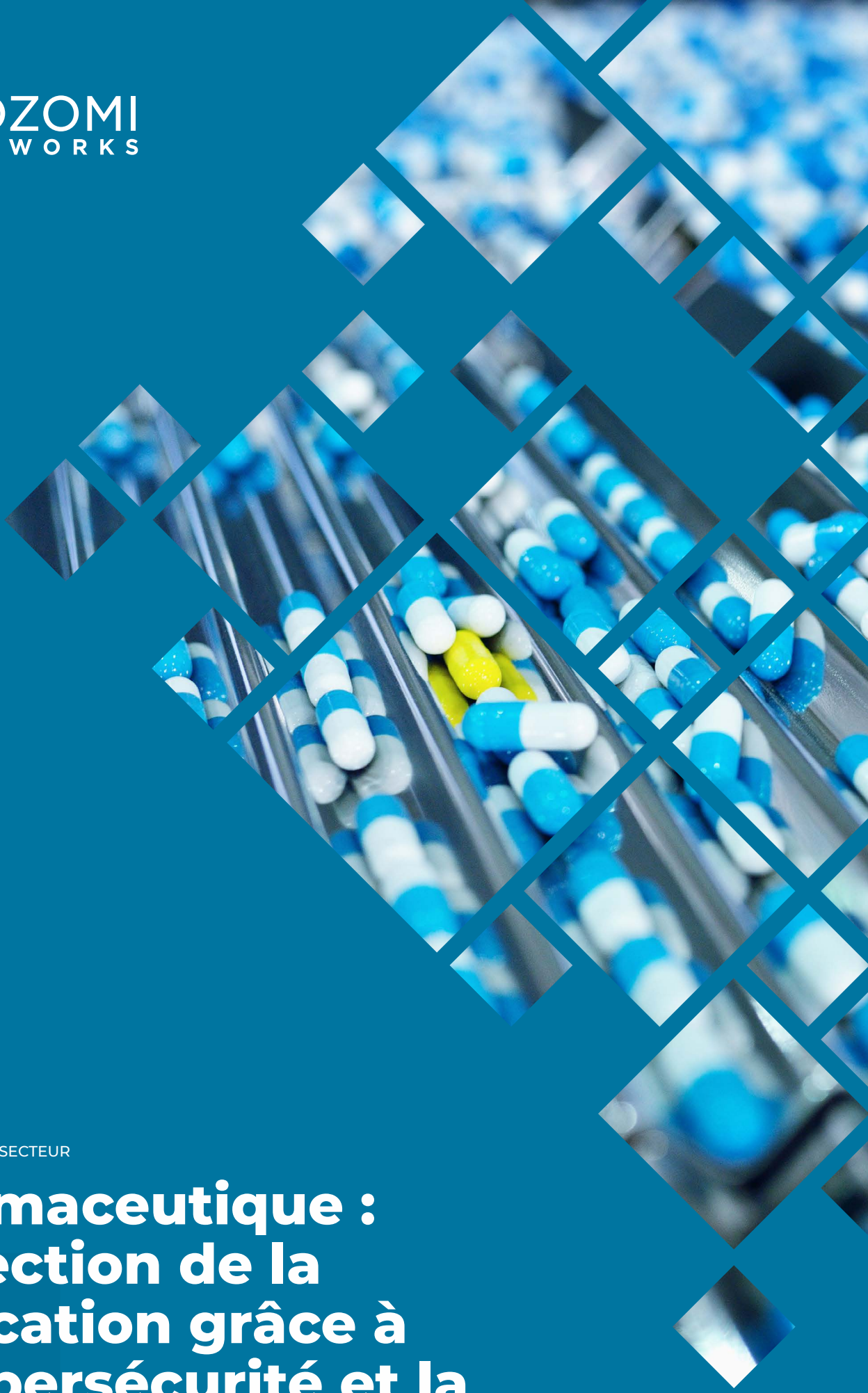
NOZOMI NETWORKS



PRÉSENTATION DE SECTEUR

Pharmaceutique : Protection de la fabrication grâce à la cybersécurité et la visibilité opérationnelle

Table des matières

1. Introduction

Protection de la fabrication de produits pharmaceutiques grâce à la cybersécurité et la visibilité opérationnelle

Avec des revenus et un financement de la R&D en hausse, l'industrie pharmaceutique devrait continuer de croître. Mais les défis actuels, tels que les politiques gouvernementales plus strictes et l'inquiétude du public face à la montée en flèche des coûts des médicaments, amènent de nombreux fabricants à tenter de maintenir leurs bénéfices par des gains d'efficacité opérationnelle.

Les fréquentes fusions et acquisitions, et les chaînes logistiques de plus en plus complexes, nécessitent une meilleure visibilité sur les environnements de technologie opérationnelle (OT), de l'Internet des objets (IoT) et de technologie de l'information (IT). Pourtant, l'interconnexion entre les appareils et les systèmes entraîne des risques accrus pour la cybersécurité. Les solutions avancées qui offrent une visibilité opérationnelle en temps réel et une sécurité IoT/OT peuvent aider l'industrie pharmaceutique à équilibrer la croissance et le risque tout en renforçant la résilience de la production.

Les entreprises pharmaceutiques adoptent la transformation digitale et les acquisitions comme moyen d'innover et d'améliorer l'efficacité. En 2018, les fusions et acquisitions ont atteint 265 milliards de dollars, soit une hausse de 26 % par rapport à l'année précédente[1]. À mesure que le secteur se consolide pour dégager des synergies, il en résulte un réseau complexe d'opérations, de réseaux et de flux de données. Cela crée des problèmes de visibilité opérationnelle et accroît la vulnérabilité aux cybermenaces.

L'approche flexible de l'industrie pharmaceutique pour ses capacités de production est un autre facteur contribuant à la vulnérabilité des systèmes. Afin de réduire les coûts de la chaîne logistique et répondre aux fluctuations de la demande, les fabricants externalisent de plus en plus leurs opérations. Ils peuvent ainsi faire rapidement évoluer la production, mais au prix d'une infrastructure complexe d'équipements et de systèmes connectés. Les entreprises doivent équilibrer les coûts et les avantages de la collaboration avec des prestataires de services et l'augmentation du cyber-risque.

Elles doivent également tenir compte d'un autre aspect de la sécurité : les données relatives aux formules et aux composés propriétaires sont devenues une cible de choix pour les pirates. Selon une étude de Deloitte, l'industrie pharmaceutique est souvent la cible numéro un des cybercriminels, en raison de sa propriété intellectuelle (PI) précieuse[2].

Le financement de la R&D et la protection des brevets sur les médicaments sont coûteux. Il n'est donc pas surprenant qu'un secteur doté de ressources d'une telle valeur soit la cible de cyberattaques. En 2017, l'une des plus grandes entreprises pharmaceutiques au monde a été ciblée par le logiciel rançonneur NotPetya.

