La sécurité dans l'industrie : rapprocher technologies de l'information (IT) et technologies opérationnelles (OT)

Pour les industriels, chaque nouveau point de connexion est une opportunité.

Et un risque.

L'état de la sécurité IT/OT dans l'industrie

Dans une usine, l'augmentation de la connectivité s'accompagne d'un accroissement de la complexité et des problèmes de sécurité.

Chaque nouvelle ressource que vous installez sur le réseau met potentiellement votre sécurité en danger et doit être surveillée.

Dans de nombreuses usines, le nombre croissant de ressources ne permet pas de bénéficier d'une visibilité totale sur la sécurité et de réellement comprendre le comportement du réseau à un instant T. Les entreprises ne sont pas en mesure d'identifier à quoi ressemble une activité normale du réseau. Lorsque des conditions anormales surviennent, elles ne disposent d'aucun point de comparaison et ne parviennent pas à identifier les menaces.

Pourquoi manquent-elles de visibilité sur le réseau ? Les environnements de système de contrôle industriel étant constitués de nombreux types d'équipements fonctionnant avec différents protocoles de l'Internet des objets industriel (IIoT), il est difficile, voire impossible, d'avoir une vue centralisée. La diversité des ressources en termes de types et d'âge pose des difficultés que les environnements IT classiques ne rencontrent pas.

Par ailleurs, le secteur industriel est en passe de devenir une cible de plus en plus attrayante pour les cybercriminels, là encore, à cause de toutes ces ressources. Chacune d'elles représente un point d'entrée potentiel. Avec autant de terminaux à leur disposition, les cybercriminels utilisent les ransomwares pour extorquer de l'argent auprès des industriels.

Sans compter que ces derniers utilisent majoritairement des ressources et des équipements vieillissants. Ayant été créés à une époque bien antérieures aux menaces actuelles, ces équipements ne sont pas conçus pour se prémunir contre les cyberattaques high-tech complexes. Et c'est aux équipes IT et opérationnelles de prendre le relais.

Pour éviter les problèmes, les équipes opérationnelles doivent assumer leur responsabilité en matière de cybersécurité.

Mais les équipes IT détiennent les clés et l'expertise.

Les défis de la cybersécurité pour les équipes opérationnelles

Les opérations de fabrication évoluent et deviennent de plus en plus connectées. Elles libèrent de nouveaux niveaux de productivité et de bénéfices pour l'industrie.

Les professionnels des technologies opérationnelles étant censés maîtriser les rouages d'une usine, ils doivent aussi évoluer. Et, en effet, les professionnels des technologies opérationnelles sont de plus en plus qualifiés en technologies de réseau et en connectivité. Mais nombreux sont ceux qui n'ont pas reçu une formation ou un enseignement suffisants en matière de cybersécurité pour gérer les nuances et les pièges de la lutte contre les ransomwares avancés ou les nouvelles menaces.

Ainsi, les usines se trouvent dans une position délicate : les équipes opérationnelles dépendent des équipes IT, qui ne se trouvent pas nécessairement sur place, pour garantir la sécurité et gérer les opérations connectées. Et ce, même si la plupart des équipes IT maîtrisent rarement la complexité des opérations de l'usine et les technologies de fabrication.

En raison de systèmes disparates (situation encore aggravée par l'écart physique ou virtuel), les équipes opérationnelles ont souvent une visibilité limitée sur les politiques de sécurité IT. Lorsqu'elles modifient le système de contrôle, elles peuvent accidentellement enfreindre les politiques de sécurité IT, et potentiellement conduire à une attaque ou provoquer une interruption non prévue.

De quoi les équipes opérationnelles ont-elles besoin ?

Pour assurer la continuité des opérations, les équipes opérationnelles doivent être plus autonomes, notamment en matière de sécurité. Sans visibilité sur le réseau, elles ne peuvent pas comprendre l'activité ou identifier les anomalies. Et si elles ne sont pas en mesure de gérer et de déployer les politiques de sécurité, elles dépendent trop largement des équipes IT, ce qui allonge les temps de réponse, crée de la confusion et nuit à la productivité.

