



Stratégie Zero Trust pour Ports Intelligents : Architecture de Confiance Zéro en Milieu Maritime

Lien :

<https://afrique-formation.com/formation/strategie-zero-trust-pour-ports-intelligents-architecture-de-confiance-zero-en-milieu-maritime>

 DURÉE
8 jours (56h)

 RÉFÉRENCE
POR193

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

🎯 OBJECTIFS DE LA FORMATION

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

- ✓ Comprendre les principes fondamentaux de la stratégie Zero Trust appliquée aux ports intelligents.
- ✓ Identifier les vulnérabilités des infrastructures numériques, industrielles et maritimes.
- ✓ Concevoir une architecture Zero Trust intégrant les environnements IT, OT, IoT et Cloud.
- ✓ Mettre en œuvre des mécanismes avancés de gestion des identités, des accès et des privilèges.
- ✓ Sécuriser les systèmes industriels portuaires (SCADA, ICS, PLC) et les réseaux opérationnels.
- ✓ Développer une gouvernance robuste des données et des infrastructures numériques.
- ✓ Détecter les cybermenaces et organiser une réponse efficace aux incidents.
- ✓ Assurer la conformité avec les normes internationales de cybersécurité maritime.
- ✓ Renforcer la résilience opérationnelle des ports face aux cyberattaques.
- ✓ Définir des indicateurs de performance et une feuille de route de transformation Zero Trust.
- ✓ Piloter un programme de cybersécurité adapté aux enjeux des Smart Ports.
- ✓ Développer une expertise opérationnelle permettant de protéger durablement les infrastructures portuaires critiques contre les cybermenaces.

👥 POUR QUI ?

- ✓ Directeurs des systèmes d'information (DSI)
- ✓ Responsables cybersécurité (CISO)
- ✓ Responsables IT et OT
- ✓ Responsables des infrastructures portuaires
- ✓ Responsables des Smart Ports et de la transformation numérique
- ✓ Ingénieurs réseaux, systèmes et cybersécurité
- ✓ Ingénieurs OT, SCADA et systèmes industriels
- ✓ Responsables Port Community System (PCS) et Terminal Operating System (TOS)
- ✓ Responsables de la gestion des risques et de la continuité d'activité
- ✓ Autorités portuaires, administrations maritimes, douanes et organismes de régulation
- ✓ Toute personne impliquée dans la conception, le déploiement, l'exploitation, la sécurisation ou la gouvernance des infrastructures numériques et industrielles des ports intelligents.



Programme détaillé

1 / FONDAMENTAUX DE LA STRATÉGIE ZERO TRUST DANS LES SMART PORTS

- Principes de la Zero Trust Architecture (ZTA)
- Enjeux de cybersécurité des ports intelligents
- Évolution des menaces visant les infrastructures maritimes critiques

2 / ÉCOSYSTÈME NUMÉRIQUE DES PORTS INTELLIGENTS

- Architecture IT, OT et IoT portuaire
- Port Community System (PCS), Terminal Operating System (TOS) et systèmes industriels
- Cartographie des actifs numériques et des flux de données

3 / CONCEPTION D'UNE ARCHITECTURE ZERO TRUST

- Vérification systématique (« Never Trust, Always Verify »)
- Segmentation réseau et micro-segmentation
- Contrôle d'accès basé sur l'identité et le contexte

4 / GESTION DES IDENTITÉS ET DES ACCÈS (IAM)

- Authentification forte (MFA)
- Gestion des privilèges (PAM)
- Gouvernance des identités des utilisateurs, équipements et applications

5 / PROTECTION DES RÉSEAUX IT/OT ET DES SYSTÈMES INDUSTRIELS

- Sécurisation des réseaux industriels portuaires
- Protection des systèmes SCADA, PLC et ICS
- Sécurisation des équipements IoT et Edge Computing

6 / GOUVERNANCE DES DONNÉES ET CYBERSÉCURITÉ CLOUD

- Classification et protection des données sensibles
- Chiffrement, gestion des clés et confidentialité
- Sécurité des environnements Cloud et hybrides

7 / DÉTECTION DES MENACES ET RÉPONSE AUX INCIDENTS

- SOC, SIEM, SOAR et Cyber Threat Intelligence
- Détection comportementale et intelligence artificielle
- Gestion des incidents et plans de réponse cyber

8 / CONFORMITÉ, NORMES ET RÉGLEMENTATIONS

- Référentiels NIST SP 800-207, IEC 62443, ISO/IEC 27001
- Exigences IMO, IACS et directives internationales
- Audit de conformité et gouvernance cyber

9 / RÉSILIENCE OPÉRATIONNELLE ET CONTINUITÉ D'ACTIVITÉ

- Plans de continuité (PCA) et de reprise (PRA)
- Cyber-résilience des infrastructures portuaires
- Gestion de crise et coordination multi-acteurs

10 / PILOTAGE DE LA PERFORMANCE CYBER

- Indicateurs de maturité Zero Trust
- Tableaux de bord cyber et KPIs

- Évaluation des risques et amélioration continue

11 / MISE EN ŒUVRE D'UNE FEUILLE DE ROUTE ZERO TRUST

- Diagnostic de maturité cybersécurité
- Planification de la transformation Zero Trust
- Gouvernance du changement et accompagnement des équipes

12 / ÉTUDES DE CAS ET CONCEPTION D'UNE ARCHITECTURE ZERO TRUST POUR UN SMART PORT

- Analyse de cyberattaques ayant affecté des infrastructures portuaires
- Élaboration d'une architecture Zero Trust adaptée à un port intelligent
- Construction d'un plan stratégique intégrant sécurité, gouvernance et résilience opérationnelle

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

 26 Oct. au 04 Nov. 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