

Gestion des Incidents Cybersécurité Portuaires : Détecter, Répondre et Se Rétablir

Lien : https://afrique-formation.com/formation/gestion-des-incidents-cybersecurite-portuaires-detecter-repondre-et-se-retablir

DURÉE
5 jours (35h)

RÉFÉRENCE
POR191

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 menaces cyber spécifiques aux infrastructures portuaires.
- Identifier les actifs critiques et évaluer les risques de cybersécurité.
- Déployer des dispositifs efficaces de détection et de surveillance des incidents.
- Mettre en œuvre une réponse structurée aux cyberattaques selon les bonnes pratiques internationales.
- Sécuriser les systèmes IT, OT, SCADA et les plateformes numériques portuaires.
- Élaborer un Plan de Réponse aux Incidents (IRP), un PRA et un PCA adaptés au contexte portuaire.
- Assurer la conformité avec les référentiels internationaux et les exigences de l'Organisation Maritime Internationale (OMI).
- Organiser des exercices de gestion de crise et améliorer la résilience des équipes.
- Exploiter les nouvelles technologies pour renforcer la cyber-résilience des ports.
- Développer une expertise opérationnelle permettant de prévenir, détecter, gérer et surmonter les incidents de cybersécurité dans les infrastructures portuaires.

POUR QUI ?

- Responsables cybersécurité (CISO)
- Responsables sécurité des systèmes d'information (RSSI)
- Responsables informatiques des autorités portuaires
- Responsables des systèmes OT/ICS et SCADA
- Responsables des opérations portuaires
- Ingénieurs réseaux et cybersécurité
- Administrateurs systèmes et réseaux
- Responsables transformation digitale et Smart Ports
- Responsables gestion des risques et continuité d'activité
- Autorités portuaires, exploitants de terminaux, opérateurs logistiques et organismes de régulation
- Toute personne impliquée dans la protection, la supervision, la gestion ou la résilience des systèmes numériques et industriels des infrastructures portuaires.

Afrique Formation

AFRIQUE FORMATION
La Référence en Afrique pour la Formation



Programme détaillé

1 / FONDAMENTAUX DE LA CYBERSÉCURITÉ PORTUAIRE

- Enjeux de la cybersécurité dans les ports et terminaux
- Panorama des menaces visant les infrastructures portuaires
- Impacts opérationnels, économiques et réglementaires

2 / IDENTIFICATION DES ACTIFS CRITIQUES ET ANALYSE DES RISQUES

- Cartographie des systèmes IT, OT et SCADA
- Identification des actifs critiques (TOS, PCS, AIS, VTS, ERP, IoT)
- Évaluation des risques et des vulnérabilités

3 / DÉTECTION DES INCIDENTS ET SURVEILLANCE DE SÉCURITÉ

- Centre opérationnel de sécurité (SOC)
- SIEM, EDR, XDR et outils de supervision
- Détection des comportements anormaux et alertes

4 / GESTION ET RÉPONSE AUX INCIDENTS CYBER

- Cycle de gestion des incidents (NIST)
- Qualification, priorisation et coordination des réponses
- Confinement, éradication et remédiation

Afrique Formation

5 / GESTION DES CYBERATTAQUES SUR LES SYSTÈMES PORTUAIRES

- Attaques par ransomware, phishing et APT
- Protection des systèmes industriels OT/ICS et SCADA
- Gestion des incidents affectant les équipements portuaires

6 / PLAN DE REPRISE ET CONTINUITÉ D'ACTIVITÉ

- Élaboration d'un Plan de Réponse aux Incidents (IRP)
- Plan de Reprise d'Activité (PRA) et Plan de Continuité d'Activité (PCA)
- Sauvegarde, restauration et reprise des opérations

7 / CONFORMITÉ RÉGLEMENTAIRE ET GOUVERNANCE

- Référentiels ISO 27001, IEC 62443, NIST CSF
- Exigences de l'OMI (IMO) en matière de cybersécurité maritime
- Gouvernance, reporting et gestion documentaire

8 / EXERCICES DE CRISE ET RETOUR D'EXPÉRIENCE

- Organisation d'exercices de simulation cyber
- Gestion de crise et communication
- Retour d'expérience (Lessons Learned) et amélioration continue

9 / TECHNOLOGIES ÉMERGENTES ET RÉSILIENCE NUMÉRIQUE

- Intelligence artificielle et détection des menaces
- Zero Trust, segmentation réseau et cyber-résilience
- Cyber Threat Intelligence et automatisation de la réponse

10 / CAS PRATIQUES ET CONSTRUCTION D'UN PLAN DE RÉPONSE AUX INCIDENTS

- Analyse d'incidents cyber ayant touché des ports internationaux
- Élaboration d'une stratégie de réponse adaptée à un port

Afrique Formation

- Construction d'une feuille de route de résilience cyber et d'amélioration continue

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

04 au 08 Jan. 2027	Présentiel - Casablanca
01 au 05 Mars 2027	Présentiel - Casablanca
26 au 30 Avr. 2027	Présentiel - Casablanca
21 au 25 Juin 2027	Présentiel - Casablanca
16 au 20 Août 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