Bien entendu, les équipes IT doivent aussi garder le contrôle. Pour la plupart des entreprises, elles représentent le centre d'expertise en matière de cybersécurité, mais dans l'industrie, elles ont besoin des équipes opérationnelles pour travailler efficacement.

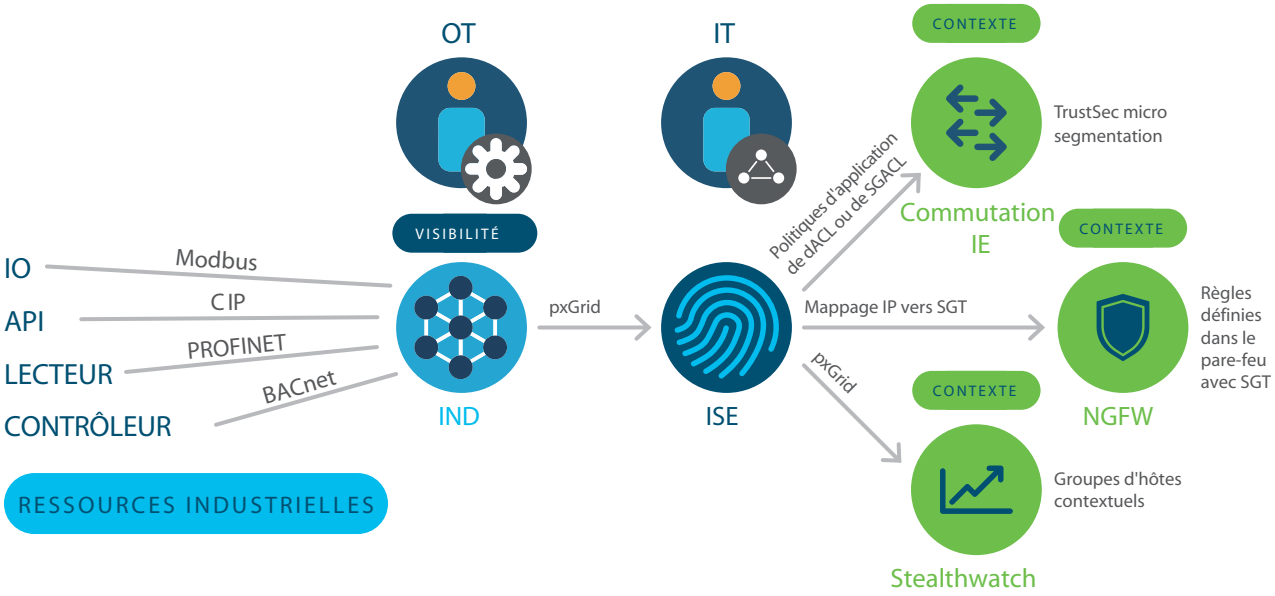
Avec les solutions de sécurité Cisco pour l'industrie, les équipes IT gardent le contrôle.

Mais les équipes opérationnelles obtiennent aussi ce dont elles ont besoin.

En combinant Cisco Industrial Network Director (IND), Cisco ISE (Identity Services Engine) et Cisco Stealthwatch, Cisco offre des solutions de sécurité conçues pour répondre aux besoins des équipes IT et opérationnelles.

Grâce à deux fonctions essentielles, ces solutions contribuent à combler le fossé entre technologies de l'information et technologies opérationnelles :

1. Elles offrent une visibilité sur les ressources présentes sur le réseau et donnent aux équipes opérationnelles une vue centralisée de l'activité du réseau afin de leur permettre de mieux reconnaître ce qui est normal et anormal.
2. Elles permettent aux équipes IT de prédéfinir les politiques de sécurité et de les attribuer dynamiquement en fonction des avis et des objectifs des équipes opérationnelles.



