Sécurité des réseaux OTICS : normes IEC 62443 et architectures de défense

Lien : https://innov-systems.com/formation/securite-des-reseaux-otics-normes-iec-62443-et-architectures-de-defense

DURÉE	RÉFÉRENCE	CATÉGORIE
5 jours (35h)	**SI63**	**PECB, IEC 62443**

Innov Systems

OBJECTIFS DE LA FORMATION

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

- Comprendre les spécificités des réseaux OT/ICS
- Maîtriser les exigences de la norme IEC 62443
- Concevoir des architectures de sécurité industrielle
- Mettre en œuvre la segmentation des réseaux OT
- Déployer des mécanismes de défense en profondeur
- Sécuriser les équipements industriels critiques
- Superviser et détecter les anomalies industrielles
- Gérer les accès et communications OT sécurisés
- Améliorer la résilience des systèmes industriels
- Réduire les risques de cyberattaques industrielles
- Intégrer IT et OT dans une stratégie de cybersécurité globale
- Étudier des cas concrets d’incidents et de protection OT

POUR QUI ?

- Ingénieurs cybersécurité industrielle
- Architectes OT/ICS
- Ingénieurs systèmes industriels
- Responsables sécurité des infrastructures critiques
- Automatisme et instrumentation industrielle
- Ingénieurs SCADA et DCS
- Consultants en cybersécurité industrielle
- RSSI (Responsables sécurité des systèmes d’information)
- Administrateurs réseaux industriels
- Chefs de projet infrastructure critique
- Techniciens maintenance industrielle
- Toute personne impliquée dans la sécurité des environnements OT/ICS

Innov Systems

Programme détaillé

1 / Introduction aux réseaux OT/ICS

- Définition des environnements OT (Operational Technology) et ICS
- Différences entre IT et OT
- Enjeux critiques des infrastructures industrielles

2 / Menaces et vulnérabilités des systèmes industriels

- Cyberattaques ciblant les environnements industriels
- Risques physiques et impacts opérationnels
- Exemples d'incidents majeurs OT/ICS

3 / Architecture des réseaux industriels

- Segmentation des réseaux OT
- Zones et conduits (zone/conduit model)
- Communication entre systèmes industriels

4 / Norme IEC 62443 : principes fondamentaux

- Présentation de la norme IEC 62443
- Concepts de sécurité par niveaux (security levels SL1 à SL4)
- Exigences pour les systèmes industriels

5 / Gestion des accès et contrôle industriel

- Authentification et autorisation des opérateurs
- Gestion des accès distants sécurisés
- Principe du moindre privilège en OT

Innov Systems

6 / Architectures de défense en profondeur

- Concept de défense en profondeur (Defense in Depth)
- Pare-feux industriels et DMZ OT
- Surveillance des flux industriels

7 / Détection et supervision des environnements OT

- IDS/IPS industriels
- Monitoring des protocoles industriels (Modbus, OPC UA)
- Détection des anomalies opérationnelles

8 / Sécurisation des équipements industriels

- Protection des PLC, SCADA et DCS
- Mise à jour et patch management
- Durcissement des systèmes industriels

9 / Gestion des incidents et continuité d’activité

- Réponse aux incidents en environnement OT
- Plans de continuité et reprise d’activité (PCA/PRA)
- Coordination IT/OT en cas de crise

10 / Études de cas et implémentations industrielles

- Analyse d’attaques sur infrastructures critiques
- Mise en place d’une architecture IEC 62443
- Bonnes pratiques de cybersécurité industrielle

Innov Systems

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

15 au 19 Fév. 2027	Présentiel - Casablanca
12 au 16 Avr. 2027	Présentiel - Casablanca
07 au 11 Juin 2027	Présentiel - Casablanca
02 au 06 Août 2027	Présentiel - Casablanca
27 Sep. au 01 Oct. 2027	Présentiel - Casablanca

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

Innov Systems — Tous droits réservés