Les effets dévastateurs de ce logiciel malveillant ont coûté à l'entreprise plus de 300 millions de dollars par trimestre, selon des estimations[3].

PROTECTION DE LA FABRICATION

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.

Compte tenu des multiples défis, l'industrie pharmaceutique éprouve un nouveau sentiment d'urgence à protéger des données précieuses et sensibles. Mais avec une infrastructure réseau complexe, il est difficile d'inventorier et défendre efficacement les ressources de l'ensemble du système, en particulier les systèmes cyber-physiques.

Les fabricants de produits pharmaceutiques ont un besoin immédiat de solutions de sécurité complètes pour inventorier les ressources industrielles, identifier les vulnérabilités, détecter les anomalies et les intrusions, et automatiser les alertes. La solution de sécurité et de de visibilité OT et IoT de Nozomi Networks a prouvé qu'elle fournissait exactement cela dans 7 des 10 plus grandes entreprises pharmaceutiques mondiales.

2. Principaux défis de l'industrie pharmaceutique

À mesure que les entreprises pharmaceutiques adoptent des chaînes logistiques de plus en plus complexes et recherchent une plus grande efficacité opérationnelle, elles sont confrontées à des défis qui, s'ils ne sont pas correctement relevés, peuvent les exposer à des risques importants.

2.1 Protection de la PI et des données précieuses contre le vol

La propriété intellectuelle (PI) est la ressource la plus précieuse d'une entreprise pharmaceutique. Selon une étude récente du Tufts Center, les fabricants de médicaments dépensent environ 2,6 milliards de dollars pour le développement d'un nouveau médicament sur ordonnance, de la conception jusqu'à l'autorisation de commercialisation[4].

Il n'est donc pas surprenant que des pirates s'infiltrent dans les réseaux OT pour accéder aux formules et aux données des composés, ou à d'autres informations qui pourraient être exploitées à des fins financières. Bien que les recettes exactes ne soient pas exposées dans l'usine, il est possible de trouver une voie d'accès au réseau informatique de l'entreprise via des appareils OT non protégés, et d'exfiltrer les formules et autres données secrètes.

Ces informations peuvent être vendues à des concurrents peu scrupuleux qui cherchent à faire progresser leur offre de produits. L'accès à des informations propriétaires pourrait également être exploité lors de négociations de fusions et acquisitions ou de prises de contrôle hostiles.

Pour compliquer le problème, les menaces peuvent provenir de sources tant externes qu'internes. Des attaquants pourraient accéder aux informations via des points vulnérables du réseau, et les salariés pourraient également agir à des fins malveillantes. Un membre du personnel pourrait par exemple être incité à accorder un accès non autorisé aux réseaux IT/OT. Des failles de sécurité peuvent également survenir de manière accidentelle, en connectant un appareil non sécurisé au réseau, ou en introduisant involontairement un logiciel malveillant via un email de phishing.

LA PI PEUT ÊTRE COMPROMISE PAR DES ACTEURS EXTERNES ET INTERNES

Un acteur malveillant pourrait exploiter des vulnérabilités du réseau OT pour accéder à des données propriétaires, tandis qu'un salarié pourrait fournir des identifiants d'accès aux systèmes internes.

Les fabricants de produits pharmaceutiques doivent prendre des mesures pour atténuer ces risques, en mettant en œuvre des processus et des programmes de sécurité efficaces.

Quelle que soit la source de la menace, la clé de la protection des informations précieuses et sensibles réside dans la surveillance continue de l'activité du réseau, et la détection rapide des anomalies et des intrusions. Il est également essentiel d'alerter le personnel de sécurité afin qu'il puisse prendre rapidement des mesures pour contenir ou éradiquer une menace.

2.2 Prévention des vulnérabilités dans les chaînes logistiques complexes

L'industrie pharmaceutique possède l'une des infrastructures les plus complexes de tous les secteurs. Un rapport récent de PwC indique que la chaîne logistique est sur le point de subir une refonte radicale[5]. L'une des stratégies déployées pour dégager des gains d'efficacité opérationnelle implique différents degrés d'externalisation.

Le modèle d'externalisation le plus innovant s'articule autour de la « fabrication pharmaceutique virtuelle », qui implique d'employer une main-d'œuvre réduite et de tout sous-traiter, de la production du lot clinique jusqu'à la production à grande échelle. Bien que peu de grandes entreprises pharmaceutiques aient entièrement externalisé leur chaîne logistique, beaucoup d'entre elles font appel à un nombre croissant de tiers.

Plutôt que d'investir dans des processus, des installations et des technologies de production internes, beaucoup optent pour cette voie moins risquée financièrement. Lorsque la demande augmente, il est facile de passer à la vitesse supérieure en faisant appel à un ou plusieurs fabricants sous contrat. Et lorsque la demande diminue, elles cessent simplement de les utiliser. Ainsi, le risque de fluctuations de la demande est transféré aux partenaires externalisés plutôt que d'avoir un impact direct sur les résultats de l'entreprise pharmaceutique.

La production, le conditionnement et la distribution externalisés sont beaucoup plus complexes qu'une approche interne. Mais pour maintenir les normes de sécurité propres à l'entreprise pharmaceutique, chaque processus de l'infrastructure décentralisée doit être surveillé pour y détecter des vulnérabilités et des menaces.

L'utilisation d'une solution de sécurité et de visibilité sur les technologies d'exploitation, associée à une console d'administration centrale (CMC) d'un centre d'opérations de sécurité (SOC), permettrait aux entreprises pharmaceutiques de surveiller l'activité réseau des systèmes concernés. Mais comme certains des équipements détenus par les partenaires externes sont susceptibles d'être utilisés pour fabriquer des produits concurrents, les partenaires seront très soucieux de la confidentialité.

Pour faire face aux problèmes de sécurité de la chaîne logistique des tiers, les entreprises pharmaceutiques exigent généralement que les prestataires externes soient en mesure de prouver qu'ils respectent leurs principaux contrôles de sécurité. Les outils de surveillance et de visibilité sur le réseau tels que la solution de Nozomi Networks sont essentiels pour fournir les preuves détaillées requises. La même solution peut être déployée par l'entreprise pharmaceutique et ses prestataires pour fournir des indicateurs et des rapports de sécurité cohérents.

LES CHAÎNES LOGISTIQUES COMPLEXES PEUVENT COMPROMETTRE LA CYBERSÉCURITÉ

L'externalisation de la chaîne logistique et les acquisitions rendent difficile la surveillance et la sécurisation des processus de production. Dans ces circonstances,

l'utilisation d'une solution de sécurité et de visibilité opérationnelle par tous les participants de la chaîne logistique est essentielle.

