Cybersécurité des systèmes IoT industriels (IIoT) menaces, normes IEC 62443 et contre-mesures

Lien : https://innov-systems.com/formation/cybersecurite-des-systemes-iot-industriels-iiot-menaces-normes-iec-62443-et-contre-mesures

DURÉE	RÉFÉRENCE	CATÉGORIE
5 jours (35h)	**SI126**	**Cybersécurité IoT, IIoT et Systèmes Robotisés**

Innov Systems

OBJECTIFS DE LA FORMATION

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

- Comprendre les risques de cybersécurité dans les environnements IIoT
- Maîtriser les concepts fondamentaux de la norme IEC 62443
- Identifier les menaces spécifiques aux systèmes industriels connectés
- Mettre en place une architecture sécurisée IT/OT
- Sécuriser les équipements et protocoles industriels
- Implémenter des stratégies de segmentation réseau et Zero Trust
- Déployer des solutions de détection et réponse aux incidents
- Renforcer la résilience des systèmes industriels
- Réduire les risques de compromission des infrastructures critiques
- Assurer la conformité aux standards de cybersécurité industrielle
- Protéger les environnements SCADA et IoT industriels
- Étudier des cas concrets de sécurisation IIoT

POUR QUI ?

- Ingénieurs cybersécurité
- Security architects
- Ingénieurs OT / ICS
- Ingénieurs industriels et automatisme
- Administrateurs réseaux industriels
- Responsables sécurité SI (RSSI / CISO)
- Consultants cybersécurité industrielle
- Ingénieurs SCADA / PLC
- DevSecOps industriels
- Responsables infrastructures critiques
- Intégrateurs systèmes industriels
- Toute personne impliquée dans la sécurité des systèmes industriels connectés

Innov Systems

Programme détaillé

1 / Introduction à la cybersécurité IIoT

- Transformation digitale de l’industrie et exposition accrue aux cybermenaces
- Différence entre IoT grand public et IIoT industriel
- Enjeux de sécurité pour les systèmes critiques

2 / Architecture des systèmes IIoT

- Composants : capteurs, automates, SCADA, edge devices
- Flux de données industriels et interconnexions IT/OT
- Zones et conduits dans les architectures industrielles

3 / Panorama des menaces cyber IIoT

- Attaques sur SCADA et systèmes industriels
- Malware, ransomware et attaques ciblées OT
- Vulnérabilités des équipements connectés industriels

4 / Surface d’attaque et points de compromission

- Protocoles industriels exposés (Modbus, OPC-UA, MQTT)
- Accès distants et maintenance industrielle
- Risques liés aux fournisseurs et tiers

5 / Norme IEC 62443 : fondamentaux

- Présentation de la norme IEC 62443
- Modèle de zones et conduits sécurisés
- Exigences de sécurité pour les systèmes industriels

Innov Systems

6 / Gestion des identités et des accès industriels

- IAM en environnement OT
- Segmentation des accès opérateurs
- Principe du moindre privilège

7 / Segmentation réseau et Zero Trust industriel

- Micro-segmentation des réseaux OT
- Architecture Zero Trust appliquée à l’industrie
- Séparation IT / OT

8 / Détection et réponse aux incidents

- Monitoring des réseaux industriels
- IDS/IPS industriels et SIEM
- Gestion des incidents de sécurité OT

9 / Sécurisation des équipements et firmware

- Mise à jour sécurisée des firmwares IoT
- Secure boot et durcissement des équipements
- Gestion des vulnérabilités industrielles

10 / Mise en œuvre et cas pratiques

- Déploiement d’une architecture sécurisée IIoT
- Mise en conformité 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

07 au 11 Déc. 2026	Distanciel
25 au 29 Jan. 2027	Présentiel - Casablanca
22 au 26 Mars 2027	Présentiel - Casablanca
17 au 21 Mai 2027	Présentiel - Casablanca
12 au 16 Juil. 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