

Cybersécurité des Systèmes de Contrôle Industriel Hydrauliques (OT Security)

Lien : https://innov-maroc.com/formation/cybersecurite-des-systemes-de-controle-industriel-hydrauliques-ot-security

DURÉE
5 jours (35h)

RÉFÉRENCE
HM56

CATÉGORIE
Automatisme et Commande des Systèmes Hydrauliques

INNOV MAROC

🎯 OBJECTIFS DE LA FORMATION

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

- ✔ Comprendre les spécificités de la cybersécurité des environnements OT appliqués aux infrastructures hydrauliques.
- ✔ Identifier les architectures et composants d'un système de contrôle industriel hydraulique.
- ✔ Distinguer les risques cyber propres aux environnements IT et OT.
- ✔ Identifier les vulnérabilités des PLC, RTU, HMI, SCADA, capteurs, actionneurs et réseaux industriels.
- ✔ Réaliser une première analyse de risques cyber sur une installation hydraulique.
- ✔ Mettre en œuvre les principes de segmentation et de défense en profondeur des réseaux OT.
- ✔ Sécuriser les accès locaux, distants et privilégiés aux systèmes industriels.
- ✔ Protéger les configurations, programmes automates, sauvegardes et paramètres critiques.
- ✔ Mettre en place des mécanismes de surveillance et de détection des comportements anormaux.
- ✔ Organiser une démarche de gestion des vulnérabilités compatible avec les contraintes de disponibilité des systèmes industriels.
- ✔ Élaborer un plan de réponse aux incidents et de continuité d'activité adapté aux infrastructures hydrauliques.
- ✔ Développer une stratégie globale permettant de renforcer la résilience cyber des stations de pompage, réseaux d'eau, barrages, systèmes SCADA et installations de traitement.

INNOV MAROC

POUR QUI ?

- Ingénieurs automaticiens
- Ingénieurs en cybersécurité industrielle
- Ingénieurs OT/ICS
- Ingénieurs hydrauliciens
- Ingénieurs électrotechniciens et électromécaniciens
- Ingénieurs instrumentation et contrôle-commande
- Responsables SCADA et télégestion
- Responsables automatisation et systèmes industriels
- Responsables IT/OT et infrastructure réseau
- Responsables cybersécurité et RSSI
- Responsables exploitation et maintenance des installations hydrauliques
- Techniciens automatisme, instrumentation et maintenance industrielle
- Administrateurs réseaux industriels
- Responsables de stations de pompage et de traitement d'eau
- Responsables de barrages et infrastructures hydrauliques critiques
- Responsables QHSE et gestion des risques
- Bureaux d'études, intégrateurs industriels et sociétés d'ingénierie
- Exploitants de réseaux d'eau, stations de traitement, systèmes d'irrigation et infrastructures hydrauliques
- Cadres des organismes publics chargés de l'eau, de l'énergie, des infrastructures et de la sécurité numérique
- Toute personne impliquée dans la conception, l'exploitation, la maintenance, la supervision ou la sécurisation des systèmes de contrôle industriels hydrauliques.

INNOV MAROC



Programme détaillé

1 / FONDAMENTAUX DE LA CYBERSÉCURITÉ OT

- Différences entre IT, OT et IoT industriel
- Architecture des systèmes de contrôle hydrauliques
- Menaces et vulnérabilités spécifiques aux environnements industriels

2 / ARCHITECTURE DES SYSTÈMES OT HYDRAULIQUES

- PLC/API, RTU, HMI et systèmes SCADA
- Capteurs, actionneurs, variateurs et équipements intelligents
- Réseaux industriels et architectures de télégestion

3 / IDENTIFICATION DES MENACES ET ANALYSE DES RISQUES

- Menaces internes et externes
- Malware, ransomware, compromission des comptes et accès non autorisés
- Analyse de criticité des équipements et scénarios d'attaque

4 / SÉCURISATION DES RÉSEAUX INDUSTRIELS

- Segmentation des réseaux IT/OT
- VLAN, pare-feu industriels et zones de sécurité
- DMZ industrielle et contrôle des communications interzones

INNOV MAROC

5 / PROTECTION DES PLC, RTU ET ÉQUIPEMENTS DE CONTRÔLE

- Gestion des accès et authentification
- Sécurisation des configurations et programmes automates
- Sauvegarde, contrôle d'intégrité et gestion des modifications

6 / CYBERSÉCURITÉ DES SYSTÈMES SCADA ET TÉLÉGESTION

- Sécurisation des serveurs SCADA et postes opérateurs
- Gestion des comptes, privilèges et accès distants
- Sécurisation des communications avec les stations déportées

7 / SURVEILLANCE ET DÉTECTION DES INCIDENTS OT

- Journalisation et analyse des événements
- Détection des comportements anormaux
- IDS/IPS industriels, SIEM et supervision de la sécurité OT

8 / GESTION DES VULNÉRABILITÉS ET MAINTENANCE SÉCURISÉE

- Inventaire des actifs OT
- Évaluation et priorisation des vulnérabilités
- Patch management et contraintes de disponibilité des installations

9 / RÉPONSE AUX INCIDENTS ET CONTINUITÉ D'ACTIVITÉ

- Élaboration d'un plan de réponse aux incidents cyber
- Isolement et confinement d'un système compromis
- Sauvegarde, restauration et maintien des fonctions critiques

10 / ATELIER PRATIQUE : PLAN DE SÉCURISATION D'UNE INSTALLATION HYDRAULIQUE

- Cartographie des actifs PLC/SCADA/réseaux et identification des points critiques

INOV MAROC

- Élaboration d'une architecture sécurisée avec segmentation, contrôle des accès, surveillance et sauvegardes
- Construction d'un plan intégrant analyse des risques, défense en profondeur, détection, réponse aux incidents, continuité d'activité et retour d'expérience

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

12 au 18 Jan. 2027	Présentiel - Casablanca
08 au 12 Mars 2027	Présentiel - Casablanca
03 au 07 Mai 2027	Présentiel - Casablanca
28 Juin au 02 Juil. 2027	Présentiel - Casablanca
23 au 27 Août 2027	Présentiel - Casablanca

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

INNOV MAROC

Réservation & Renseignements

Téléphone : +212 522 247 210
Email : contact@innov-maroc.com
Web : https//www.innov-maroc.com

INNOV MAROC — Tous droits réservés