Secureworks®

Secureworks Taegis ManagedXDR pour OT

La solution MDR de Secureworks basée sur la plate-forme SOC Taegis XDR, aide les entreprises à prévenir, détecter et répondre aux menaces Cyber ciblant les environnements industriels dans une approche convergée IT et OT.

Défendez-vous contre les cybermenaces ciblant les actifs de vos réseaux industriels grâce à la Détection et Réponse Managées (MDR) Secureworks® « Taegis™ ManagedXDR for OT ». Protégez les actifs de votre entreprise en offrant une surveillance, une détection et une réponse collaborative et commune à l'ensemble de l'environnement IT et OT de l'organisation. Bénéficiez d'un accès rapide à des experts en sécurité, à des analyses avancées et à une connaissance approfondie du paysage mondial de la menace pour renforcer la résilience face aux cyberattaques et réduire les risques y compris pour vos réseaux industriels.

Raisons pour lesquelles les organisations doivent sécuriser leurs environnements

Perturbations opérationnelles : Les entreprises s'appuient sur leurs systèmes informatiques et opérationnels (IT et OT) pour maintenir les cadences de production et garantir la qualité des produits. Une attaque cyber pourrait perturber ces systèmes, entraînant des temps d'arrêt coûteux, des retards de production et des risques pour la sécurité physique. Par exemple, un temps d'arrêt non planifié coûte environ 9 000 dollars par minute aux fabricants, soit plus de 500 000 dollars toutes les heures.

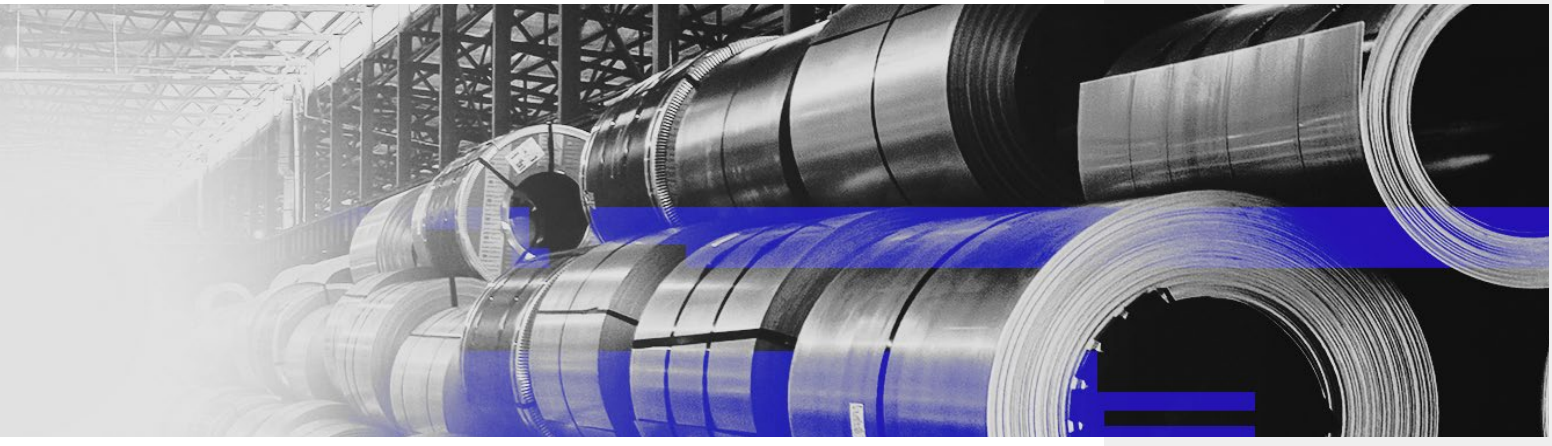
Protection des données sensibles : Les organisations stockent des données sensibles telles que de la propriété intellectuelle, des informations financières et des données clients dans leurs systèmes IT et OT. Une faille de cybersécurité pourrait entraîner le vol de ces données, ce qui pourrait causer des dommages irréparables à la réputation et à la stabilité financière de l'entreprise.

