Management de la cybersécurité industrielle (IEC 62443) appliquée aux réseaux de gaz et vapeur

Lien : https://innov-maroc.com/formation/management-de-la-cybersecurite-industrielle-iec-62443-appliquee-aux-reseaux-de-gaz-et-vapeur

DURÉE
5 jours (35h)

RÉFÉRENCE
AGV68

CATÉGORIE
Réglementation et Conformité

OBJECTIFS DE LA FORMATION

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

- Comprendre les principes fondamentaux de la cybersécurité appliquée aux systèmes industriels OT.
- Maîtriser les exigences de la norme IEC 62443 et des principaux référentiels internationaux.
- Concevoir une architecture réseau sécurisée pour les installations de gaz et de vapeur.
- Identifier les vulnérabilités et évaluer les risques cyber des infrastructures industrielles.
- Mettre en œuvre les mesures de protection adaptées aux systèmes SCADA, DCS, PLC et IIoT.
- Déployer des mécanismes de surveillance, de détection et de réponse aux incidents de cybersécurité.
- Sécuriser les communications industrielles, les accès distants et les équipements connectés.
- Élaborer une gouvernance de cybersécurité conforme aux bonnes pratiques internationales.
- Développer des plans de continuité d'activité et renforcer la résilience des installations critiques.
- Être capable de concevoir, piloter et améliorer un programme complet de cybersécurité industrielle garantissant la disponibilité, l'intégrité, la confidentialité et la sûreté des réseaux de gaz et de vapeur.

POUR QUI ?

- Ingénieurs cybersécurité industrielle (OT)
- Ingénieurs automatisme, instrumentation et contrôle-commande
- Ingénieurs SCADA, DCS et systèmes industriels
- Responsables maintenance et fiabilité
- Responsables HSE et gestion des risques industriels
- Responsables des infrastructures critiques et des utilités industrielles
- Administrateurs de réseaux industriels et spécialistes IIoT
- Responsables informatique industrielle (IT/OT)
- Auditeurs cybersécurité, consultants IEC 62443 et organismes de contrôle
- Sociétés d'ingénierie, entreprises EPC, exploitants des secteurs pétrolier, gazier, chimique, énergétique, pharmaceutique, agroalimentaire et manufacturier, ainsi que toute personne impliquée dans la conception, l'exploitation, la sécurisation ou l'audit des réseaux industriels de gaz et de vapeur.

Programme détaillé

1 / FONDAMENTAUX DE LA CYBERSÉCURITÉ INDUSTRIELLE ET DES SYSTÈMES OT

- Différences entre les environnements IT et OT
- Architecture des réseaux de gaz, de vapeur et des utilités industrielles
- Menaces cyber visant les infrastructures critiques

2 / NORMES ET RÉFÉRENTIELS INTERNATIONAUX

- Présentation de la norme IEC 62443
- ISO/IEC 27001, NIST Cybersecurity Framework et NIS2
- Exigences réglementaires applicables aux infrastructures industrielles

3 / ARCHITECTURE SÉCURISÉE DES RÉSEAUX INDUSTRIELS

- Segmentation des réseaux OT et IT
- Conception des zones et conduits (Zones & Conduits)
- Sécurisation des protocoles industriels (Modbus, OPC UA, Profinet, DNP3)

4 / GESTION DES RISQUES ET ÉVALUATION DES VULNÉRABILITÉS

- Identification des actifs critiques
- Analyse des risques cyber et des scénarios d'attaque
- Audits techniques, tests de vulnérabilité et plans de remédiation

5 / PROTECTION DES ÉQUIPEMENTS INDUSTRIELS

- Sécurisation des automates PLC, DCS, SCADA et RTU
- Gestion des accès, authentification et contrôle des privilèges
- Durcissement (Hardening) des équipements industriels

6 / SURVEILLANCE, DÉTECTION ET RÉPONSE AUX INCIDENTS

- Détection des intrusions (IDS/IPS) et supervision SOC
- Journalisation, SIEM et surveillance des événements OT
- Gestion des incidents cyber et procédures de reprise

7 / CYBERSÉCURITÉ DES SYSTÈMES CONNECTÉS ET IIOT

- Sécurisation des capteurs intelligents et objets connectés
- Cloud industriel, Edge Computing et Digital Twin
- Gestion sécurisée des accès distants et de la télémaintenance

8 / GOUVERNANCE, CONFORMITÉ ET CULTURE CYBER

- Élaboration d'une politique de cybersécurité industrielle
- Sensibilisation et formation du personnel
- Gestion documentaire, audits et amélioration continue

9 / CONTINUITÉ D'ACTIVITÉ ET RÉSILIENCE DES INSTALLATIONS

- Plans de continuité d'activité (PCA) et de reprise après sinistre (PRA)
- Sauvegardes, redondance et haute disponibilité
- Exercices de simulation et gestion de crise cyber

10 / ÉTUDES DE CAS ET STRATÉGIE DE CYBERSÉCURITÉ DES RÉSEAUX DE GAZ ET DE VAPEUR

- Analyse d'incidents cyber sur des infrastructures industrielles

- Élaboration d'une feuille de route conforme à l'IEC 62443
- Construction d'un programme de cybersécurité intégrant gouvernance, protection, surveillance, résilience 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

09 au 13 Nov. 2026	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