

Cybersécurité Industrielle : Maîtriser les Vulnérabilités et Renforcer vos Systèmes MES et ERP

Lien : https://innov-maroc.com/formation/cybersecurite-industrielle-maitriser-les-vulnerabilites-et-renforcer-vos-systemes-mes-et-erp

DURÉE
5 jours (35h)

RÉFÉRENCE
II29

CATÉGORIE
Cybersécurité OT & Sécurité Réseau Industrielle

INNOV MAROC

🎯 OBJECTIFS DE LA FORMATION

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

- ✔ Comprendre les vulnérabilités et risques propres aux systèmes industriels et MES
- ✔ Maîtriser les bonnes pratiques et standards internationaux de cybersécurité industrielle
- ✔ Savoir sécuriser les flux de données, l’accès aux systèmes et la traçabilité
- ✔ Être capable de détecter, analyser et répondre efficacement aux incidents
- ✔ Développer une culture de sécurité et un plan de formation continue pour le personnel
- ✔ Assurer la conformité aux normes et recommandations internationales
- ✔ Intégrer les correctifs et mises à jour de manière sécurisée
- ✔ Réduire les risques liés aux attaques ciblant ERP, MES et automates industriels
- ✔ Améliorer la résilience des systèmes industriels face aux cybermenaces
- ✔ Former les participants à l’utilisation d’outils de sécurité spécialisés pour ICS

👥 POUR QUI ?

- ✔ Informaticiens et ingénieurs systèmes travaillant dans l’industrie
- ✔ Responsables sécurité informatique dans les environnements industriels
- ✔ Opérateurs et administrateurs de systèmes MES et ERP industriels
- ✔ Techniciens de maintenance des systèmes automatisés
- ✔ Analystes SOC spécialisés en systèmes industriels
- ✔ Chefs de projet IT/OT pour l’urbanisation des systèmes d’information
- ✔ Toute personne souhaitant renforcer la sécurité des infrastructures industrielles

INOV MAROC



Programme détaillé

1 / Compréhension des systèmes industriels et MES

- Identifier les composants critiques des systèmes industriels (PLC, SCADA, MES)
- Comprendre les flux de données et l'urbanisation des systèmes d'information industriels
- Analyser les dépendances entre systèmes ERP, MES et traçabilité

2 / Analyse des vulnérabilités spécifiques aux environnements industriels

- Découvrir les failles classiques dans les systèmes MES et ERP industriels
- Identifier les vecteurs d'attaque physique et logique sur les automates et serveurs
- Utiliser des outils de scanning ICS pour détecter les vulnérabilités

3 / Normes et standards de cybersécurité industrielle

- Appliquer les recommandations NIST ICS Security Guidelines
- Implémenter les bonnes pratiques de la norme ISA/IEC 62443
- Connaître les contrôles SANS pour la sécurité des systèmes industriels

4 / Gestion des accès et authentification

- Mettre en place une gestion stricte des utilisateurs et des privilèges
- Sécuriser l'authentification des applications MES et ERP industriels
- Mettre en œuvre une politique de contrôle d'accès basée sur les rôles

INNOV MAROC

5 / Sécurisation des communications et réseaux industriels

- Segmenter les réseaux industriels et IT pour limiter les risques
- Chiffrer les flux de données critiques et sensibles
- Surveiller le trafic réseau pour détecter les anomalies et intrusions

6 / Protection des données et traçabilité

- Sécuriser les bases de données MES et ERP contre les accès non autorisés
- Assurer l’intégrité et la disponibilité des données industrielles
- Implémenter des journaux de traçabilité conformes aux standards industriels

7 / Détection et réponse aux incidents

- Développer des plans de réponse aux incidents ICS
- Mettre en place des systèmes de détection d’intrusion spécifiques aux environnements industriels
- Effectuer des simulations et tests de réaction face aux attaques

8 / Gestion des correctifs et mises à jour

- Planifier et déployer les mises à jour des systèmes MES, ERP et automates
- Évaluer l’impact des correctifs sur les opérations industrielles
- Tester les correctifs dans des environnements simulés avant déploiement

9 / Audits et conformité

- Réaliser des audits internes de sécurité industrielle
- Vérifier la conformité aux normes ISA/IEC 62443 et aux directives internes
- Préparer les rapports d’audit et recommandations d’amélioration

10 / Formation continue et sensibilisation

- Former le personnel IT et opérationnel aux bonnes pratiques de cybersécurité

INNOV MAROC

- Organiser des ateliers pratiques de sécurisation des systèmes industriels
- Mettre en place un programme de veille sur les nouvelles menaces ICS

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 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.

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