axians

Le Security Operations Center IT/OT d'Axians

La question n'est pas de savoir si votre entreprise sera compromise, mais quand. Notre Security Operations Center gère et contrôle l'ensemble des mesures de cybersécurité 24 heures sur 24.

VINCI ENERGIES

MISE EN SITUATION DES ENTREPRISES

Il ne suffit pas de protéger

Dans l'environnement IT/OT, les entreprises voient leur flexibilité et leur efficacité nettement améliorées par la numérisation qui, dans le même temps, en fait toutefois des cibles privilégiées pour les criminels. Recourant à des méthodes de plus en plus professionnelles, ces derniers portent préjudice aux entreprises en tentant d'utiliser les données et les informations à leur avantage. Lorsqu'elles cherchent à identifier et à enrayer leurs attaques, les entreprises se retrouvent face à des défis complexes, imputables notamment à la multitude de systèmes déployés, lesquels présentent des vulnérabilités de natures très hétérogènes.

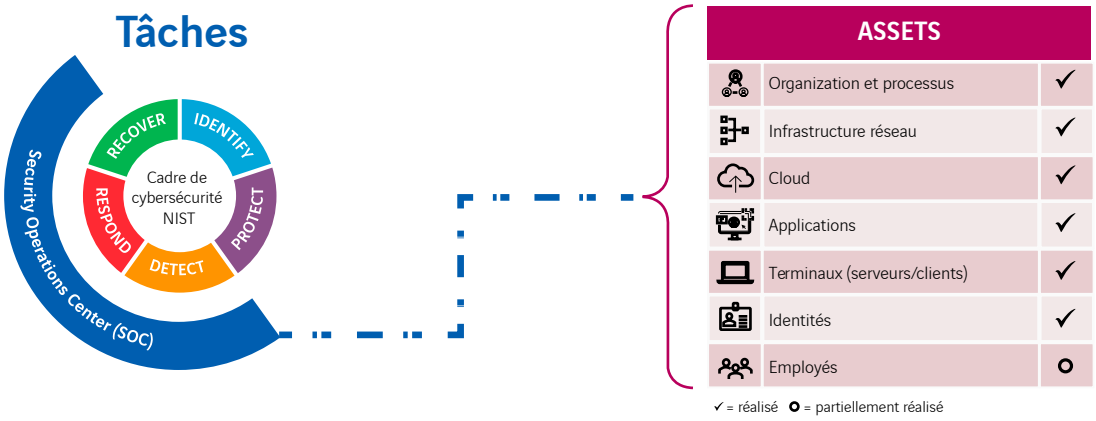
IL EST FRÉQUENT QUE LES ENTREPRISES SOIENT INFORMEÉS PAR DES TIERS QU'ELLES ONT ÉTÉ VICTIMES D'ATTAQUES MENÉES AVEC SUCCÈS

LA PLUPART DES VICTIMES ÉTAIENT DOTÉES DE MESURES PRÉVENTIVES ET DE DISPOSITIFS DE SÉCURITÉ ACTUELS (ET À JOUR)

IL N'EXISTE PAS DE PROTECTION 100 % EFFICACE. LA QUESTION N'EST PAS DE SAVOIR SI L'ATTAQUE VA RÉUSSIR, MAIS QUAND

La mise en situation des entreprises les conduit à prendre des mesures et à réaliser des investissements dans les secteurs de la détection et de la réponse.

Les seules mesures préventives, basées sur le développement d'autres éléments dans le domaine de la protection, sont insuffisantes pour assurer à l'entreprise une protection à long terme contre les dangers des cyberattaques. Pour détecter plus rapidement les incidents de sécurité et y réagir dans les meilleurs délais, les entreprises doivent augmenter leurs investissements de cybersécurité dans les secteurs de la détection et de la réponse.
Chez Axians, le Security Operations Center (SOC) associe experts, outils et processus dans le but de détecter, de prévenir, d'analyser et d'évaluer les risques en matière de cybersécurité. Il soutient par ailleurs la mise en œuvre de mesures visant à pallier les risques de cybersécurité, telles que la fourniture de données forensiques afin de conserver des preuves et de documenter les atteintes à la cybersécurité.



Le cadre de cybersécurité NIST sert de base au service du SOC pour les tâches de détection, de réponse et de reprise et tient compte des actifs ci-dessus. Des systèmes complémentaires (p. ex. scanners de vulnérabilités, etc.) prennent en charge d'autres tâches.

Ce qu'implique le SOC IT/OT d'Axians

La convergence des systèmes IT et OT, associée à l'utilisation croissante d'Internet, y compris dans des environnements industriels, confronte les entreprises à la difficulté de définir des architectures de sécurité préservant à la fois la productivité et la sécurité. Les coûts doivent rester modérés, les normes industrielles, règlementations et directives devant par ailleurs être respectées.

