Sécurité des réseaux OT & convergence ITOT : segmentation, purdue model et DMZ industrielle

Lien : https://innov-systems.com/formation/securite-des-reseaux-ot-convergence-itot-segmentation-purdue-model-et-dmz-industrielle

DURÉE
5 jours (35h)

RÉFÉRENCE
SI118

CATÉGORIE
Sécurité Technique : Cryptographie, Protocoles et Infrastructures

Innov Systems

OBJECTIFS DE LA FORMATION

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

- Comprendre les fondamentaux des réseaux OT et industriels
- Maîtriser les principes de la convergence IT/OT
- Appliquer le modèle Purdue pour segmenter les réseaux industriels
- Concevoir une DMZ industrielle sécurisée
- Sécuriser les protocoles industriels critiques
- Mettre en place des architectures Zero Trust en OT
- Détecter les menaces dans les environnements industriels
- Réduire les risques cyber-physiques
- Appliquer les normes IEC 62443 et standards industriels
- Améliorer la résilience des systèmes OT
- Concevoir des architectures industrielles sécurisées
- Étudier des cas concrets de sécurisation IT/OT

POUR QUI ?

- Ingénieurs cybersécurité industrielle
- Architectes réseaux OT/IT
- Ingénieurs automatisme et SCADA
- Ingénieurs industriels
- SRE industriels
- Responsables cybersécurité (CISO / RSSI)
- Administrateurs réseaux industriels
- Consultants cybersécurité OT
- Ingénieurs systèmes industriels
- Chefs de projet Industrie 4.0
- Responsables infrastructures critiques
- Toute personne impliquée dans la sécurité des environnements industriels OT/IT

Innov Systems

Programme détaillé

1 / Introduction aux réseaux OT et à la convergence IT/OT

- Différences entre environnements IT et OT
- Évolution vers l'industrie connectée et l'Industrie 4.0
- Enjeux de cybersécurité dans les systèmes industriels

2 / Architecture des systèmes OT

- SCADA, PLC, DCS et systèmes industriels
- Flux de données entre capteurs, automates et supervision
- Contraintes de disponibilité et temps réel

3 / Modèle Purdue pour la segmentation OT

- Présentation des niveaux du Purdue Model
- Segmentation logique et physique des réseaux
- Bonnes pratiques d'implémentation

4 / Zones et conduits dans les architectures OT

- Concept de zones de sécurité industrielles
- Contrôle des flux entre zones
- Gestion des accès inter-segments

5 / DMZ industrielle et sécurisation des échanges

- Rôle de la DMZ entre IT et OT
- Proxy industriels et passerelles sécurisées
- Filtrage et inspection des communications

Innov Systems

6 / Sécurité des protocoles industriels

- Modbus, OPC-UA, DNP3 et autres protocoles OT
- Vulnérabilités et protections associées
- Chiffrement et authentification industrielle

7 / Segmentation réseau et contrôle d’accès

- VLAN, micro-segmentation et firewalls industriels
- Zero Trust appliqué aux environnements OT
- Gestion des accès utilisateurs et machines

8 / Détection des menaces en environnement OT

- IDS/IPS industriels
- Détection d’anomalies comportementales
- Monitoring des flux industriels critiques

9 / Gouvernance et conformité OT

- Normes IEC 62443 et NIST ICS
- Politiques de cybersécurité industrielle
- Gestion des risques cyber physiques

10 / Cas pratiques et architectures sécurisées OT

- Mise en place d’une architecture IT/OT segmentée
- Construction d’une DMZ industrielle sécurisée
- Retours d’expérience et bonnes pratiques

Innov Systems

Approche pédagogique

- Support Ecrit et Projection
- Exposés Interactifs, Podcasts et Vidéos
- Brainstorming et Jeux de Rôle
- Cas Pratiques et Labs inclus pour leur impact opérationnel
- Test de Validation des Acquis des Connaissances

Prochaines dates programmées

07 au 11 Déc. 2026	Distanciel
25 au 29 Jan. 2027	Présentiel - Casablanca
22 au 26 Mars 2027	Présentiel - Casablanca
17 au 21 Mai 2027	Présentiel - Casablanca
12 au 16 Juil. 2027	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-systems.com
Web : https//www.innov-systems.com

Innov Systems — Tous droits réservés