



Face à la menace cyber, préservez votre outil de production !

Les systèmes et installations industriels sont aujourd'hui de plus en plus ouverts sur le monde extérieur. Leur interconnexion avec les réseaux bureautiques, les systèmes ERP, et la multiplication des commandes à distance laissent de nombreuses portes ouvertes aux cyberattaquants.

Le développement de l'industrie 4.0 implique les technologies de 5G, plateformes numériques, réalité virtuelle... La plupart des sites industriels français, créés il y a plusieurs dizaines d'années, sont encore peu adaptés à ces évolutions :

- ils utilisent des systèmes hérités, difficilement corrigeables;
- ils utilisent des protocoles de communication et des processus pas ou peu documentés car souvent propriétaires;
- ils possèdent un système de production avec un besoin fort en disponibilité au risque de s'exposer à des conséquences financières et opérationnelles importantes;
- la cartographie des actifs et le suivi des équipements est, au mieux, non réalisé et, au pire, non réalisable.

Le défi consiste à mettre en place une organisation et concevoir une architecture capable d'assurer la disponibilité, l'intégrité et la confidentialité des données entre les systèmes.

SERMA Group, société d'expertise, de conseil et de test pour les technologies électroniques, les systèmes embarqués et les systèmes d'information, travaille depuis plus de 30 ans avec de nombreux clients industriels.

Filiaire à 100% de SERMA Group, SERMA Safety and Security a développé la méthodologie «**CERMA - (Cybersecurity Evaluation and Risk Management)**» pour accompagner les industriels à mettre en place les niveaux de sécurité techniques et organisationnels nécessaires pour faire face aux potentielles cyberattaques.

OFFRE

ETAT DES LIEUX DES INSTALLATIONS EXISTANTES

1

ANALYSE DE RISQUE

2

PROPOSITION DE MESURES DE SÉCURITÉ ORGANISATIONNELLES ET TECHNIQUES

3

ACCOMPAGNEMENT À LA MISE EN OEUVRE DES MESURES DE CYBER-SÉCURITÉ

4

MAINTIEN EN CONDITION DE SÉCURITÉ, TESTS D'INTRUSION

5

NOTRE SAVOIR-FAIRE

1// ÉTAT DES LIEUX DES INSTALLATIONS EXISTANTES

- **Diagnostic de «Maturité» (version flash ou détaillée)** pour évaluer les points forts et les actions à entreprendre à court, moyen et long terme y compris la cartographie des actifs par rapport aux standards et bonnes pratiques de sécurité numérique
- **Audit de « Conformité »** pour évaluer les exigences des normes IEC 62443, NIST SP800-82/SP800-53 ou tout autre référentiel spécifique client

2// ANALYSE DE RISQUE

- **Analyse de risque cyber industriel**, basée sur EBIOS Risk Manager et les recommandations de la norme IEC62443 qui intègre les spécificités de l'IEC 62443 et en particulier l'approche zones et conduits

3// PROPOSITIONS DE MESURES DE SÉCURITÉ ORGANISATIONNELLES ET TECHNIQUES

- Définition d'architecture (approche de défense en profondeur)
- Proposition de mesures de sécurité (organisationnelles et techniques)
- Décontamination de supports amovibles et transfert de données
- Supervision de la sécurité

4// ACCOMPAGNEMENT À LA MISE EN OEUVRE DES MESURES DE CYBER-SÉCURITÉ

- Accompagnement pour la rédaction d'un appel d'offre ou support à réponse à appels d'offres
- Mise en place des processus et du corpus documentaire visant à élever le niveau de sécurité y compris ce qui a trait à la gestion de crise (incident, continuité d'activité, ...) en cas de cyberattaque
- Conception d'architectures et déploiement des solutions dans le contexte client en suivant les bonnes pratiques sécurité
- Documentations techniques : DAT, DI, DR, DEX
- Réalisation du pilotage, déploiement, migration et mise en production
- Support, Maintenance, Contrat d'Assistance de Support Technique (CAST)
- Mise en place d'un SOC (centre des opérations de sécurité)
- Audit, support et suivi des fournisseurs (ISO/IEC)
- Veille technologique

5// MAINTIEN EN CONDITION DE SÉCURITÉ, TESTS D'INTRUSION



NOS DOMAINES D'EXPERTISE



Aéronautique



Communication



Energie



Médical



Transport



Automobile



Défense



Industrie



Spatial



Pétrole et Gaz



contact_S3@serma.com
www.serma-safety-security.com

www.serma.com