BÉNÉFICES

Assurer la surveillance, la détection et l'investigation des menaces, ainsi qu'une réponse collaborative pour les organisations dotées d'environnements informatiques avec une composante industrielle

Réduire le risque d'interruption de la production et d'atteinte à la réputation et aux bénéfices en cas de cyberattaque

Combler les lacunes internes en matière de cybersécurité dues à l'absence de ressources et au traditionnel manque d'attention portée à la sécurité des technologies



Conformité : Les entreprises doivent se conformer à des exigences réglementaires de plus en plus strictes régissant la protection des données et la cybersécurité. Le non-respect de ces réglementations peut entraîner des amendes, des actions en justice et des dommages à la réputation de l'entreprise.

Risque lié à la chaîne d'approvisionnement : Les organisations travaillent souvent au travers d'un réseau de fournisseurs et de partenaires qui peuvent avoir accès à leurs systèmes IT et OT. Une faille de cybersécurité exploitée au travers d'un accès fournisseur pourrait affecter l'ensemble des opérations, causant des dommages financiers et de réputation significatifs.

Défis autour de la cybersécurité dans l'industrie manufacturière

Les entreprises manufacturières dépendent de leur technologie opérationnelle (OT) pour alimenter leurs opérations, générer des revenus et permettre à leur entreprise de concourir et d'innover. Cependant, la numérisation croissante des processus industriels et la convergence de la technologie de l'information (IT) et de l'OT ont également rendu ces systèmes plus vulnérables aux menaces de cybersécurité.

La transformation numérique a fait converger plusieurs tendances en matière de cybersécurité. Quelques statistiques à ce sujet :

70% Gartner projette qu'en 2025, 70% des organisations avec un volume critique d'assets auront convergé leurs fonctions de sécurité pour l'ensemble des environnements IT et OT.[1]

23% Selon Gartner, le secteur industriel est celui le plus visé par les cyberattaques, avec 23,2 % de l'ensemble des attaques.[2]

65% Selon le rapport Manufacturing Industry Outlook de Deloitte, 65 % des entreprises actives dans les secteurs de la fabrication, du pétrole et du gaz, des services publics et de l'exploitation minière considèrent la cybersécurité comme leur priorité absolue en matière de gouvernance.[3]

Dans l'ensemble, la sécurisation des environnements IT et OT est cruciale pour les entreprises manufacturières afin d'assurer la continuité des activités, protéger les données sensibles et maintenir la conformité réglementaire. En mettant en place des mesures robustes de cybersécurité, les fabricants peuvent minimiser le risque de cyberattaques et se défendre contre les menaces cybernétiques pour l'ensemble de leurs opérations.

1 Gartner Market Guide for OT, August 2022
2 Gartner Product Leaders insight, mars 2022
3 Deloitte's 2022 Manufacturing Industry Outlook

Introduction de la solution MDR pour l'OT basée sur Taegis XDR

Secureworks « Taegis ManagedXDR for OT » est une solution globale de détection et de réponse gérée basée sur la plateforme Taegis XDR, l'alliance technologique avec nos partenaires de solution OT et l'expertise en matière de cybersécurité industrielle des analystes Secureworks. Elle est conçue pour protéger les organisations des cyberattaques ciblant les environnements convergés IT et OT.

Taegis est une plateforme de sécurité cloud-native qui traite plus de 640 milliards d'événements par jour pour plus de 4000 clients. La plateforme propose des centaines d'intégrations, y compris avec les outils OT leaders tels que Dragos, SCADAfence et Claroty, qui sont pris en charge et analysés, en complément des données propriétaires de Secureworks et des renseignements mondiaux sur la menace générés par notre équipe de recherche Counter Threat Unit™ (CTU).

Taegis est soutenu par un vaste réseau d'experts en sécurité constamment disponibles pour nos clients. Notre SOC est doté d'analystes de sécurité en 24/7, et des experts OT aident à enquêter et à fournir des orientations pour remédier aux menaces visant les actifs opérationnels. Les conclusions de la CTU™, ainsi que les informations provenant des 3 000 interventions en réponse à des incidents et des engagements offensifs que Secureworks réalise chaque année, sont intégrées dans Taegis. Les clients ont accès à un « Threat Engagement Manager » qui présente des examens trimestriels de l'activité de menace et fournit des orientations pour renforcer la cyber résilience globale de l'entreprise.