L'interconnexion requise par une chaîne logistique externalisée augmente considérablement les points d'entrée des cyberattaques. Les réseaux OT sont compromis par les points faibles supplémentaires introduits par des tiers et des prestataires externes. Tout en profitant des avantages d'une chaîne logistique évolutive, les fabricants de produits pharmaceutiques et leurs partenaires externes doivent redoubler de vigilance, et surveiller les communications ou connexions inhabituelles qui pourraient indiquer une cybermenace ou une intrusion.

2.3 Prévention des temps d'arrêt non planifiés

La production cohérente et vérifiée de médicaments n'est pas une option. Elle est exigée par la loi. Par conséquent, l'intégrité du processus de production est essentielle pour garantir que les produits pharmaceutiques répondent aux normes prescrites.

LES CYBERATTAQUES PEUVENT PROVOQUER DES TEMPS D'ARRÊT ET LA REVALIDATION DU SYSTÈME

Lorsque les entreprises pharmaceutiques manquent de visibilité sur leur réseau de contrôle de la fabrication,

il est difficile de détecter les menaces et les risques qui peuvent avoir un impact sur la production ou déclencher la nécessité d'une revalidation.

L'arrêt des systèmes peut nécessiter un processus de « revalidation » pour vérifier les normes de qualité et veiller à ce que les équipements de fabrication conservent la précision de leur étalonnage et leurs mesures.

Malheureusement, des temps d'arrêt peuvent se produire pour de multiples raisons, notamment des erreurs accidentelles et non intentionnelles, ainsi qu'à des cyberattaques. Par exemple, des points d'accès Wifi malveillants pourraient ralentir ou même arrêter la chaîne de production. Ou bien, l'entreprise pourrait être frappée par une attaque de logiciels malveillants. Compte tenu de l'augmentation des menaces, de la valeur de la propriété intellectuelle de l'industrie pharmaceutique, et des vulnérabilités inhérentes aux chaînes logistiques pharmaceutiques, le risque de temps d'arrêt non planifié est élevé.

Et comme toute interruption de la chaîne de production coûte cher à une entreprise pharmaceutique, les temps d'arrêt doivent être réduits au minimum ou évités.

Heureusement, les entreprises pharmaceutiques peuvent prendre des mesures préventives pour éviter les pannes des équipements et minimiser les temps d'arrêt.

La visibilité en temps réel sur les réseaux de contrôle de la fabrication est désormais possible grâce à l'inventaire automatique des systèmes et la surveillance en continu. Une meilleure connaissance des systèmes permet de détecter et d'atténuer plus rapidement les menaces, ce qui renforce la cyber-résilience et réduit les temps d'arrêt. De plus, la possibilité de localiser la source d'un problème peut accélérer considérablement les mesures correctives et éviter plus de pertes.

LE COÛT ÉLEVÉ D'UN CYBERINCIDENT

ENTREPRISE

Multinationale

CYBERINCIDENT

Logiciel rançonneur : NotPetya

IMPACT

Arrêt de la production

Impossibilité d'honorer les commandes de vaccins, ventes perdues et commandes en souffrance

Augmentation des dépenses marketing et administratives, et des coûts de production

Remédiation technologique

COÛT

670 M de dollars

2.4 Maximisation des avantages de la convergence IT/OT

À mesure que les fabricants de produits pharmaceutiques adoptent la connectivité via l'IoT, tout change, du développement et de la production de nouveaux médicaments jusqu'à la façon de servir les patients.

L'industrie pharmaceutique peut maximiser les avantages de la convergence IT/OT/IoT pour améliorer la sécurité, prévoir (et prévenir) les arrêts de la production, et réduire les coûts. L'objectif est de réduire les écarts entre la sécurité des systèmes industriels et celle des systèmes informatiques.

Mais c'est plus facile à dire qu'à faire. Il existe d'importants écarts entre la sécurité des systèmes informatiques et celle des systèmes industriels, car les départements qui en sont responsables ont traditionnellement une structure organisationnelle, des priorités et des mandats distincts. Pour réduire les angles morts et les risques liés aux systèmes de contrôle industriels, les équipes informatiques et industrielles doivent unir leurs forces, et établir une stratégie globale de gestion des risques pour la sécurité sur l'ensemble de l'entreprise.

Mais les combiner n'est pas simple. Les réseaux industriels du secteur pharmaceutique sont vastes et complexes, et comprennent des ressources et des processus inhabituels pour les départements informatiques. Ils peuvent également utiliser des protocoles de communication non sécurisés ou propriétaires, qui ne peuvent être évalués correctement avec les outils de sécurité informatique existants.

Il existe heureusement des technologies qui facilitent l'intégration IT/OT. Par exemple, la solution de Nozomi Networks est conçue pour surveiller et offrir une visibilité sur les réseaux OT et de l'IoT en temps réel, et détecter les menaces. Il s'agit d'une solution sûre pour les technologies industrielles, qui fournit également une visibilité et une détection des menaces nécessaires aux équipes informatiques.

LA VALEUR DE LA COLLABORATION IT/OT

Il existe des technologies qui facilitent l'intégration IT/OT. Par exemple, la solution de cybersécurité et de visibilité Nozomi Networks **facilite l'intégration et le partage des informations dans les environnements OT, IoT et IT.**

La surveillance combinée de la sécurité IT/OT aidera les fabricants pharmaceutiques à bénéficier d'une visibilité opérationnelle unifiée et étendre leurs défenses contre les cybermenaces. Les données et les alertes relatives aux technologies industrielles peuvent être facilement partagées avec des outils informatiques de SIEM et de gestion des tickets, ce qui permet à votre entreprise d'utiliser ses outils et ses flux de travail existants pour gérer les menaces sur les technologies industrielles.

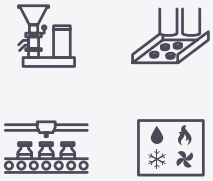
3. La solution Nozomi Networks

3.1 Comment la solution Nozomi Networks renforce la résilience et la cyberdéfense de l'industrie pharmaceutique

Nozomi Networks aide les entreprises pharmaceutiques 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.

LEADERSHIP DANS L'INDUSTRIE PHARMACEUTIQUE



Déployé dans
7 du Top 10 des principales entreprises pharma

Nozomi Networks fournit une visibilité OT/IoT, une détection et une compréhension des menaces à des milliers de sites industriels parmi les plus importants au 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 de produits pharmaceutiques 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).

