

Cybersécurité des systèmes de contrôle industriel (SCADADCSPLC) : risques et contre-mesures

Lien : https://innov-maroc.com/formation/cybersecurite-des-systemes-de-controle-industriel-scadadcsplc-risques-et-contre-mesures

DURÉE
8 jours (56h)

RÉFÉRENCE
II42

CATÉGORIE
Cybersécurité OT & Sécurité Réseau Industrielle

INNOV MAROC

OBJECTIFS DE LA FORMATION

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

- Comprendre l'architecture et le fonctionnement des systèmes de contrôle industriel SCADA, DCS et PLC.
- Identifier les principales cybermenaces ciblant les infrastructures industrielles.
- Réaliser une analyse des risques conforme aux référentiels internationaux.
- Concevoir des architectures OT sécurisées basées sur la segmentation et le principe Zero Trust.
- Mettre en œuvre des mesures de protection des automates, serveurs SCADA, DCS et équipements de terrain.
- Déployer des solutions de détection d'intrusion, de supervision et de surveillance continue des réseaux industriels.
- Gérer efficacement les vulnérabilités, les mises à jour de sécurité et le durcissement des équipements industriels.
- Élaborer des plans de réponse aux incidents et assurer la continuité des opérations industrielles.
- Sécuriser les principaux protocoles de communication utilisés dans les systèmes industriels.
- Réaliser des audits de cybersécurité et garantir la conformité aux normes IEC 62443, IEC 62351, NIST et ISO 27001.
- Intégrer les nouvelles technologies (IIoT, Cloud, IA) dans une stratégie de cybersécurité industrielle.
- Développer une expertise permettant de concevoir, exploiter et maintenir des systèmes de contrôle industriel résilients face aux cyberattaques tout en garantissant la sécurité, la disponibilité et la continuité des procédés industriels.

INNOV MAROC

POUR QUI ?

- Ingénieurs automatisme et contrôle-commande
- Ingénieurs SCADA et DCS
- Ingénieurs cybersécurité industrielle
- Ingénieurs réseaux industriels
- Ingénieurs instrumentation
- Responsables OT (Operational Technology)
- Responsables cybersécurité (CISO)
- Analystes SOC et SOC OT
- Responsables maintenance industrielle
- Responsables HSE et gestion des risques
- Consultants en cybersécurité industrielle
- Personnel des industries pétrolières et gazières, centrales électriques, réseaux d'eau, industries chimiques, pharmaceutiques, minières, agroalimentaires, cimenteries, sidérurgies, infrastructures critiques, intégrateurs de systèmes, sociétés EPC, bureaux d'études et organismes de certification
- Toute personne impliquée dans la conception, l'exploitation, la maintenance, l'audit ou la sécurisation des systèmes de contrôle industriel souhaitant développer une expertise avancée en cybersécurité des environnements SCADA, DCS, PLC, IIoT et infrastructures critiques.

INNOV MAROC



Programme détaillé

1 / INTRODUCTION À LA CYBERSÉCURITÉ DES SYSTÈMES INDUSTRIELS

- Architecture des environnements IT, OT et ICS
- Fonctionnement des SCADA, DCS, PLC, HMI et RTU
- Panorama des cybermenaces industrielles

2 / ARCHITECTURES DES SYSTÈMES DE CONTRÔLE INDUSTRIEL

- Réseaux industriels et topologies
- Zones, conduits et segmentation selon IEC 62443
- Convergence IT/OT et nouveaux risques

3 / ANALYSE DES RISQUES CYBER

- Identification des actifs critiques
- Analyse des vulnérabilités et scénarios d'attaque
- Méthodes HAZOP, EBIOS, NIST et IEC 62443

4 / MENACES ET VECTEURS D'ATTAQUE

- Malware, ransomware et attaques ciblées
- Intrusions sur les réseaux industriels
- Études de cas : Stuxnet, Triton, Industroyer, BlackEnergy

INNOV MAROC

5 / PROTECTION DES RÉSEAUX OT

- Pare-feu industriels et DMZ
- Segmentation, microsegmentation et Zero Trust
- Contrôle des accès et gestion des identités

6 / SÉCURISATION DES ÉQUIPEMENTS INDUSTRIELS

- Protection des automates PLC, DCS, RTU et IED
- Durcissement des systèmes (Hardening)
- Gestion des correctifs et des configurations

7 / DÉTECTION D'INTRUSION ET SUPERVISION

- IDS/IPS industriels
- SIEM, SOC OT et surveillance continue
- Analyse comportementale et Threat Intelligence

8 / RÉPONSE AUX INCIDENTS ET CONTINUITÉ D'ACTIVITÉ

- Détection, qualification et gestion des incidents
- Plans de reprise (PRA) et continuité (PCA)
- Exercices de crise cyber

9 / CYBERSÉCURITÉ DES PROTOCOLES INDUSTRIELS

- Modbus, DNP3, OPC UA, IEC 61850, PROFINET et EtherNet/IP
- Sécurisation des communications industrielles
- Chiffrement, authentification et intégrité des données

10 / CONFORMITÉ, AUDIT ET GOUVERNANCE

- IEC 62443, NIST SP 800-82, ISO 27001 et IEC 62351
- Audits de cybersécurité industrielle

INOV MAROC

- Gestion documentaire et conformité réglementaire

11 / DIGITALISATION, IIOT ET INDUSTRIE 4.0

- Cybersécurité des objets connectés industriels
- Cloud industriel et Edge Computing
- Intelligence artificielle pour la détection des anomalies

12 / ATELIER PRATIQUE : ÉVALUATION ET SÉCURISATION D'UN SYSTÈME SCADA/DCS

- Réalisation d'une analyse de risques complète d'une architecture industrielle
- Élaboration d'un plan de sécurisation intégrant segmentation, surveillance, détection d'intrusion, réponse aux incidents et conformité aux normes internationales
- Construction d'une feuille de route de cybersécurité visant à renforcer la résilience des systèmes de contrôle industriel

Approche pédagogique

- Support Ecrit et Projection
- Exposés Interactifs, Podcasts et Vidéos
- Brainstorming et Jeux de Rôle
- Mises en Situation pour faciliter l'assimilation
- Cas Pratiques et Labs inclus pour leur impact opérationnel
- Test de Validation des Acquis des Connaissances

INNOV MAROC

Prochaines dates programmées

15 au 24 Fév. 2027	Présentiel - Casablanca
12 au 21 Avr. 2027	Présentiel - Casablanca
07 au 16 Juin 2027	Présentiel - Casablanca
02 au 11 Août 2027	Présentiel - Casablanca
27 Sep. au 06 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-maroc.com
Web : https//www.innov-maroc.com

INNOV MAROC — Tous droits réservés

INNOV MAROC