



Sécurisation des Technologies Opérationnelles (OT) en Environnement Portuaire

Lien :

<https://afrique-formation.com/formation/securisation-des-technologies-operationnelles-ot-en-environnement-portuaire>

 DURÉE
8 jours (56h)

 RÉFÉRENCE
POR192

 CATÉGORIE
**Numérique, Data et
Systèmes
d'Information Portuaire**

🎯 OBJECTIFS DE LA FORMATION

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

- ✓ Comprendre les spécificités des technologies opérationnelles (OT) dans les environnements portuaires.
- ✓ Identifier les principales cybermenaces ciblant les infrastructures portuaires critiques.
- ✓ Concevoir une architecture OT sécurisée intégrant les meilleures pratiques internationales.
- ✓ Sécuriser les systèmes SCADA, PLC, TOS, PCS et les équipements industriels connectés.
- ✓ Mettre en œuvre des solutions de supervision, de détection et de réponse aux incidents cyber.
- ✓ Maîtriser les référentiels IEC 62443, NIST, ISO/IEC 27001, ISO 28000 et les exigences IMO/ISPS.
- ✓ Développer des plans de continuité d'activité et de reprise après incident.
- ✓ Intégrer les nouvelles technologies (IoT, IA, Cloud, Digital Twins) dans une approche de cybersécurité OT.
- ✓ Renforcer la gouvernance, la conformité et la gestion des risques cyber des infrastructures portuaires.
- ✓ Développer une stratégie de cybersécurité OT adaptée aux Smart Ports et aux ports africains.
- ✓ Améliorer la résilience des opérations portuaires face aux cyberattaques.
- ✓ Être capable de piloter un programme global de sécurisation des technologies opérationnelles en environnement portuaire.

POUR QUI ?

- ✓ Responsables cybersécurité (CISO)
- ✓ Responsables OT et automatisme industriel
- ✓ Ingénieurs réseaux industriels
- ✓ Ingénieurs SCADA, ICS et PLC
- ✓ Responsables des systèmes d'information portuaires
- ✓ Directeurs techniques des autorités portuaires
- ✓ Responsables des opérations portuaires
- ✓ Responsables maintenance et exploitation
- ✓ Responsables HSE et gestion des risques
- ✓ Intégrateurs de systèmes industriels
- ✓ Cadres des administrations portuaires, maritimes et des infrastructures critiques
- ✓ Toute personne impliquée dans la conception, l'exploitation, la maintenance, la cybersécurité ou la gouvernance des technologies opérationnelles des ports et terminaux maritimes.



Programme détaillé

1 / FONDAMENTAUX DES TECHNOLOGIES OPÉRATIONNELLES (OT) EN ENVIRONNEMENT PORTUAIRE

- Différences entre IT (Information Technology) et OT (Operational Technology)
- Architecture des systèmes OT dans les ports modernes
- Enjeux de cybersécurité des infrastructures portuaires critiques

2 / ARCHITECTURE DES SYSTÈMES INDUSTRIELS PORTUAIRES

- SCADA, PLC, DCS, RTU et réseaux industriels
- Terminal Operating Systems (TOS) et Port Community Systems (PCS)
- Intégration des équipements automatisés et des systèmes IoT

3 / MENACES CYBER ET ANALYSE DES RISQUES OT

- Typologie des cyberattaques ciblant les infrastructures portuaires
- Vulnérabilités des systèmes industriels
- Analyse de risques et cartographie des actifs critiques

4 / CONCEPTION D'UNE ARCHITECTURE OT SÉCURISÉE

- Segmentation des réseaux IT/OT
- Zones de sécurité, DMZ industrielles et contrôle des accès
- Défense en profondeur (Defense in Depth)

5 / SÉCURISATION DES SYSTÈMES INDUSTRIELS ET DES ÉQUIPEMENTS

- Protection des automates industriels, serveurs SCADA et équipements réseau
- Gestion des correctifs (Patch Management) et durcissement (Hardening)
- Sécurisation des accès distants et des fournisseurs

6 / SUPERVISION, DÉTECTION ET RÉPONSE AUX INCIDENTS

- Surveillance des réseaux OT et détection des anomalies
- SOC OT, SIEM et plateformes de supervision industrielle
- Gestion des incidents cyber et procédures de réponse

7 / NORMES, RÉFÉRENTIELS ET CONFORMITÉ

- IEC 62443, NIST CSF, ISO/IEC 27001 et ISO 28000
- Exigences de l'OMI (IMO) et du Code ISPS
- Audits de cybersécurité et conformité réglementaire

8 / CONTINUITÉ D'ACTIVITÉ ET RÉSILIENCE DES OPÉRATIONS PORTUAIRES

- Plans de continuité (PCA) et plans de reprise (PRA)
- Gestion de crise cyber dans les ports
- Exercices, simulations et amélioration continue

9 / DIGITALISATION, SMART PORTS ET TECHNOLOGIES ÉMERGENTES

- IoT industriel, 5G, Cloud et Edge Computing
- Intelligence artificielle appliquée à la cybersécurité OT
- Jumeaux numériques (Digital Twins) des infrastructures portuaires

10 / GOUVERNANCE ET MANAGEMENT DE LA CYBERSÉCURITÉ OT

- Organisation de la gouvernance cyber
- Gestion des fournisseurs et des risques tiers

- Sensibilisation, formation et culture cybersécurité

11 / ÉTUDES DE CAS DE CYBERATTAQUES PORTUAIRES

- Analyse de cyberincidents majeurs dans les ports internationaux
- Retours d'expérience et leçons apprises
- Bonnes pratiques pour renforcer la résilience

12 / ATELIER PRATIQUE : ÉLABORATION D'UNE STRATÉGIE DE SÉCURISATION OT

- Réalisation d'un diagnostic de maturité cybersécurité OT
- Élaboration d'une feuille de route de sécurisation
- Construction d'un plan d'action intégrant gouvernance, technologies, conformité et résilience

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

 23 Nov. au 02 Déc. 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@afrique-formation.com

 Web : <https://www.afrique-formation.com>

Afrique Formation