SCADA : Sécurité des infrastructures informatiques industrielles

Lien : https://innov-systems.com/formation/scada-securite-des-infrastructures-informatiques-industrielles

DURÉE
3 jours (21h)

RÉFÉRENCE
SEC66

CATÉGORIE
Sécurité Technique : Cryptographie, Protocoles et Infrastructures

OBJECTIFS DE LA FORMATION

À l'issue de cette formation, vous serez capable de :

- Connaitre les bases techniques des systèmes SCADA
- Comprendre comment analyser les risques d'une architecture
- Savoir identifier les menaces et les vulnérabilités
- Auditer un système SCADA
- Développer une politique de cybersécurité

POUR QUI ?

- Responsables de la sécurité des SI
- Architectes
- Chefs de projets
- Administrateurs système et réseau

Programme détaillé

1 / Introduction : enjeux d'une infrastructure industrielle

- Les enjeux d'un système d'information
- Spécificités et contraintes opérationnelles
- Les référentiels sur la sécurité des systèmes d'information industriels
- Les types d'architectures de système SCADA
- Évolution des infrastructures industrielles : Monolithique, IOT
- Ressource et information sur la sécurité

2 / Présentation des composants des infrastructures SCADA

- Partie industrielle (vannes, boutons, capteur, etc.)
- Automates
- Supervision/IHM
- Protocoles industriels (série, IP)

3 / Architectures et technologies réseaux des systèmes SCADA

- Architecture
- Technologies utilisées
- Isolation des réseaux industriels

4 / Risques et menaces

- Etude et compréhension des attaques courantes
- Exemples d'attaques réelles, déroulements et impacts (Stuxnet)
- Les facteurs de risques
- Les grands risques et familles de vulnérabilités
- Les menaces APT (Advanced Persistent Threat)

- Les postures de sécurité moderne des systèmes ICS

5 / Les menaces communes aux SI et SCADA

- La problématique de sécurité dans les systèmes SCADA
- Les problématiques réseau : protocole, support de transmission, interconnexion
- Les problématiques d'évolution : le monde de l'IOT
- Les problématiques de patching : la gestion des mises à jour
- Problématique Logicielle : mobiles, application WEB / TOP 10 OWASP

6 / Introduction à la sécurité des systèmes SCADA

- L'analyse des attaques : construction de l'arbre d'attaque de STUXNET
- Les techniques d'authentification et les méthodes de chiffrement
- Protéger l'ensemble de la chaîne industrielle et les postes opérationnels
- Bien sécuriser les accès et les postes à distance et garantir la disponibilité du réseau

7 / Mesures de sécurité

- Solutions techniques de filtrage, de cloisonnement et de détection d'intrusion
- Firewall industriel
- Diode et passerelle unidirectionnelle industrielle
- Chiffrement IPSEC/SSL
- Sondes de détection d'intrusion
- Analyse passive de trafic
- Honeypot
- Solutions techniques de durcissement système
- Automates de nouvelle génération certifiés CSPN (Siemens S7_1500 et Schneider M580)
- Commutateurs Ethernet (bureautique et industriel)
- Systèmes d'exploitation Windows et Linux
- Applications
- Automates programmables

8 / Auditer son environnement

- Discutions et diagnostic préalable
- Tests et recommandations pour évaluation de la sécurité
- Failles couramment rencontrées
- Définir une politique de sécurité
- Mener une évaluation des risques
- Sécurisation technique
- Sécurisation fonctionnelle
- Focus sur le "patch management"

9 / Détermination des niveaux de classification ANSSI

- Analyse basée sur le guide ANSSI relatif aux réseaux industriels

Approche pédagogique

- Support Ecrit et Projection
- Exposés Interactifs, Podcasts et Vidéos
- Brainstorming et Jeux de Rôle
- Cas Pratiques et Labs inclus pour leur impact opérationnel
- Test de Validation des Acquis des Connaissances

Prochaines dates programmées

05 au 07 Août 2026	Présentiel - Casablanca
30 Sep. au 02 Oct. 2026	Distanciel
25 au 27 Nov. 2026	Distanciel

Autres dates possibles sur demande. Contactez-nous pour organiser une session intra-entreprise.

Réservation & Renseignements

Téléphone : +212 522 247 210
Email : contact@innov-systems.com
Web : https//www.innov-systems.com