AFRIQUE FORMATION
La Référence en Afrique pour la Formation



Cyber Sécurité en Milieu Maritime et Portuaire

Lien : https://afrique-formation.com/formation/cyber-securite-en-milieu-maritime-et-portuaire

DURÉE
10 jours (70h)

RÉFÉRENCE
POR111

CATÉGORIE
Qualité, Sûreté, Sécurité et Réglementation Maritime (STCW, ISPS, POLMAR)

Afrique Formation

OBJECTIFS DE LA FORMATION

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

- Comprendre les enjeux spécifiques de la cybersécurité dans le secteur maritime et portuaire
- Identifier et évaluer les risques cyber sur les infrastructures maritimes
- Appliquer les réglementations internationales et nationales
- Protéger les systèmes critiques OT et IT contre les attaques
- Mettre en place une stratégie de réponse efficace aux cyber-incidents
- Renforcer la culture cybersécurité au sein des équipes
- Réaliser un audit et un plan d’amélioration continue
- Garantir la continuité des opérations en cas d’incident
- Utiliser les innovations technologiques pour améliorer la sécurité
- Développer la coopération avec les autorités et partenaires

POUR QUI ?

- Responsables sûreté et sécurité maritime
- Directeurs et responsables informatiques
- Ingénieurs systèmes et réseaux
- Officiers de la marine marchande
- Gestionnaires de terminaux portuaires
- Responsables de maintenance OT/IT
- Auditeurs internes et externes en cybersécurité
- Autorités portuaires et maritimes
- Membres d’équipes de réponse aux incidents
- Forces navales et garde-côtes
- Cadres du secteur logistique maritime
- Entreprises opérant des systèmes de navigation et de communication

Afrique Formation

AFRIQUE FORMATION
La Référence en Afrique pour la Formation



Programme détaillé

1 / Introduction à la cybersécurité maritime et portuaire

- Présentation des menaces spécifiques au secteur maritime et portuaire
- Panorama des incidents récents dans le domaine
- Règlementations internationales et nationales applicables

2 / Cadre réglementaire et conformité

- Code ISPS et exigences liées à la cybersécurité
- Directives de l'OMI sur la cybersécurité maritime
- Normes ISO et bonnes pratiques pour la sûreté des systèmes d'information

3 / Identification des menaces et vulnérabilités

- Cartographie des actifs numériques critiques
- Analyse des vecteurs de cyberattaque spécifiques au maritime
- Évaluation des risques et priorisation

4 / Sécurité des systèmes OT (Operational Technology) et IT

- Différences et interactions entre OT et IT
- Protocoles spécifiques aux systèmes industriels maritimes
- Mesures de protection adaptées aux environnements portuaires

Afrique Formation

5 / Protection des réseaux et infrastructures critiques

- Segmentation réseau et filtrage
- Gestion des accès et authentification forte
- Surveillance et détection d’intrusion

6 / Gestion des cyber-incidents

- Procédure de réponse aux incidents
- Coordination avec les autorités et parties prenantes
- Documentation et retour d’expérience

7 / Sécurité des systèmes de navigation et de communication

- Protection des systèmes AIS, GPS et ECDIS
- Sécurité des communications maritimes (VHF, satellite, etc.)
- Contre-mesures face au spoofing et au jamming

8 / Sécurité des systèmes portuaires

- Protection des systèmes de gestion de terminal
- Sécurité des systèmes de contrôle d’accès physique
- Prévention des intrusions via équipements connectés

9 / Cyber-espionnage et cybercriminalité maritime

- Techniques utilisées par les cybercriminels
- Impact économique et opérationnel des cyberattaques
- Études de cas réels

10 / Sensibilisation et formation du personnel

- Bonnes pratiques pour réduire le risque humain
- Simulation d’attaques pour évaluer la réactivité

Afrique Formation

- Communication interne et culture cybersécurité

11 / Audit et évaluation de la cybersécurité

- Méthodologie d’audit de sécurité informatique
- Tests d’intrusion et analyses de vulnérabilités
- Suivi des plans de remédiation

12 / Continuité d’activité et reprise après sinistre

- Élaboration d’un plan de continuité d’activité
- Sauvegarde et restauration des données
- Redondance et résilience des systèmes

13 / Exercice pratique de gestion de cybercrise

- Simulation d’une cyberattaque maritime
- Répartition des rôles et coordination
- Débriefing et amélioration des procédures

14 / Perspectives et innovations en cybersécurité maritime

- Nouvelles technologies et solutions émergentes
- Intelligence artificielle et cybersécurité
- Partenariats internationaux pour renforcer la sécurité

Afrique Formation

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

08 au 19 Fév. 2027	Présentiel - Casablanca
05 au 16 Avr. 2027	Présentiel - Casablanca
31 Mai au 11 Juin 2027	Présentiel - Casablanca
26 Juil. au 06 Août 2027	Présentiel - Casablanca
20 Sep. au 01 Oct. 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 — Tous droits réservés