Axians contribue à réaliser cette convergence sécuritaire IT et OT tout en préservant la compétitivité de son cœur de métier. Axians propose un service SOC holistique, intégrant la dimension OT en coopération avec Actemium, notre société sœur. Depuis son Security Operations Center IT/OT hautement spécialisé et certifié ISO 27001, installé dans le centre de compétence uptownBasel, Axians propose la planification, la mise en œuvre et l'intégration à votre infrastructure ainsi qu'un service 24h/24, 7j/7. Notre plateforme en est la pièce maîtresse et permet une application adaptée à vos besoins. Elle comprend aussi des mises à jour permanentes, une Threat Intelligence intégrée et des améliorations continues. De l'analyse des données de log aux rapports personnalisés du tableau de bord du client. Nous proposons ce service tout au long du processus, de la collecte de données au tableau de bord du client.

Niveaux de la plateforme du SOC d´Axians

Un SOC complète les outils d'analyse d'un SIEM par des fonctionnalités étendues de Threat Hunting, telles que des solutions avancées de Threat Intelligence, des scanners de vulnérabilités réseau, une gestion intégrée des vulnérabilités, ainsi que des outils d'analyse de cybersécurité forensique permettant de circonscrire plus efficacement les menaces potentielles.

L’union fait la force : le SOC hybride

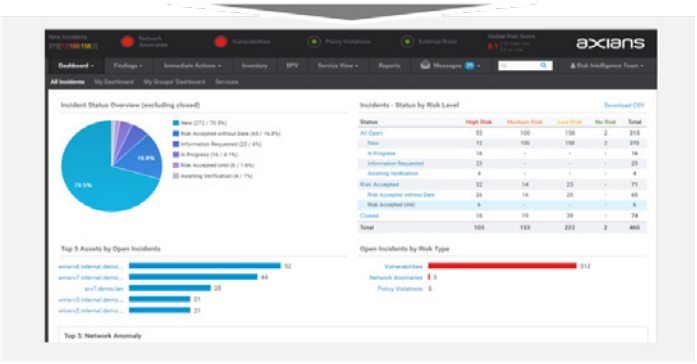
L’externalisation d’un Security Operations Center exige une collaboration étroite entre l’entreprise du client et nos experts en sécurité. Cette coopération est donc pour nous un partenariat qui permettra à nos deux entreprises de relever les défis ensemble. Avec notre solution, nous vous proposons un service de SOC qui va de la collecte des données au tableau de bord du client.

Rapports et tableau de bord

L’élaboration de rapports clairs et intuitifs ou encore le tableau de bord sont des éléments centraux de notre service. Des rapports clairs contribuent à mettre en lumière les incidents de sécurité et les KPI correspondants. À ce stade, nous faisons la distinction entre les deux types de rapports que nous mettons à votre disposition. Le rapport CISO sert de base pour les décisions de risques critiques et le tableau de bord SIEM offre une représentation en temps réel de toutes les informations de sécurité.

CISO - Report

Dashboard für CERT mit allen aktuellen Informationen



Vos avantages

- **Identification rapide des incidents de cybersécurité,** y compris dans des scénarios complexes
- **Protection** des actifs critiques et **garantie** de conformité aux exigences réglementaires
- **Identification précoce de la menace** et évaluation de l'impact sur les services critiques
- **Rapports différenciés par niveau** sur la situation de sécurité actuelle au sein de l'entreprise
- **Analyse et corrélation automatique** de tous les événements pertinents à l'aide de l'intelligence artificielle et de l'expertise humaine
- **Surveillance 24h/24, 7j/7** - Détection rapide des hackers dissimulés dans le réseau de l'entreprise
- **Interface client directement reliée au service du SOC** - Les experts en cybersécurité d'Axians réagissent immédiatement en cas d'incidents de sécurité
- **L'union fait la force – le SOC hybride:** collaboration étroite entre les clients et Axians
- **Intégration à l'infrastructure du client** (p. ex. système de ticket client)
- **Vos données, notre priorité :** stockage des données dans l'infrastructure du client
- **Penser globalement – Protéger localement :** Notre SOC suisse est installé dans le centre de compétences « Uptown Basel » ; autres centres SOC dans la région EMEA
- **Réduction des coûts** - le dispositif fonctionne sans main-d'œuvre interne
- **Convergence IT/OT par Axians et Actemium** – le meilleur de l'IT et de l'OT
- **Un niveau maximal de qualité et de sécurité de l'information** – SOC IT/OT certifié ISO 9001 et ISO 27001

Integriertes Managementsystem
ISO 9001 ISO/IEC 27001

VINCI ENERGIES
CREATING YOUR DATA-DRIVEN FACTORY

ACTEMIUM axians

Industrial performance - digitally improved.

02/2023

axians

Axians IT Services AG · Arlesheim · Rotkreuz · Zurich · Romanel-sur-Lausanne · Martigny
Tél. : +41 61 716 70 70
Courriel : info-ch.security@axians.com · www.axians.ch / soc24x7.services