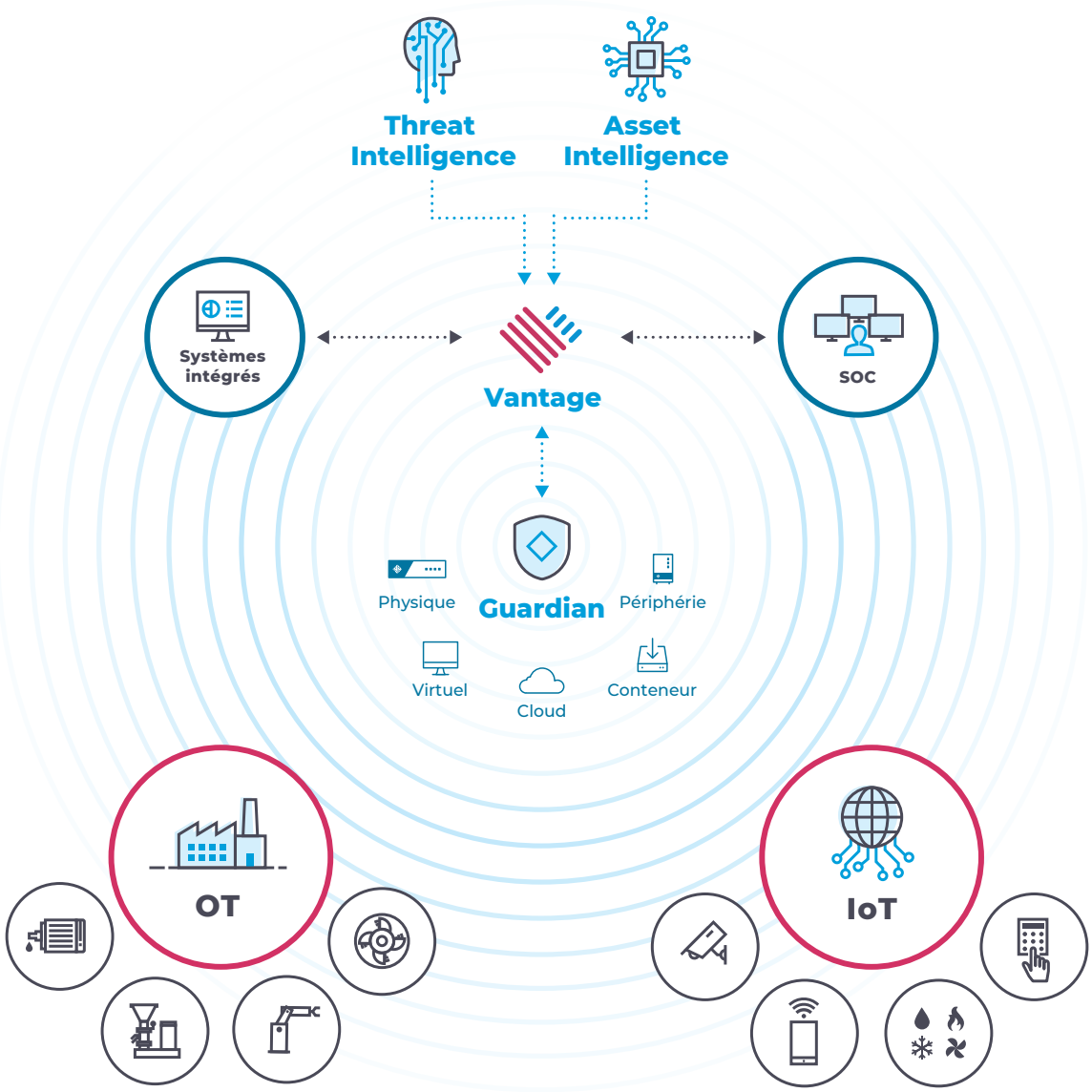
ABONNEMENT

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

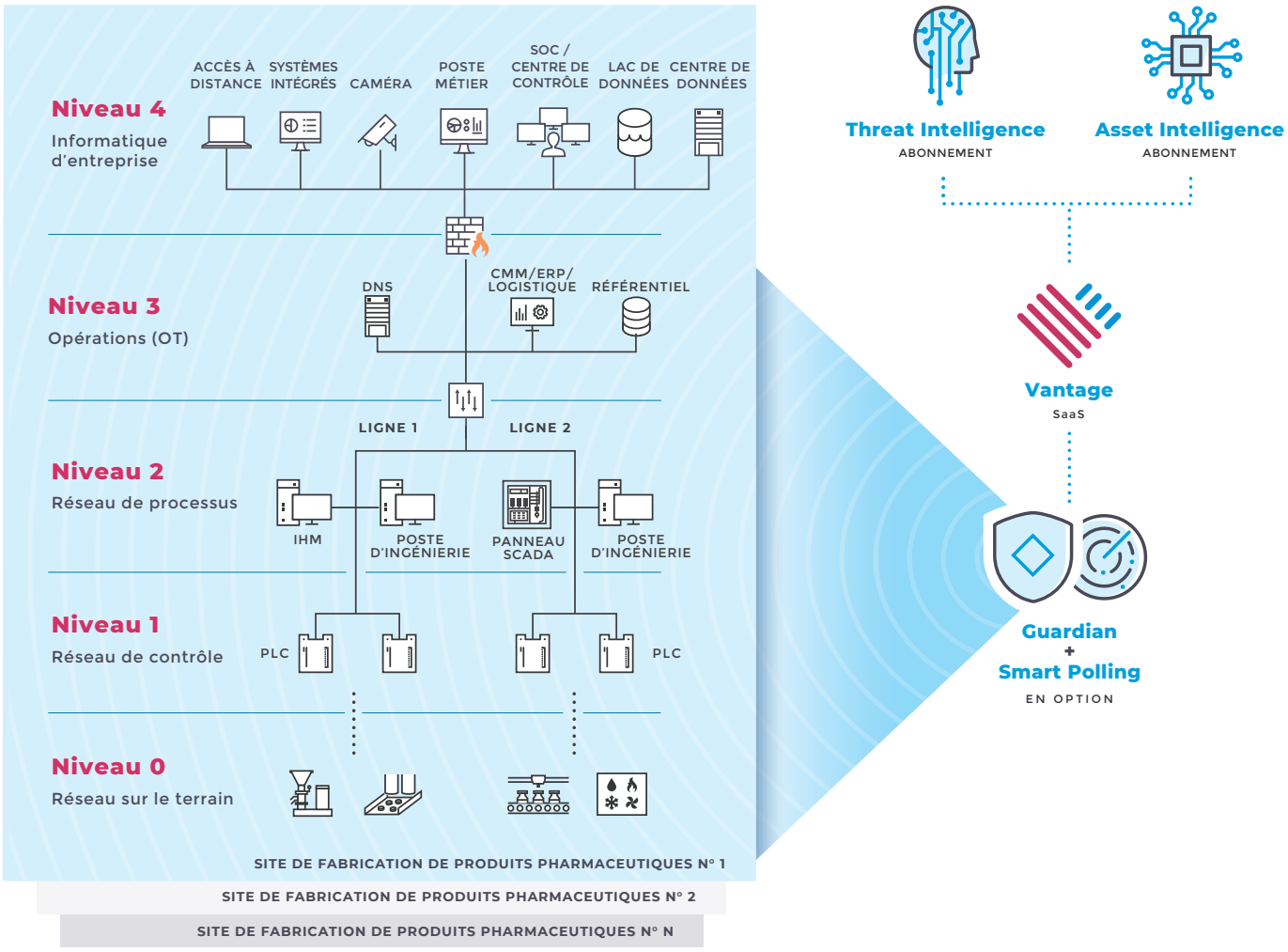
Vous pouvez protéger une grande variété d'environnements mixtes grâce à la découverte rapide des ressources, la visualisation du réseau en temps réel et des renseignements actualisés sur les menaces.



