



Segmentation réseau et architecture Zero Trust pour environnements industriels

Lien :

<https://innov-maroc.com/formation/segmentation-reseau-et-architecture-zero-trust-pour-environnements-industriels>

 DURÉE
5 jours (35h)

 RÉFÉRENCE
II58

 CATÉGORIE
**Cybersécurité OT &
Sécurité Réseau
Industrielle**

🎯 OBJECTIFS DE LA FORMATION

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

- ✓ Comprendre les principes fondamentaux de la cybersécurité des environnements industriels OT/IT.
- ✓ Identifier les différences entre les architectures informatiques IT et opérationnelles OT.
- ✓ Cartographier les actifs, équipements et flux de communication d'une infrastructure industrielle.
- ✓ Évaluer la criticité des équipements et identifier les principales surfaces d'attaque.
- ✓ Concevoir une stratégie de segmentation adaptée aux architectures industrielles.
- ✓ Maîtriser les concepts de VLAN, zones de sécurité, conduits et DMZ industrielle.
- ✓ Définir des règles de filtrage et de contrôle des flux entre les différents segments.
- ✓ Comprendre et appliquer les principes de l'architecture Zero Trust aux environnements OT.
- ✓ Mettre en œuvre les principes de moindre privilège, authentification forte et contrôle des accès.
- ✓ Concevoir une stratégie de micro-segmentation permettant de limiter les mouvements latéraux.
- ✓ Mettre en place une surveillance des communications et une détection des comportements anormaux.
- ✓ Développer une architecture de cybersécurité industrielle robuste permettant de réduire la surface d'attaque, protéger les systèmes critiques et améliorer la résilience des infrastructures OT.

POUR QUI ?

- ✓ Ingénieurs cybersécurité industrielle
- ✓ Ingénieurs réseaux et télécommunications
- ✓ Ingénieurs automatisme et contrôle-commande
- ✓ Ingénieurs informatique industrielle
- ✓ Ingénieurs systèmes et réseaux
- ✓ Architectes OT/IT
- ✓ Responsables cybersécurité
- ✓ Responsables IT et OT
- ✓ Responsables SOC et Security Operations
- ✓ Responsables infrastructure et réseaux industriels
- ✓ Responsables Industrie 4.0 et transformation numérique
- ✓ Administrateurs réseaux et systèmes
- ✓ Automaticiens et intégrateurs de systèmes industriels
- ✓ Techniciens réseaux et télécommunications industrielles
- ✓ Responsables SCADA, DCS et systèmes de contrôle
- ✓ Responsables maintenance et Asset Management
- ✓ Consultants et bureaux d'études en cybersécurité industrielle
- ✓ Entreprises industrielles des secteurs de l'énergie, pétrole & gaz, chimie, pétrochimie, mines, manufacturing, eau et infrastructures critiques
- ✓ Toute personne impliquée dans la conception, l'exploitation, la sécurisation ou la supervision des réseaux industriels OT/IT souhaitant maîtriser la segmentation réseau et les architectures Zero Trust.



Programme détaillé

1 / FONDAMENTAUX DE LA CYBERSÉCURITÉ INDUSTRIELLE OT/IT

- Différences entre réseaux IT et réseaux OT
- Spécificités des systèmes SCADA, DCS, PLC et IIoT
- Menaces et vulnérabilités propres aux environnements industriels

2 / CARTOGRAPHIE ET CLASSIFICATION DES ACTIFS INDUSTRIELS

- Inventaire des équipements et systèmes critiques
- Identification des flux réseau OT/IT
- Classification des actifs selon leur criticité et leur niveau de risque

3 / PRINCIPES DE SEGMENTATION DES RÉSEAUX INDUSTRIELS

- Segmentation physique et logique
- VLAN, sous-réseaux et zones de sécurité
- Réduction des communications inutiles entre segments

4 / ARCHITECTURE OT/IT ET DMZ INDUSTRIELLE

- Séparation des réseaux bureautiques et industriels
- Conception d'une Industrial DMZ
- Contrôle des échanges entre IT, DMZ et OT

5 / FIREWALLS ET CONTRÔLE DES FLUX INDUSTRIELS

- Pare-feu réseau et pare-feu industriel
- Règles de filtrage et listes de contrôle d'accès
- Whitelisting et contrôle des communications autorisées

6 / ARCHITECTURE ZERO TRUST EN ENVIRONNEMENT INDUSTRIEL

- Principes « Never Trust, Always Verify »
- Vérification continue des utilisateurs, équipements et connexions
- Application du moindre privilège dans les systèmes OT

7 / GESTION DES IDENTITÉS ET DES ACCÈS

- Authentification forte et contrôle des privilèges
- Gestion des comptes utilisateurs et comptes techniques
- RBAC, MFA et contrôle des accès distants

8 / MICRO-SEGMENTATION ET PROTECTION DES SYSTÈMES CRITIQUES

- Segmentation des cellules, lignes de production et équipements
- Isolation des automates et systèmes critiques
- Limitation des mouvements latéraux

9 / SURVEILLANCE, DÉTECTION ET RÉPONSE AUX INCIDENTS

- Monitoring des flux réseau industriels
- Détection des comportements anormaux
- Journalisation, alertes et intégration avec SIEM/SOC

10 / ATELIER PRATIQUE : CONCEPTION D'UNE ARCHITECTURE ZERO TRUST INDUSTRIELLE

- Cartographie d'une infrastructure OT/IT
- Élaboration des zones, conduits, DMZ et règles de communication

- Conception d'une architecture intégrant segmentation, Zero Trust, contrôle d'accès, supervision et réponse aux incidents

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

 19 au 23 Oct. 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>

Document généré le 11/10/2026 — Réf : II58

INNOV MAROC — Tous droits réservés