SECUREWORKS MDR FOR OT INCLUS :

- « Taegis ManagedXDR for OT », notre solution de détection et de réponse managée (MDR) permettant la surveillance, la détection, l'investigation et la réponse collaborative aux menaces.
- Accès illimité et rapide à des experts en sécurité dans les 90 secondes, 24 heures sur 24 et 7 jours sur 7
- Des experts en sécurité orientés OT qui enquêtent sur des menaces spécifiques à l'OT et fournissent des orientations pour une réponse collaborative.
- Intégration avec les outils OT des clients (notamment Dragos, SCADAfence et Claroty)
- Mise en place collaborative de processus d'escalade IT et OT, de playbooks de triage et de réponse ainsi que des rapports adaptés.
- Support à l'intégration, chasse aux menaces mensuelle et revues de sécurité trimestrielles avec un responsable de l'engagement en matière de menaces.
- Accès à des services proactifs visant à améliorer la cyber-résilience

CARACTÉRISTIQUES PRINCIPALES :	BÉNÉFICES
Surveillance et détection des menaces IT	La plateforme Taegis assure une surveillance 24 heures sur 24 pour détecter les signes de comportement malveillant dans l'ensemble de vos environnements IT et OT, y compris les terminaux, le réseau, le cloud, l'OT, l'identité, et bien plus encore.
Surveillance du trafic OT	Les intégrations tierces avec Taegis ainsi que les satellites comme nos boitiers IDPS/NDR iSensor préviennent et détectent les activités suspicieuces au sein de vos environnements IT+OT
Triage des alertes et investigation des activités suspectes	Les experts en sécurité de notre SOC étudient les menaces potentielles dans votre environnement IT et OT, et déterminent si une alerte représente une véritable menace. Les analystes de sécurité du SOC sont disponibles dans les 90 secondes grâce à la fonctionnalité de chat en direct de Taegis.
Réponse collaborative	Collaborer avec des experts en sécurité pour coordonner la réponse adéquate aux menaces découvertes dans votre environnement OT
Chasse aux menaces mensuelle	Les playbooks de chasse aux menaces au travers des signaux faibles sont exécutés à partir des données collectées dans les environnements IT et OT.
Intégration avec l'ensemble des outils d'OT du client	Ingestion de Dragos, SCADAfence et Claroty, et accès direct si nécessaire aux consoles de la plateforme par nos experts OT.
Examens trimestriels de la sécurité	Rapport du Threat Engagement Manager afin d'examiner les activités observées dans les environnements IT+OT et fournir des recommandations.
Services proactifs	Unités de service Secureworks incluses pour une utilisation sur un large catalogue de services proactifs permettant d'améliorer la cyber-résilience.

POURQUOI SECUREWORKS ?

Détection supérieure : Nous filtrons le plus grand volume de bruit en provenance de la plupart des sources IT et OT, afin de détecter les véritables menaces.

Réponse inégalée : Veillez à ce que tout incident soit entièrement corrigé avant qu'il n'ait un impact, grâce à un accès illimité, 24 heures sur 24, à notre SOC pour enquêter sur les menaces découvertes et fournir une réponse collaborative.

Une architecture ouverte sans compromis : une architecture ouverte avec des centaines d'intégrations qui évite le verrouillage dans des écosystèmes fournisseurs, permettant aux organisations d'être pérennes et agiles face à l'évolution et à la croissance des outils.

Un meilleur retour sur investissement : Faible coût total de possession en minimisant les coûts liés à l'embauche de ressources de sécurité supplémentaires et à l'achat d'outils, tout en réduisant les risques et en maximisant les investissements les plus importants.

Une vaste expertise en matière de sécurité : Des analystes SOC, des chercheurs en menaces, des personnes chargées de répondre aux incidents, des chasseurs de menaces et du personnel chargé de la réussite des clients, tous travaillant ensemble pour obtenir les meilleurs résultats en matière de sécurité pour nos clients.

Les bonnes solutions d'un leader du secteur : Où que vous en soyez dans votre démarche de sécurité, Secureworks dispose des solutions, de la technologie et du personnel nécessaires pour réduire vos risques, protéger vos investissements et combler vos lacunes en matière de ressources.

Secureworks®

Secureworks® (NASDAQ : SCWX) est un leader mondial de la cybersécurité qui protège les progrès de ses clients grâce à Secureworks Taegis™, une plateforme analytique de sécurité native dans le cloud qui s'appuie sur plus de 20 ans de recherche et de renseignements sur les menaces réelles, améliorant ainsi la capacité des clients à détecter les menaces avancées, à rationaliser et à collaborer sur les enquêtes, et à automatiser les bonnes actions.

For more information, call **1-877-838-7947** to speak to a Secureworks security specialist.
secureworks.com