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

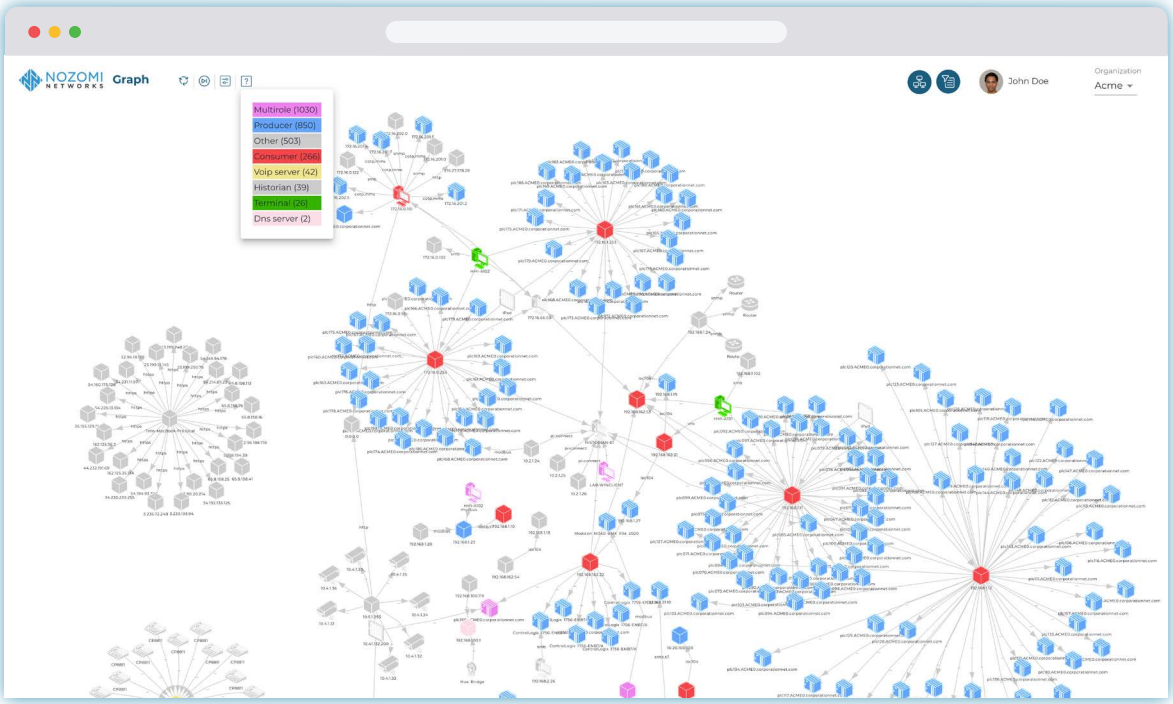
4.1 Cas d'utilisation : Visibilité sur une chaîne logistique fragmentée

Les chaînes logistiques pharmaceutiques peuvent être extrêmement complexes. Tandis que les entreprises poursuivent leur croissance par la transformation digitale et les fusions-acquisitions, elles sont confrontées au défi de l'intégration de systèmes d'exploitation et de chaînes logistiques disparates. Les efforts déployés pour répondre à des demandes fluctuantes ont par ailleurs accru le recours à l'externalisation. Il en résulte des équipements et des systèmes interconnectés qu'il est difficile d'inventorier et de surveiller en temps réel.

Comme nous l'avons mentionné précédemment, les entreprises pharmaceutiques exigent généralement de leurs partenaires d'externalisation qu'ils démontrent leur conformité aux contrôles de sécurité établis. Cela signifie que tous les intervenants de la chaîne logistique ont besoin de leur propre outil de visibilité et de surveillance OT/IoT pour fournir la preuve de leur conformité. Heureusement, la même solution peut être déployée par l'entreprise pharmaceutique et ses prestataires pour fournir des indicateurs et des rapports de sécurité cohérents.

Pour repérer et résoudre les cybermenaces, tous les acteurs de la fabrication ont besoin d'une visibilité en temps réel sur leurs ressources, leurs connexions, leurs communications, leurs protocoles et autres. De nombreux problèmes courants de visibilité sur la chaîne logistique peuvent être résolus par la visualisation interactive en direct des environnements opérationnels. Une grande quantité d'informations utiles est disponible, notamment :

- Une visibilité sur l'ensemble du réseau de contrôle industriel, indiquant les zones, les liens, le trafic, etc.
- La possibilité de consulter différents sous-réseaux et segments de réseau, et de les filtrer
- Le rôle de chaque nœud et le trafic entre les nœuds
- Les protocoles utilisés pour communiquer entre les nœuds et les zones
- Des informations sur le trafic réseau, telles que le débit, les protocoles et les connexions TCP ouvertes
- Des attributs détaillés sur les postes et les connexions



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

PROBLÉMATIQUE

- Gagner en visibilité sur une chaîne logistique complexe.

LA SOLUTION

Utilisation de la visualisation du réseau en temps réel pour améliorer la compréhension du système

- La solution de Nozomi Networks offre une visibilité complète sur les ressources OT/IoT et le réseau industriel d'un opérateur.
- Les entreprises pharmaceutiques et les prestataires tiers peuvent gérer et surveiller efficacement les processus, identifier les risques pour la fiabilité et résoudre les problèmes.