Cisco Industrial Network Director (IND)

- Fournit aux équipes opérationnelles une solution de surveillance du réseau conviviale
- Permet au personnel opérationnel de demander des politiques de sécurité en spécifiant leur objectif

Cisco ISE (Identity Services Engine)

- Permet de contrôler pleinement l'accès aux ressources stratégiques
- Permet aux équipes IT de créer des politiques de sécurité qui sont appliquées dynamiquement aux ressources de l'usine en fonction des besoins signalés par les équipes opérationnelles

Cisco Stealthwatch

- Surveille et analyse le trafic réseau pour aider à créer des politiques
- Contribue à accélérer la détection et la correction des menaces

Connexion via le connecteur pxGrid

Cisco Industrial Network Director est une solution de gestion du réseau conçue pour les départements OT.

Cisco IND fournit aux équipes opérationnelles un système facilement intégré pour une surveillance du réseau conviviale. Il permet aux équipes opérationnelles d'avoir une vue complète de leur topologie réseau afin de mieux comprendre ce qui est normal et ce qui est source d'inquiétude.

Les utilisateurs de Cisco IND disposent d'une visibilité intégrale et d'un contrôle total sur les appareils réseau connectés à l'infrastructure Ethernet industrielle. Cisco IND détecte automatiquement les appareils qui utilisent des protocoles industriels courants tels que CIP et PROFINET pour permettre une vue intégrée et dynamique des appareils connectés et de l'infrastructure de réseau.

Connexion à Cisco ISE via Cisco Platform Exchange Grid

Alors que les équipes opérationnelles vaquent à leurs occupations et gèrent la connectivité des ressources, Cisco IND communique avec Cisco ISE. Le personnel opérationnel peut spécifier ses objectifs, comme connecter un appareil à un fournisseur distant, et Cisco ISE applique dynamiquement les politiques de sécurité appropriées à ce scénario, en fonction de la précédente définition de la politique IT. C'est Cisco Platform Exchange Grid (pxGrid) qui rend cela possible. Notre plate-forme ouverte et évolutive permet à plusieurs solutions de sécurité de partager facilement des données et de fonctionner de concert.

