Cyber-SOC

Centre opérationnel de sécurité IT/OT 24x7

Service managé de détection et de réponse à incident

Alors que la connectivité numérique joue un rôle central dans le développement de l'innovation et de l'économie mondiale, l'augmentation des cyber-attaques constitue un obstacle majeur à notre progression continue et collective.

Le recours accru au cloud public, les supply chains hautement connectées et l'utilisation de systèmes informatiques (IT) et de systèmes de contrôle industriels (ICS) dans des environnements de technologie opérationnelle (OT), ainsi que les nouvelles façons de travailler, ont mis en évidence de nouveaux « angles » d'attaque.

ims NETWORKS

Ensemble, réduisons votre risque cyber

CYBERSÉCURITÉ

1 Réduire la surface d'attaque

Grâce à une compréhension de votre environnement IT, cloud et OT basée sur les risques, notre service de gestion des vulnérabilités (VDR), identifie et hiérarchise les vulnérabilités et les menaces sur vos systèmes. Notre équipe SOC vous accompagne dans la définition et la réalisation de votre plan de correction des vulnérabilités. Dans un objectif d'amélioration continue, ce service permet en outre de valider ou corriger le périmètre de supervision, et la politique de détection.

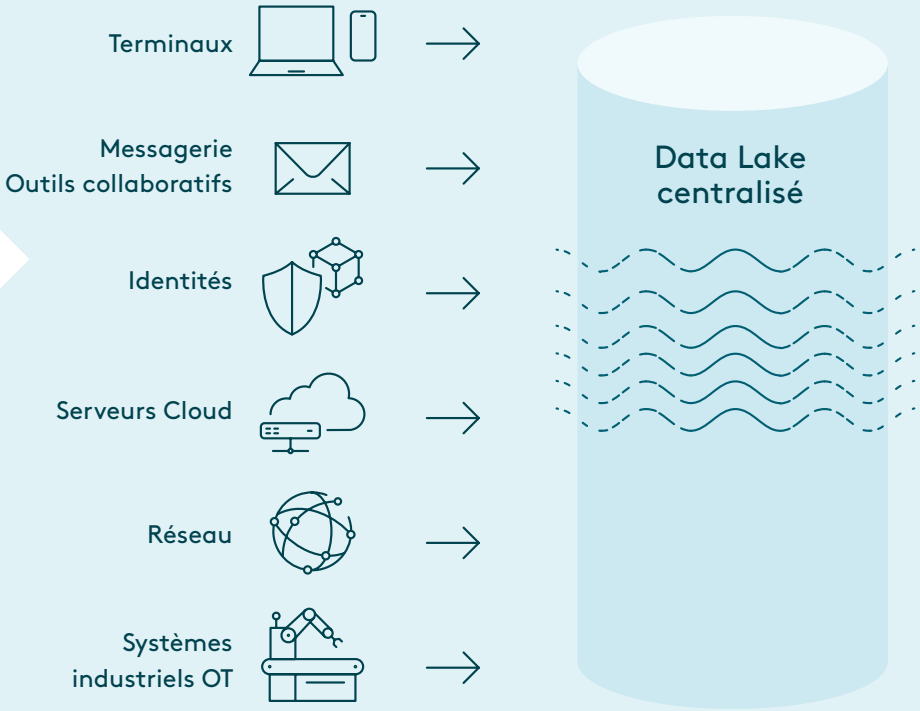
2 Conception & Build

Définition et implémentation des règles de détection en fonction de ce qui est critique et en lien avec le Framework MITRE ATT&CK.

- Définition de l'architecture cible et des scénarios d'attaque
- Déploiement de la plateforme et Intégration de l'ensemble des sources

3 Plateforme de détection SAAS

La plateforme de détection s'étend des points d'extrémité réseau et cloud jusqu'aux réseaux OT avec des capteurs déployés sur les actifs critiques de votre organisation.



Analyse de vulnérabilités

Threat Intelligence

Renseignements complets à partir des feeds de Threat Intelligence et des scans de vulnérabilité

Threat hunting

Recherche proactive de menaces qui auraient pu échapper aux systèmes par les analystes SOC

Anticiper, détecter et réagir avec le Cyber SOC

4 Détection et réponse à incident 24/7

Le SOC IMS Networks détecte en temps réel et permet de réagir aux menaces connues et inconnues, y compris les cyberattaques complexes. Notre service de détection d'incidents comprend la mise en place de la plateforme de détection des incidents de sécurité et le service managé associé en 24/7.

5 Amélioration continue

Dispositif de pilotage et d'accompagnement : Responsable Opérationnel Client (ROC), comités de pilotage et stratégique

Corrélation des informations et analyse avancée

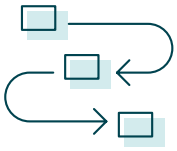
- Corrélation des informations issues des différentes sources et des données du Threat intelligence et du Threat Hunting.
- Moteur d'analyse avancé des données pour détecter les anomalies comportementales, comprenant l'apprentissage automatique, l'UEBA (Advanced Enterprise Behavioral Analytics) et les analyses statistiques.

Détection incident

Analyse automatisée des alertes

Qualification et analyse humaine

Qualification complexe et approfondie humaine



Réponse aux incident et gestion de crise

En cas d'attaque grave ou de crise, elle soutient la cellule de sécurité du client pour diriger les efforts d'investigation, d'atténuation de la menace et de remédiation aux incidents à distance ou sur site.

Opérations d'investigation

Mesures d'atténuation immédiates

Préconisations pour les actions de remédiation

Accompagnement à la remédiation

Réponse d'urgence aux incidents graves

EN 4 H – état des lieux et réponse au téléphone

EN 24 H – intervention d'urgence à distance

EN 48 H – expert de la réponse à incident sur site

- Analyse des logiciels malveillants et reverse engineering
- Analyse criminalistique numérique
- Services de conseil proactifs : entrainement, tests

Notre solution Cyber SOC 24/7

Notre SOC (Security Operations Center) assure en 24/7 un service complet allant de l'analyse des vulnérabilités, à la détection d'incidents de sécurité, jusqu'à la réponse et l'atténuation immédiate en cas de crise majeure.

Périmètre informatique (IT), cloud et opérationnel (OT)

Réactivité élevée avec SLA engageants

Détection adaptée aux nouvelles menaces et threat hunting

Temps de déploiement très court

Reporting personnalisé et amélioration continue

Certifié ISO 27001 et conforme RGPD

Nous vous aidons à concevoir, optimiser et intégrer des infrastructures numériques complexes, et à les opérer dans le cadre de services managés réseau et cybersécurité.

Tous nos services sont certifiés ISO 27001, permettant d'apprécier le risque et de mettre en place des mesures de sécurité et de contrôle appropriées pour assurer la **disponibilité,** la **confidentialité, l'intégrité** et la **traçabilité** de leurs actifs informationnels.

afaq ISO 27001 Sécurité de l'information AFNOR CERTIFICATION

ims NETWORKS

TOULOUSE – PARIS – CASTRES – BORDEAUX – SOPHIA ANTIPOLIS – LYON

contact@imsnetworks.com
+33 (0)5 63 73 50 13
www.imsnetworks.com