RÉSULTATS

Connaissance de la situation du réseau

Visibilité complète sur le réseau et les processus de contrôle industriel

Meilleure surveillance des vulnérabilités et des risques pour la fiabilité

Dépannage plus rapide des problèmes et des changements apportés au système

4.2 Cas d'utilisation : Évaluation des risques en production

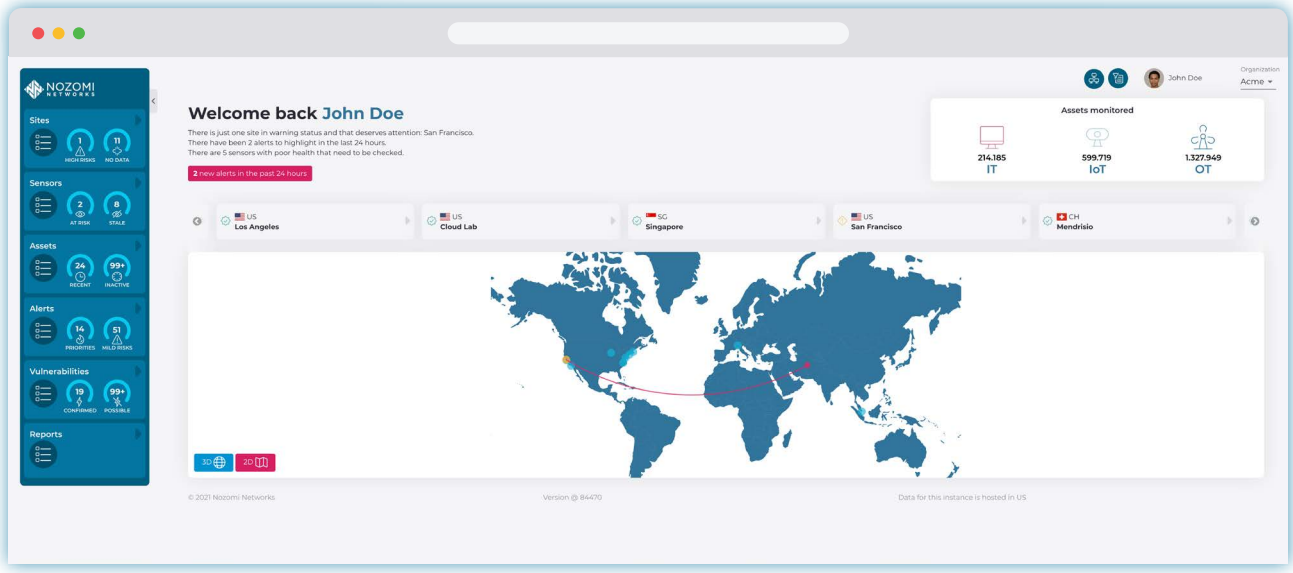
L'industrie pharmaceutique est très réglementée en ce qui concerne la qualité et la sécurité des produits commercialisés. Par exemple, la Food and Drug Administration (FDA) des États-Unis et l'Agence européenne des médicaments (EMA) publient toutes deux des lignes directrices pour le contrôle de l'efficacité des médicaments dans leur région.

Les entreprises pharmaceutiques suivent également les bonnes pratiques de fabrication (BPF) et les normes de validation des systèmes informatiques pour auditer les systèmes de production, respecter les directives réglementaires et maintenir la qualité constante des produits.

Malgré cela, l'environnement de la fabrication pharmaceutique peut être extrêmement complexe, ce qui rend difficile la conformité aux normes. Il intègre généralement des milliers de dispositifs connectés, et le niveau de complexité cyber-physique augmente lorsque des équipements utilisés par des tiers, tels que des prestataires de services et des partenaires, sont ajoutés. Les cybermenaces peuvent compromettre la validation du processus de fabrication, entraînant des rappels et des sanctions réglementaires.

Les pertes associées aux temps d'arrêt font que les fabricants de produits pharmaceutiques hésitent à mettre en œuvre de nouveaux contrôles de sécurité en raison des préoccupations liées à la revalidation. Ils sont extrêmement préoccupés par l'impact que les correctifs, les dispositifs mal configurés, les accès non autorisés et les ordinateurs portables infectés, pourraient avoir sur la conformité aux normes et la production. Tout changement ou nouvelle mesure de sécurité, notamment l'application d'un correctif, est susceptible de déclencher une revalidation du système, ou de perturber les processus et paralyser l'usine.

En visualisant et en renseignant les réseaux et les processus, les entreprises pharmaceutiques peuvent identifier et évaluer les cyber-risques en temps réel. Armés de ces informations, ils peuvent alors hiérarchiser ce qui doit être corrigé et à quel endroit, en perturbant le moins possible les chaînes de production.



Le tableau de bord Nozomi Networks
Le tableau de bord offre une vue personnalisable sur l'état du réseau et de la sécurité, mettant ainsi les informations essentielles à portée de main.

PROBLÉMATIQUE

- Évaluation des risques dans l'environnement de production.

LA SOLUTION

Détection automatisée des menaces et des vulnérabilités pour identifier et traiter rapidement les risques

- La solution de Nozomi Networks protège contre les perturbations opérationnelles en offrant une meilleure visibilité sur le réseau OT, une surveillance en continu, et une détection automatisée des menaces et des vulnérabilités.
- Les entreprises pharmaceutiques peuvent tirer parti de la détection et de la visibilité sur les menaces qui en résultent pour réduire les risques et mettre en place des contrôles pratiques qui minimisent la nécessité de valider les systèmes informatiques.

