



Audit de sécurité des systèmes de contrôle industriel (Pentest OT)

Lien :

<https://innov-maroc.com/formation/audit-de-securite-des-systemes-de-controle-industriel-pentest-ot>

 DURÉE
8 jours (56h)

 RÉFÉRENCE
II53

 CATÉGORIE
**Cybersécurité OT &
Sécurité Réseau
Industrielle**

© OBJECTIFS DE LA FORMATION

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

- ✓ Comprendre les spécificités de la cybersécurité des environnements OT/ICS.
- ✓ Identifier les principaux actifs composant une architecture industrielle : PLC, RTU, SCADA, DCS et SIS.
- ✓ Cartographier les équipements, flux de communication et dépendances d'un réseau industriel.
- ✓ Comprendre les principaux protocoles de communication utilisés dans les environnements OT.
- ✓ Identifier les vulnérabilités techniques et les mauvaises configurations susceptibles d'affecter les systèmes industriels.
- ✓ Maîtriser une méthodologie structurée d'audit et de test d'intrusion adaptée aux environnements OT.
- ✓ Réaliser des contrôles de sécurité non intrusifs afin de limiter les risques de perturbation des procédés.
- ✓ Évaluer la sécurité des automates, stations d'ingénierie, postes opérateurs, serveurs et équipements réseau.
- ✓ Analyser la segmentation entre réseaux IT et OT et identifier les chemins d'accès à risque.
- ✓ Mettre en place des mécanismes de surveillance, détection et journalisation adaptés aux environnements industriels.
- ✓ Élaborer des recommandations de durcissement et de remédiation compatibles avec les exigences de disponibilité et de sûreté des installations.
- ✓ Produire un rapport d'audit de cybersécurité OT hiérarchisant les vulnérabilités, les risques cyber-physiques et les actions correctives prioritaires.

POUR QUI ?

- ✓ Ingénieurs cybersécurité industrielle
- ✓ Ingénieurs OT/ICS
- ✓ Ingénieurs automatisme et contrôle-commande
- ✓ Ingénieurs instrumentation
- ✓ Ingénieurs réseaux industriels
- ✓ Ingénieurs systèmes et infrastructure
- ✓ Responsables cybersécurité
- ✓ Responsables sécurité OT
- ✓ Responsables automatisme et contrôle-commande
- ✓ Responsables IT/OT
- ✓ Responsables SOC et sécurité industrielle
- ✓ Administrateurs réseaux et systèmes industriels
- ✓ Automaticiens et ingénieurs PLC/SCADA/DCS
- ✓ Architectes réseaux OT
- ✓ Analystes SOC spécialisés en environnements industriels
- ✓ Auditeurs et consultants en cybersécurité industrielle
- ✓ Responsables risques et conformité
- ✓ Responsables QHSE et sécurité des procédés
- ✓ Intégrateurs de systèmes industriels et sociétés d'ingénierie
- ✓ Entreprises des secteurs de l'énergie, pétrole et gaz, chimie, pétrochimie, mines, ciment, eau, transport, agroalimentaire, pharmaceutique et manufacturing
- ✓ Toute personne chargée d'évaluer, auditer, surveiller ou renforcer la sécurité des infrastructures OT/ICS et des systèmes de contrôle industriel.



Programme détaillé

1 / FONDAMENTAUX DE LA CYBERSÉCURITÉ OT/ICS

- Différences entre cybersécurité IT et OT
- Enjeux de disponibilité, intégrité et sécurité des procédés
- Menaces et scénarios d'attaque visant les environnements industriels

2 / ARCHITECTURES DES SYSTÈMES DE CONTRÔLE INDUSTRIEL

- Automates PLC, RTU, SCADA et DCS
- Systèmes instrumentés de sécurité (SIS)
- Architectures Purdue, zones et conduits industriels

3 / CARTOGRAPHIE ET INVENTAIRE DES ACTIFS OT

- Identification des équipements et flux de communication
- Classification et criticité des actifs industriels
- Cartographie des dépendances entre systèmes

4 / PROTOCOLES ET COMMUNICATIONS INDUSTRIELLES

- Principes de fonctionnement des protocoles OT
- Ethernet industriel et protocoles de communication
- Identification des risques liés aux protocoles historiquement peu sécurisés

5 / ANALYSE DES VULNÉRABILITÉS OT

- Identification des failles de configuration
- Analyse des systèmes, services et équipements exposés
- Évaluation de la criticité et du risque industriel

6 / MÉTHODOLOGIE DU PENTEST OT

- Préparation, périmètre et règles d'engagement
- Tests non intrusifs et validation contrôlée des vulnérabilités
- Gestion des risques pour éviter toute perturbation du procédé

7 / AUDIT DES PLC, SCADA ET DCS

- Vérification des configurations et mécanismes d'accès
- Gestion des comptes, privilèges et authentification
- Analyse des postes opérateurs, serveurs et stations d'ingénierie

8 / TESTS DE SÉCURITÉ DES RÉSEAUX INDUSTRIELS

- Analyse de la segmentation réseau
- Vérification des pare-feu, zones DMZ et conduits OT
- Identification des chemins d'attaque potentiels entre IT et OT

9 / DÉTECTION ET SURVEILLANCE DES MENACES OT

- Journalisation et analyse des événements
- Détection des comportements anormaux
- Introduction aux solutions IDS/IPS et SIEM adaptées à l'OT

10 / REMÉDIATION ET DURCISSEMENT DES SYSTÈMES OT

- Réduction de la surface d'attaque
- Durcissement des équipements et systèmes

- Gestion des correctifs et des vulnérabilités avec prise en compte des contraintes industrielles

11 / GESTION DES RISQUES ET CONFORMITÉ

- Analyse de risques cyber-physiques
- Principes des référentiels IEC 62443 et ISO 27001
- Élaboration de politiques et procédures de cybersécurité OT

12 / ATELIER PRATIQUE : AUDIT ET PLAN DE REMÉDIATION OT

- Analyse d'une architecture industrielle simulée
- Identification et hiérarchisation des vulnérabilités
- Élaboration d'un rapport de pentest et d'un plan intégrant segmentation, durcissement, surveillance, gestion des accès et continuité des opérations

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

 16 au 25 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>

INNOV MAROC