Sécurité des robots industriels et collaboratifs protéger les contrôleurs et les réseaux de production

Lien : https://innov-systems.com/formation/securite-des-robots-industriels-et-collaboratifs-proteger-les-controleurs-et-les-reseaux-de-production

DURÉE
5 jours (35h)

RÉFÉRENCE
RIO11

CATÉGORIE
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 cyber liés aux robots industriels et cobots
- Identifier les vulnérabilités des contrôleurs et réseaux industriels
- Mettre en place des architectures sécurisées IT/OT
- Sécuriser les communications industrielles
- Appliquer les principes de Zero Trust en environnement industriel
- Protéger les accès aux systèmes robotisés
- Superviser et détecter les incidents de sécurité OT
- Assurer la continuité de production en cas d’attaque
- Renforcer la résilience des infrastructures industrielles
- Déployer des bonnes pratiques de cybersécurité industrielle
- Réduire les risques d’interruption de production
- Étudier des cas concrets de sécurisation de robots industriels

POUR QUI ?

- Ingénieurs cybersécurité industrielle
- Ingénieurs automatisme
- Ingénieurs robotique
- Architectes OT/IT
- Administrateurs réseaux industriels
- SRE industriels
- Responsables production industrielle
- RSSI / CISO
- Techniciens maintenance industrielle
- Intégrateurs systèmes industriels
- Consultants cybersécurité OT
- Toute personne impliquée dans la robotique industrielle et la sécurité des systèmes de production

Innov Systems

Programme détaillé

1 / Introduction à la cybersécurité en robotique industrielle

- Enjeux de sécurité dans les environnements Industrie 4.0
- Différence entre robots industriels et cobots
- Surface d’attaque des systèmes robotisés

2 / Architecture des systèmes robotiques industriels

- Contrôleurs de robots et automates (PLC)
- Réseaux industriels (PROFINET, EtherCAT, Modbus)
- Intégration IT/OT dans les usines connectées

3 / Menaces et vulnérabilités des systèmes robotisés

- Attaques sur les contrôleurs industriels
- Interception et falsification des communications
- Risques liés aux accès distants et maintenance

4 / Sécurisation des contrôleurs de robots

- Durcissement des systèmes embarqués
- Gestion des accès et authentification forte
- Mise à jour et patch management

5 / Sécurisation des réseaux industriels

- Segmentation réseau et zones de sécurité
- Firewalls industriels et IDS/IPS OT
- Zero Trust appliqué aux environnements industriels

Innov Systems

6 / Sécurité des cobots et interaction homme-machine

- Gestion des zones collaboratives sécurisées
- Détection d’anomalies comportementales
- Sécurité fonctionnelle vs cybersécurité

7 / Gestion des identités et des accès (IAM)

- Contrôle des utilisateurs et machines
- Principe du moindre privilège
- Traçabilité des accès aux systèmes industriels

8 / Supervision et monitoring des systèmes industriels

- Surveillance des événements en temps réel
- SIEM appliqué aux environnements OT
- Détection des comportements anormaux

9 / Résilience et continuité de production

- Plans de reprise après incident (DRP)
- Redondance des systèmes critiques
- Stratégies de résilience industrielle

10 / Cas pratiques et bonnes pratiques de sécurisation

- Audit de sécurité d’une cellule robotisée
- Mise en place d’une architecture sécurisée
- Retours d’expérience industriels

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

01 au 05 Fév. 2027	Présentiel - Casablanca
29 Mars au 02 Avr. 2027	Présentiel - Casablanca
24 au 28 Mai 2027	Présentiel - Casablanca
19 au 23 Juil. 2027	Présentiel - Casablanca
13 au 17 Sep. 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