RÉSULTATS

Surveillance de la conformité en continu

Détection rapide des menaces et des vulnérabilités

Remédiation rapide et efficace

Amélioration de la fiabilité opérationnelle

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

5.1 Cas d'utilisation : Protection de la PI des entreprises contre le cyberespionnage

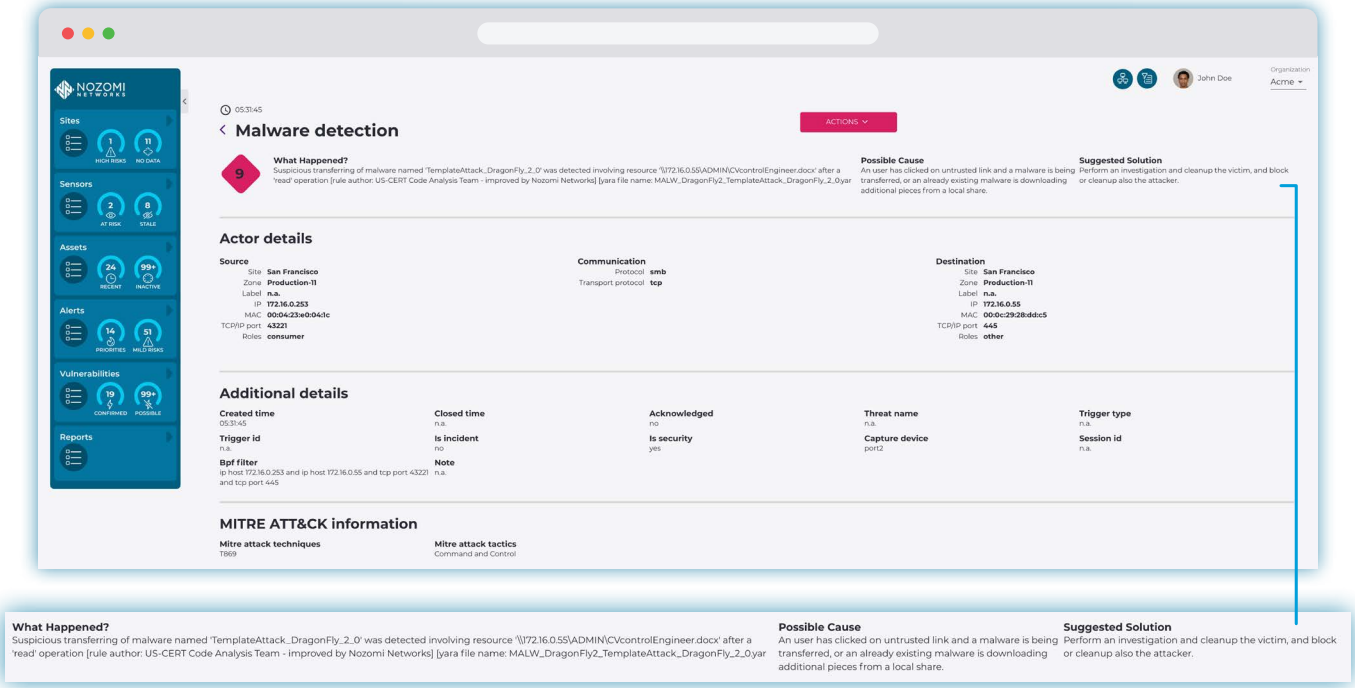
Dans un contexte de concurrence féroce pour gagner des parts de marché, les résultats des essais cliniques et les spécifications de fabrication peuvent être tout aussi précieux que les brevets et les formules.

En 2016, l'une des plus grandes entreprises pharmaceutiques d'Europe a été victime d'un vol de propriété intellectuelle. Deux salariés de l'entreprise ont volé des secrets commerciaux et communiqué des données confidentielles de l'entreprise à une entreprise sponsorisée par un gouvernement étranger. Depuis plus de dix ans, le groupe de pirates Winnti lance des cyberattaques contre des entreprises pharmaceutiques et de santé, ainsi que d'autres entreprises industrielles[6]. Des études révèlent que les infections de logiciels malveillants débutent souvent par un email de phishing.

Une fois activé, le programme peut localiser des données confidentielles de l'entreprise et les transmettre aux pirates.

Les cybermenaces se présentent sous de multiples formes, externes et internes, planifiées et non intentionnelles. Les attaques peuvent s'infiltrer via les technologies métiers informatiques ou industrielles, et se propager à l'ensemble de l'entreprise pharmaceutique. Par exemple, des pirates ont trouvé un moyen de compromettre les systèmes industriels non sécurisés connectés à l'infrastructure informatique, afin d'accéder à une propriété intellectuelle précieuse.

Pour protéger la position concurrentielle et la réputation de l'entreprise, il est essentiel pour les fabricants de produits pharmaceutiques de bien protéger les plans de développement des produits, les résultats des recherches et autres secrets de propriété intellectuelle confidentiels.



La solution Nozomi Networks : Détails des alertes

La solution de Nozomi Networks adopte une approche multidimensionnelle pour détecter les cyber-risques et les menaces. Elle utilise à la fois l'identification des menaces via des signatures et la détection des anomalies pour découvrir des attaques et fournir des informations claires et exploitables.

PROBLÉMATIQUE

- Protection de la confidentialité des secrets commerciaux et des formules.

LA SOLUTION

Une approche globale de la détection des cyber-risques et des menaces

- La solution de Nozomi Networks adopte une approche multidimensionnelle pour identifier les activités suspectes, qu'elles soient externes ou internes, accidentelles ou intentionnelles.
- Tous les résultats de la détection des menaces sont mis en corrélation avec le contexte opérationnel pour un aperçu détaillé. Par exemple, la solution compare les particularités du réseau telles que l'accès VPN et les plages IP attribuées à des fournisseurs de ressources connus à un référentiel. Si l'activité se situe en dehors des plages normales, une alerte est déclenchée.

RÉSULTATS

Identification proactive des activités non autorisées

Traitement accéléré des incidents par le personnel de sécurité

Confinement et élimination rapides des menaces

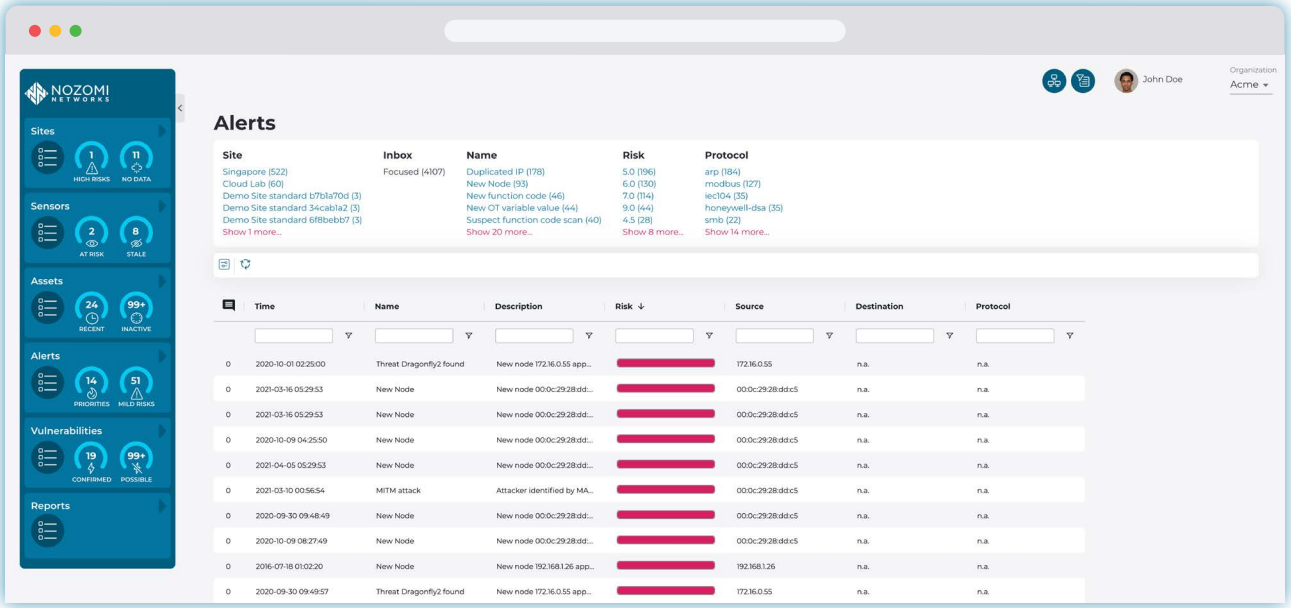
5.2 Cas d'utilisation : Détection des logiciels malveillants avancés présents sur les réseaux IT, IoT et OT

Les entreprises pharmaceutiques sont des cibles attrayantes pour les cybercriminels, en raison de leur propriété intellectuelle extrêmement précieuse, notamment les formules propriétaires et les brevets de médicaments en instance. Selon le rapport sur les menaces de Proofpoint au troisième trimestre 2018, l'industrie pharmaceutique est le secteur numéro un visé par des attaques d'emails frauduleux[7].

