

Cybersécurité des Systèmes Portuaires : Protéger les Infrastructures Critiques Maritimes

Lien : https://afrique-formation.com/formation/cybersecurite-des-systemes-portuaires-proteger-les-infrastructures-critiques-maritimes

DURÉE
8 jours (56h)

RÉFÉRENCE
POR190

CATÉGORIE
Numérique, Data et Systèmes d'Information Portuaire

Afrique Formation

OBJECTIFS DE LA FORMATION

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

- Comprendre les cybermenaces spécifiques aux infrastructures portuaires et maritimes.
- Identifier les vulnérabilités des systèmes IT, OT, ICS et SCADA utilisés dans les ports.
- Réaliser une analyse des risques et mettre en œuvre des mesures de protection adaptées.
- Sécuriser les réseaux, les systèmes industriels et les équipements connectés.
- Mettre en place des dispositifs de surveillance, de détection et de réponse aux incidents cyber.
- Développer des stratégies de résilience, de continuité et de reprise des activités.
- Appliquer les normes internationales de cybersécurité maritime et industrielle.
- Renforcer la gouvernance de la cybersécurité et la protection des données sensibles.
- Sensibiliser les équipes aux bonnes pratiques et développer une culture de cybersécurité.
- Élaborer une stratégie globale de sécurisation des infrastructures critiques portuaires.
- Intégrer la cybersécurité dans les projets de transformation numérique des Smart Ports.
- Développer une expertise opérationnelle pour protéger durablement les infrastructures critiques maritimes contre les cyberattaques.

POUR QUI ?

- Responsables cybersécurité (CISO)
- Responsables des systèmes d'information portuaires
- Administrateurs réseaux et systèmes
- Responsables OT, ICS et SCADA
- Ingénieurs cybersécurité
- Responsables des opérations portuaires
- Responsables de la transformation digitale
- Responsables gestion des risques et continuité d'activité
- Responsables HSE et sûreté portuaire
- Data Analysts et architectes systèmes
- Cadres des autorités portuaires, opérateurs de terminaux, compagnies maritimes, ministères des Transports et de la Sécurité, ainsi que toute personne impliquée dans la protection des systèmes d'information et des infrastructures critiques portuaires.

Afrique Formation

AFRIQUE FORMATION
La Référence en Afrique pour la Formation



Programme détaillé

1 / FONDAMENTAUX DE LA CYBERSÉCURITÉ PORTUAIRE

- Panorama des cybermenaces dans le secteur maritime
- Enjeux de la cybersécurité des ports intelligents
- Impacts opérationnels, économiques et stratégiques des cyberattaques

2 / ARCHITECTURE DES SYSTÈMES D'INFORMATION PORTUAIRES

- Terminal Operating System (TOS)
- Port Community System (PCS), ERP et systèmes métiers
- Réseaux IT, OT et infrastructures numériques portuaires

3 / CYBERSÉCURITÉ DES SYSTÈMES INDUSTRIELS (OT/ICS/SCADA)

- Fonctionnement des systèmes de contrôle industriel portuaires
- Sécurisation des automates, capteurs et équipements connectés
- Normes IEC 62443 et bonnes pratiques industrielles

4 / GESTION DES RISQUES CYBER ET ANALYSE DES VULNÉRABILITÉS

- Identification des actifs critiques
- Analyse des risques et cartographie des menaces
- Audits de sécurité et tests de vulnérabilité

Afrique Formation

5 / PROTECTION DES RÉSEAUX ET DES INFRASTRUCTURES CRITIQUES

- Segmentation réseau et architecture Zero Trust
- Pare-feu industriels, IDS/IPS et contrôle des accès
- Sécurisation des communications maritimes et des infrastructures cloud

6 / GESTION DES IDENTITÉS, ACCÈS ET DONNÉES SENSIBLES

- Gestion des identités (IAM)
- Authentification multifacteur (MFA) et gestion des privilèges
- Protection des données portuaires et conformité réglementaire

7 / SURVEILLANCE, DÉTECTION ET RÉPONSE AUX INCIDENTS

- Centre opérationnel de sécurité (SOC)
- SIEM, EDR, XDR et intelligence sur les menaces
- Gestion des incidents et procédures de réponse

8 / CYBERSÉCURITÉ DES ÉQUIPEMENTS CONNECTÉS ET DE L'IoT PORTUAIRE

- Sécurisation des capteurs, grues intelligentes et AGV
- Gestion des risques liés aux objets connectés
- Surveillance continue des équipements critiques

9 / RÉSILIENCE, CONTINUITÉ D'ACTIVITÉ ET REPRISE APRÈS INCIDENT

- Élaboration d'un Plan de Continuité d'Activité (PCA)
- Plan de Reprise d'Activité (PRA)
- Exercices de simulation de cybercrise

10 / CADRE RÉGLEMENTAIRE ET STANDARDS INTERNATIONAUX

- Directives de l'Organisation Maritime Internationale (OMI/IMO)
- ISO/IEC 27001, NIST Cybersecurity Framework et IEC 62443

Afrique Formation

- Exigences réglementaires nationales et internationales

11 / GOUVERNANCE CYBER ET CULTURE DE LA SÉCURITÉ

- Politique de cybersécurité portuaire
- Sensibilisation et formation des collaborateurs
- Pilotage de la cybersécurité par les indicateurs de performance (KPIs)

12 / ÉTUDES DE CAS ET ÉLABORATION D'UNE STRATÉGIE CYBER POUR UN PORT

- Analyse d'incidents cyber ayant affecté des infrastructures portuaires
- Évaluation de la maturité cyber d'un port
- Construction d'une feuille de route de cybersécurité et de résilience numérique

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

30 Nov. au 09 Déc. 2026	Présentiel - Casablanca
08 au 17 Fév. 2027	Présentiel - Casablanca
05 au 14 Avr. 2027	Présentiel - Casablanca
31 Mai au 09 Juin 2027	Présentiel - Casablanca
26 Juil. au 04 Août 2027	Présentiel - Casablanca

Autres dates possibles sur demande. Contactez-nous pour organiser une session intra-entreprise.

Afrique Formation

Réservation & Renseignements

Téléphone : +212 522 247 210
Email : contact@afrique-formation.com
Web : https//www.afrique-formation.com

Afrique Formation — Tous droits réservés

Afrique Formation