Cybersécurité

SECURE SCADA – Piloter la cybersécurité d'un réseau industriel et prévenir les intrusions OT

Vous allez apprendre à

Avec la transformation numérique des infrastructures industrielles (industrie 4.0, IoT, automatisation), les environnements OT sont devenus des cibles privilégiées des cyberattaquants. L'interconnexion croissante des systèmes industriels avec les systèmes informatiques (IT/OT convergence) expose les automates, les superviseurs SCADA, les capteurs et les équipements réseau à des risques critiques.

Cette formation opérationnelle sur 3 jours permet aux automaticiens, intégrateurs, administrateurs et techniciens OT de comprendre les vulnérabilités spécifiques aux systèmes industriels, d'appliquer les bonnes pratiques de sécurisation, et de mettre en œuvre les recommandations de l'ANSSI.

Public visé

- RSSI
- Intégrateurs OT/SCADA
- Responsables supervision ou maintenance industrielle
- Responsables techniques / industriels
- Administrateurs systèmes industriels
- Automaticiens

Les objectifs de la formation

À l'issue de cette formation, le participant sera capable de :

- Identifier les vulnérabilités critiques d'un système industriel connecté
- Appliquer les bonnes pratiques de défense en profondeur dans un contexte OT
- Sécuriser les automates programmables et leurs interfaces
- Mettre en place un cloisonnement réseau adapté (VLAN, filtrage MAC, ACL)
- Installer et configurer un système de détection d'incident (SIEM) adapté à l'environnement industriel
- Réaliser un audit basique de sécurité sur un réseau OT

Les prérequis de la formation

- Connaissances de base en automatisme industriel (API, supervision)
- Connaissances générales en réseaux IP et architecture de supervision
- Appétence pour les environnements techniques (protocoles, topologies)

Programme de la formation

Jour 1 : Fondamentaux OT & vulnérabilités industrielles
Matin :

- Introduction à la cybersécurité OT
- Risques réels & exemples d'attaques industrielles (Stuxnet, Colonial Pipeline)
- Vulnérabilités SCADA
- Démonstration : attaque sur une supervision vulnérable
- **Quiz n°1 :** Étude de cas sur un incident SCADA réel + 10 QCM

Après-midi :

- Protocoles industriels (Modbus, S7, OPC-UA…)
- Défense en profondeur
- Recommandations de l'ANSSI (guides CSI, guides hygiène)
- **Quiz n°2 :** Étude de cas d'audit de sécurité + 10 QCM

Jour 2 : Cloisonnement, durcissement, sécurisation API
Matin :

- VLAN, DMZ, routage sécurisé
- ACL, filtrage MAC
- Architecture réseau OT sécurisée
- **Quiz n°3 :** Cas d'architecture non segmentée à analyser + 10 QCM

Après-midi :

- Sécurisation des API (S7-1500, mots de passe, affichage)
- Gestion des droits d'accès et des sessions SCADA
- Test d'intrusion simulé sur un automate non protégé
- **Quiz n°4 :** Cas d'une mauvaise configuration SCADA + 10 QCM

Jour 3 : Supervision, détection et audit OT
Matin :

- SIEM, ELK, journalisation dans les systèmes industriels
- Analyse de logs, alertes, faux positifs
- Méthodologie d'analyse de risque simplifiée
- **Quiz n°5 :** Étude de cas sur détection d'intrusion + 10 QCM

Après-midi :

- Introduction au pentest SCADA
- Planification, exécution et restitution
- **Quiz n°6 :** Cas de réponse à incident & plan d'action + 10 QCM

TP final (2h) : Simulation d'intrusion sur un réseau SCADA/IoT avec rapport d'analyse

- Identification des failles
- Remontée d'alertes
- Recommandations post-attaque