

Conformité IEC 62443 : mise en place d'un CSMS industriel

Lien :
https://innov-maroc.com/formation/conformite-iec-62443-mise-en-place-dun-csms-industriel

DURÉE
8 jours (56h)

RÉFÉRENCE
II54

CATÉGORIE
Cybersécurité OT & Sécurité Réseau Industrielle

INNOV MAROC

🎯 OBJECTIFS DE LA FORMATION

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

- Comprendre la structure, les principes et les objectifs de la série IEC 62443.
- Comprendre le rôle et les composants d'un Cybersecurity Management System (CSMS).
- Définir le périmètre d'un CSMS adapté à une infrastructure industrielle.
- Mettre en place une gouvernance claire de la cybersécurité des systèmes OT.
- Identifier, inventorier et classifier les actifs industriels selon leur criticité.
- Réaliser une analyse structurée des risques cybersécurité applicables aux environnements ICS/SCADA.
- Concevoir une architecture de sécurité basée sur les concepts de zones et conduits.
- Déterminer les niveaux de sécurité appropriés en fonction des risques et des objectifs de protection.
- Définir les exigences et mesures de sécurité techniques et organisationnelles.
- Mettre en place une démarche de gestion des vulnérabilités, correctifs et changements.
- Structurer les processus de surveillance, détection, réponse aux incidents et retour d'expérience.
- Préparer les audits et constituer les éléments de preuve nécessaires à l'évaluation de la conformité.
- Définir des KPI et une feuille de route permettant d'assurer l'amélioration continue du CSMS.
- Développer une démarche complète permettant de passer d'une approche ponctuelle de cybersécurité à un système de management OT structuré, documenté, auditable et durable.

INNOV MAROC

POUR QUI ?

- Responsables cybersécurité industrielle
- Responsables OT / IT-OT
- RSSI et responsables sécurité des systèmes industriels
- Responsables ICS/SCADA
- Responsables automatisme et contrôle-commande
- Ingénieurs cybersécurité OT
- Ingénieurs réseaux industriels
- Architectes IT/OT
- Ingénieurs systèmes industriels
- Responsables infrastructure et télécommunications industrielles
- Responsables maintenance et fiabilité
- Responsables risques industriels et QHSE
- Responsables conformité et audit
- Chefs de projets Industrie 4.0 et transformation digitale
- Intégrateurs de systèmes ICS/SCADA
- Consultants en cybersécurité industrielle
- Auditeurs internes et responsables gouvernance cyber
- Exploitants d'infrastructures critiques dans les secteurs de l'énergie, pétrole et gaz, chimie, pétrochimie, mines, eau, transport et manufacturing
- Toute personne chargée de concevoir, déployer, maintenir, auditer ou améliorer un système de management de la cybersécurité industrielle conformément aux principes de l'IEC 62443.

INFOV MAROC



Programme détaillé

1 / FONDAMENTAUX DE L'IEC 62443 ET DU CSMS

- Structure et objectifs de la série IEC 62443
- Principes du Cybersecurity Management System (CSMS)
- Différences entre gouvernance IT et gouvernance cybersécurité OT

2 / GOUVERNANCE ET POLITIQUE DE CYBERSÉCURITÉ OT

- Définition de la politique de cybersécurité industrielle
- Rôles, responsabilités et autorités
- Organisation de la gouvernance entre exploitant, intégrateur et fournisseur

3 / PÉRIMÈTRE ET CARTOGRAPHIE DES ACTIFS INDUSTRIELS

- Identification des actifs ICS, SCADA, PLC, DCS et réseaux
- Inventaire des équipements et dépendances
- Classification des actifs selon leur criticité

4 / ANALYSE DES RISQUES CYBERSÉCURITÉ INDUSTRIELLE

- Identification des menaces et vulnérabilités
- Analyse des scénarios d'attaque
- Évaluation de la probabilité, de l'impact et du niveau de risque

INNOV MAROC

5 / ZONES, CONDUITS ET ARCHITECTURE DE SÉCURITÉ

- Définition des zones de sécurité
- Sécurisation des conduits de communication
- Segmentation des réseaux et séparation IT/OT

6 / DÉFINITION DES SECURITY LEVELS

- Principes des Security Levels (SL)
- Détermination du niveau de sécurité cible
- Alignement des mesures de protection avec les risques identifiés

7 / EXIGENCES DE SÉCURITÉ ET MESURES DE PROTECTION

- Contrôle des accès et authentification
- Gestion des communications et segmentation
- Protection des logiciels, configurations et données industrielles

8 / GESTION DES VULNÉRABILITÉS ET DES CHANGEMENTS

- Identification et traitement des vulnérabilités
- Gestion des correctifs en environnement OT
- Change Management et maintien de l'état sécurisé

9 / SURVEILLANCE, DÉTECTION ET RÉPONSE AUX INCIDENTS

- Monitoring des réseaux et systèmes industriels
- Journalisation et analyse des événements
- Procédures de réponse aux incidents et retour d'expérience

10 / AUDIT, ÉVALUATION ET PREUVES DE CONFORMITÉ

- Préparation aux audits IEC 62443
- Documentation et traçabilité des mesures de sécurité

INOV MAROC

- Identification et traitement des écarts de conformité

11 / INDICATEURS ET AMÉLIORATION CONTINUE DU CSMS

- Définition des KPI et indicateurs de maturité cyber
- Revues périodiques du système de management
- Plans d'amélioration et suivi des actions correctives

12 / ATELIER PRATIQUE : DÉPLOIEMENT D'UN CSMS INDUSTRIEL

- Cartographie d'une architecture OT et identification des actifs critiques
- Analyse des risques et définition des zones, conduits et niveaux de sécurité
- Construction d'une feuille de route CSMS intégrant gouvernance, procédures, mesures techniques, audits, indicateurs et amélioration continue

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

Prochaines dates programmées

01 au 10 Fév. 2027	Présentiel - Casablanca
29 Mars au 07 Avr. 2027	Présentiel - Casablanca
24 Mai au 02 Juin 2027	Présentiel - Casablanca
19 au 28 Juil. 2027	Présentiel - Casablanca
13 au 22 Sep. 2027	Présentiel - Casablanca

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

INOV MAROC

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