Où se situent les plus grandes failles de sécurité ? Au niveau de la surface des menaces qui s'étend en raison d'une connectivité accrue entre les systèmes IT, IoT et OT, et du recours à des fournisseurs tiers.

Dans les réseaux OT utilisés dans le processus de fabrication des produits pharmaceutiques qui contiennent des milliers de dispositifs qui ne prennent pas en compte la sécurité dans leur conception. L'intégration de machines physiques avec des logiciels et des capteurs connectés signifie que ces ressources industrielles se connectent, communiquent et interagissent en tant que systèmes cyber-physiques (CPS). Cela augmente considérablement la surface d'attaque que les cybercriminels peuvent utiliser pour accéder aux réseaux OT et IT.

Lorsqu'une attaque commence par l'infiltration du réseau informatique via une campagne de phishing par email, elle peut finalement migrer vers le réseau industriel via des systèmes accessibles aux deux environnements. S'ils ne sont pas maîtrisés, des logiciels malveillants peuvent entraîner le vol de propriété intellectuelle et perturber dangereusement les processus de production pharmaceutique.



La solution Nozomi Networks : Liste d'alertes

La solution de Nozomi Networks alerte les équipes de sécurité des activités de reconnaissance et d'infiltrations à un stade précoce, et fournit les informations nécessaires pour les traiter avant que des dommages ne se produisent. Le service Threat Intelligence fournit des informations actualisées sur les menaces et les vulnérabilités afin de conserver une longueur d'avance sur le paysage dynamique des menaces et réduire le délai moyen de détection (MTTD).

PROBLÉMATIQUE

- Détection des logiciels malveillants avancés présents sur les réseaux IT/OT.

LA SOLUTION

Surveillance automatisée du réseau OT de l'industrie pharmaceutique pour identifier les menaces

- La solution de Nozomi Networks détecte les menaces persistantes avancées à chaque phase d'une attaque. Elle alerte les opérateurs sur les activités de reconnaissance et d'infection à un stade précoce, et fournit les informations nécessaires pour prendre des mesures avant que l'attaque finale ne se produise.
- Grâce aux intégrations avec plusieurs pare-feux, la solution de Nozomi Networks ne se contente pas de détecter, mais de prévenir en déclenchant automatiquement des règles qui bloquent une attaque dès la détection de commandes anormales.

RÉSULTATS

Détection précoce des logiciels malveillants

Identification d'une activité de préparation d'attaque qui diffère d'un comportement normal

Déclenchement automatique de règles pour bloquer les cyberattaques (en cas d'intégration avec des pare-feux compatibles)

6. Conclusion

Une visibilité approfondie sur les environnements OT et IoT de l'industrie pharmaceutique renforce la résilience opérationnelle

Les entreprises pharmaceutiques adoptent rapidement des outils et des technologies pour gagner en efficacité opérationnelle. Cependant, l'automatisation et l'externalisation augmentent les risques et élargissent la surface des menaces. Il est donc difficile de faire rapidement face à des perturbations opérationnelles et repousser les cybermenaces.

LEADERSHIP DANS L'INDUSTRIE PHARMACEUTIQUE

Déployé dans

7 du Top 10

des entreprises pharmaceutiques

Avec la solution de Nozomi Networks, la visibilité et la cybersécurité sont faciles à implémenter. Elle améliore la visibilité sur les ressources OT/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 des entreprises pharmaceutiques, la solution de Nozomi Networks permet aux opérateurs d'améliorer leur visibilité opérationnelle, d'évaluer les risques opérationnels, de défendre la propriété intellectuelle de l'entreprise, et de détecter les logiciels malveillants présents sur les réseaux IT/OT.

La solution réside dans la détection des menaces et la visibilité OT/IoT. Sans cela, 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 nombreuses entreprises pharmaceutiques non pas une visibilité claire sur les ressources, les connexions et les communications de leurs usines.

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 et des vulnérabilités. Mais avec la bonne technologie et en se concentrant sur les meilleures pratiques, les fabricants de produits pharmaceutiques peuvent améliorer leur résilience opérationnelle.

EN SAVOIR PLUS

Les plus grandes entreprises pharmaceutiques au monde ont choisi notre solution innovante de visibilité OT et IoT pour accélérer la transformation digitale et réduire les cyber-risques.

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 attribuent à Nozomi Networks le meilleur score

★★★★★

« 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
Pharmaceutique

CONSULTEZ

FICHE PRODUIT
Vantage

TÉLÉCHARGEZ

FICHE PRODUIT
Threat Intelligence

TÉLÉCHARGEZ

8. Références

1. **« Pharmaceutical sector M&A resurgence in 2018 »,** The Pharma Letter, 2018.
2. **« What Has Pharma Learned from the Merck Cyber Attack »,** Pharmaceutical Executive, 2018.
3. **« NotPetya ransomware outbreak cost Merck more than $300M per quarter »** TechRepublic, 2017.
4. **« A Tough Road: Cost To Develop One New Drug Is $2.6 Billion; Approval Rate for Drugs Entering Clinical Development is Less Than 12% »,** Policy & Medicine, 2019.
5. **« Pharma 2020: Supplying the future »,** PwC, 2019.
6. **« Winnti Malware Rampages Through Major International Companies »,** CPO Magazine, 2019.
7. **« Quarterly Threat Report: Q3 2018 »,** Proofpoint, 2018.

Nozomi Networks

La solution leader de sécurité et de visibilité OT et IoT

Nozomi Networks est le leader de la sécurité et de la visibilité sur les systèmes industriels et de l'IoT L'entreprise accélère la transformation digitale en unifiant la visibilité de la cybersécurité pour les plus grandes infrastructures critiques de, l'énergie, la fabrication, l'extraction minière, le transport, la construction automatisée dans le monde entier. Par l'innovation et la recherche, Nozomi Networks rend possible la gestion des cyber-risques grandissants grâce à la visibilité sur le réseau, la détection des menaces et l'expertise opérationnelle de grande qualité.

IB-PHARMA-FR-A4-004

nozominetworks.com