

Audit de Cybersécurité Portuaire : Évaluer les Vulnérabilités des Systèmes Critiques

Lien : https://afrique-formation.com/formation/audit-de-cybersecurite-portuaire-evaluer-les-vulnerabilites-des-systemes-critiques

DURÉE
5 jours (35h)

RÉFÉRENCE
POR189

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 enjeux de la cybersécurité dans les infrastructures portuaires critiques.
- Identifier les principales menaces et vulnérabilités des systèmes IT, OT et industriels.
- Maîtriser la méthodologie d'audit de cybersécurité adaptée aux environnements portuaires.
- Évaluer les risques cyber et leur impact sur les opérations portuaires.
- Réaliser des analyses de vulnérabilités et interpréter leurs résultats.
- Élaborer des plans de remédiation et de renforcement de la sécurité.
- Mettre en œuvre les bonnes pratiques de gestion des incidents et de résilience opérationnelle.
- Produire des rapports d'audit conformes aux standards internationaux.
- Renforcer la conformité avec les référentiels IMO, NIST, ISO 27001 et IEC 62443.
- Développer une expertise en audit et gouvernance de la cybersécurité des systèmes portuaires critiques.

POUR QUI ?

- Responsables cybersécurité (CISO)
- Responsables de la sécurité des systèmes d'information (RSSI)
- Auditeurs en cybersécurité
- Responsables informatiques des autorités portuaires
- Administrateurs réseaux et systèmes
- Ingénieurs OT, SCADA et ICS
- Responsables des Terminal Operating Systems (TOS)
- Responsables sûreté portuaire et conformité ISPS
- Responsables gestion des risques et continuité d'activité
- Cadres des autorités portuaires, terminaux à conteneurs et opérateurs logistiques
- Toute personne impliquée dans l'audit, la sécurisation, la gestion ou la résilience des systèmes numériques et industriels des ports et terminaux maritimes.

Afrique Formation

AFRIQUE FORMATION
La Référence en Afrique pour la Formation



Programme détaillé

1 / FONDAMENTAUX DE LA CYBERSÉCURITÉ PORTUAIRE

- Panorama des cybermenaces ciblant les ports et terminaux
- Architecture des systèmes IT, OT, SCADA et ICS portuaires
- Enjeux économiques, opérationnels et sécuritaires des infrastructures critiques

2 / GOUVERNANCE, RÉGLEMENTATION ET RÉFÉRENTIELS

- Exigences de l'IMO, du Code ISPS et des autorités portuaires
- Référentiels NIST Cybersecurity Framework, ISO/IEC 27001 et IEC 62443
- Gouvernance cyber et gestion des risques

3 / MÉTHODOLOGIE D'AUDIT DE CYBERSÉCURITÉ

- Préparation, cadrage et planification d'un audit
- Cartographie des actifs critiques et analyse des processus
- Collecte des preuves et techniques d'audit

4 / IDENTIFICATION DES VULNÉRABILITÉS DES SYSTÈMES CRITIQUES

- Analyse des vulnérabilités des réseaux IT et OT
- Audit des systèmes TOS, PCS, SCADA, IoT et équipements connectés
- Évaluation des accès, configurations et faiblesses techniques

Afrique Formation

5 / ANALYSE DES RISQUES ET ÉVALUATION DES MENACES

- Identification des scénarios d'attaque
- Analyse des impacts opérationnels, financiers et HSE
- Méthodes de cotation et priorisation des risques cyber

6 / TESTS DE SÉCURITÉ ET ÉVALUATION TECHNIQUE

- Scans de vulnérabilités et revues de configuration
- Tests d'intrusion (Pentest) et exercices Red Team/Blue Team
- Limites et bonnes pratiques des tests sur systèmes industriels

7 / PLANS DE REMÉDIATION ET RENFORCEMENT DE LA SÉCURITÉ

- Élaboration d'un plan d'actions correctives
- Segmentation réseau, contrôle des accès et durcissement des systèmes
- Gestion des correctifs et amélioration continue

8 / GESTION DES INCIDENTS ET RÉSILIENCE OPÉRATIONNELLE

- Détection, réponse et investigation des incidents
- Plans de continuité d'activité (PCA) et de reprise après sinistre (PRA)
- Exercices de simulation et gestion de crise cyber

9 / TABLEAUX DE BORD, CONFORMITÉ ET REPORTING

- Indicateurs de performance (KPIs) et de maturité cyber
- Rédaction des rapports d'audit et suivi des recommandations
- Préparation aux audits réglementaires et certifications

10 / ÉTUDES DE CAS ET MISSION D'AUDIT COMPLÈTE

- Analyse de cyberattaques ayant affecté des infrastructures portuaires
- Réalisation d'un audit complet d'un terminal portuaire

Afrique Formation

- Élaboration d'une feuille de route de cybersécurité pour une infrastructure critique

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

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
06 au 10 Sep. 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@afrique-formation.com
Web : https//www.afrique-formation.com

Afrique Formation

Afrique Formation — Tous droits réservés