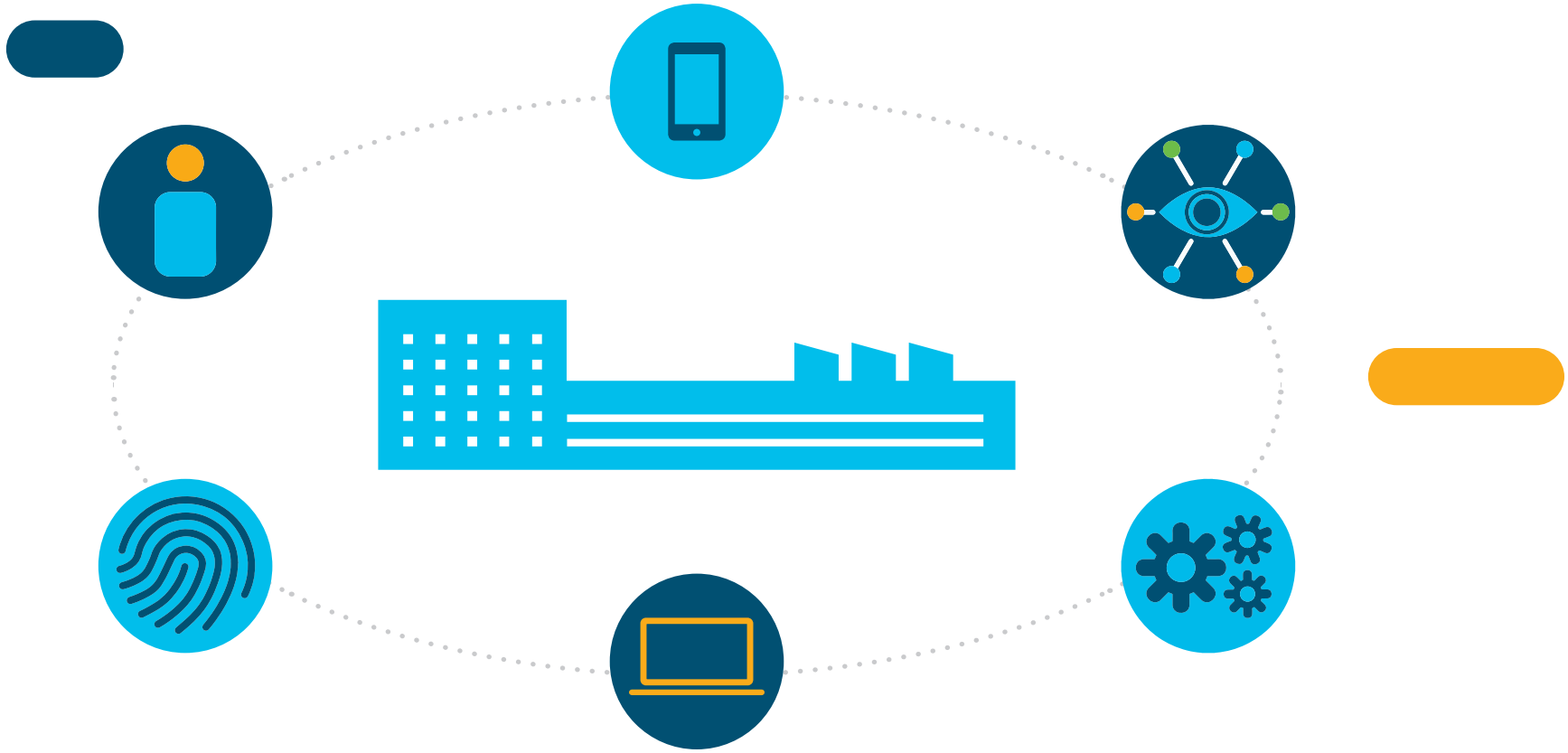
LES BÉNÉFICES

- **Permettre aux équipes opérationnelles d'attribuer dynamiquement des politiques de sécurité définies par l'IT en fonction des besoins :** il suffit de grouper et de baliser les ressources selon les besoins et de spécifier les objectifs via pxGrid afin de déployer les politiques prédéfinies de Cisco ISE
- **Visualiser l'activité du réseau de l'usine :** donne aux équipes opérationnelles une visibilité totale sur les ressources du réseau et industrielles grâce à une surveillance en temps réel
- **Simplifier l'intégration et la détection :** unifie les terminaux industriels tels que les automates programmables industriels, les E/S, les interfaces utilisateur-machine, les lecteurs et bien plus encore sur une même plate-forme ; de puissantes API permettent aussi d'établir une connexion à d'autres systèmes
- **Appliquer des techniques de sécurité d'entreprise à l'usine :** offre des fonctions de sécurité Cisco telles que la microsegmentation TrustSec, les groupes d'hôtes contextuels et les règles de pare-feu basées sur les balises de groupe de sécurité à utiliser sur le réseau de l'usine

Cisco ISE est un puissant outil permettant de contrôler l'accès aux ressources connectées de l'usine.

Cisco ISE donne à votre département IT la possibilité de définir et de déployer des politiques d'accès pour toute la topologie du réseau. Pendant que les équipes opérationnelles travaillent, Cisco ISE fonctionne avec Cisco IND afin de leur permettre d'attribuer des politiques de sécurité prédéfinies aux ressources industrielles, en fonction des définitions précédemment établies par l'équipe IT.

Mais il va encore plus loin. Cisco ISE permet aux équipes IT de contrôler l'accès des experts et des fournisseurs distants, afin qu'ils obtiennent les informations dont ils ont besoin sans compromettre la sécurité. Les fonctionnalités de segmentation, de confinement et de correction garantissent une réponse rapide, précise et efficace aux menaces qui pèsent sur le réseau.



Cisco Stealthwatch est une solution de visibilité et d'analyse évolutive.

Pour définir des politiques de sécurité efficaces, le département IT doit être en mesure de faire la différence entre une journée type et une journée qui sort de l'ordinaire sur leur réseau.

Cisco Stealthwatch offre le niveau de visibilité sur le réseau et la capacité d'analyse approfondie dont les équipes IT ont besoin pour élaborer la meilleure politique de sécurité possible et rester informées de l'activité du réseau.

En outre, Cisco Stealthwatch fournit des informations instantanées sur les menaces ainsi qu'une détection accélérée et une analyse améliorée de celles-ci.

Lorsqu'un trafic anormal est détecté, les équipes IT peuvent rapidement en déterminer l'origine à partir de l'historique des audits et de l'analyse des menaces. Les fonctions de segmentation intégrées renforcent la sécurité du réseau et contribuent à prévenir la propagation des infections.

Exemples d'utilisation

Boostez l'efficacité de vos équipes opérationnelles, tout laissant le contrôle de la sécurité aux équipées IT

CE QUE VOUS POUVEZ FAIRE : donnez aux équipes IT la possibilité de définir des politiques de sécurité qui s'appliquent dynamiquement en fonction des objectifs et de l'avis des équipes opérationnelles.

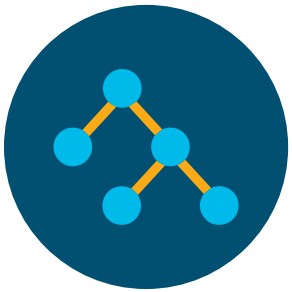
POURQUOI C'EST IMPORTANT : les équipes opérationnelles doivent être en mesure de prendre en charge la sécurité pour garantir la continuité de l'activité, mais pour cela, l'expertise des équipes IT est indispensable.

Donnez à vos équipes opérationnelles une visibilité complète sur la topologie du réseau de l'usine

CE QUE VOUS POUVEZ FAIRE : créez une vue centralisée du réseau afin de permettre aux équipes opérationnelles de se tenir informées de l'état du réseau et d'avoir des informations plus approfondies sur les ressources individuelles.

POURQUOI C'EST IMPORTANT : les équipes opérationnelles ont besoin d'une meilleure visibilité sur la sécurité pour pouvoir la renforcer.

Segmentez les réseaux



CE QUE VOUS POUVEZ FAIRE : créez des zones réseau distinctes dans votre topologie globale pour limiter l'accès et prévenir les infections.

POURQUOI C'EST IMPORTANT : les cybercriminels sont à l'affut de tous les points d'entrée possibles. Par exemple, l'attaque par ransomware de WannaCry en mai 2017 est partie d'un poste de travail unique qui était connecté à tout le réseau. La segmentation contribue à empêcher que les infections se propagent.

Activez l'accès à distance

CE QUE VOUS POUVEZ FAIRE : activez un accès à distance sécurisé afin de permettre à des experts distants, tels que les fournisseurs et les sous-traitants d'aider à résoudre les problèmes, d'appliquer des correctifs et bien plus encore, sans avoir recours aux équipes IT à chaque incident.

POURQUOI C'EST IMPORTANT : permettre aux équipes opérationnelles de donner accès à une sélection de ressources à des entreprises tierces contribue à renforcer l'agilité et à assurer la continuité des opérations.

Le moment est venu de donner aux équipes opérationnelles les outils dont elles ont besoin.

Les solutions de sécurité Cisco pour l'industrie permettent aux industriels d'offrir à leurs équipes opérationnelles la possibilité d'appliquer des politiques de sécurité et de bénéficier d'une meilleure visibilité sur la sécurité, tout laissant le contrôle aux équipes informatiques.

En combinant Cisco ISE, Cisco IND et Cisco Stealthwatch, nos solutions proposent une vue en temps réel de la topologie du réseau ainsi que des fonctionnalités d'alerte, de segmentation et bien plus encore. Les équipes opérationnelles et IT reçoivent en continu les informations dont elles ont besoin pour garantir la continuité des opérations.

L'ensemble repose sur des technologies que maîtrisent les équipes IT, ce qui renforce la facilité d'utilisation. Enfin, il n'est plus nécessaire de faire appel à plusieurs fournisseurs pour assurer la sécurité de votre réseau.

Pour en savoir plus, rendez-vous sur cisco.com/go/ind