

Cyberrésilience des infrastructures critiques africaines

Lien :
https://afrique-formation.com/formation/cyberresilience-des-infrastructures-critiques-africaines

DURÉE
8 jours (56h)

RÉFÉRENCE
GRC65

CATÉGORIE
Cybersécurité et Risques Numériques

Afrique Formation

🎯 OBJECTIFS DE LA FORMATION

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

- ✔ Comprendre les enjeux de la cyberrésilience des infrastructures critiques
- ✔ Identifier et évaluer les cyberrisques majeurs
- ✔ Mettre en place une gouvernance efficace de la cybersécurité
- ✔ Renforcer la protection des systèmes d’information et des environnements industriels
- ✔ Développer des capacités de détection et de réponse aux incidents
- ✔ Élaborer des plans de continuité et de reprise d’activité
- ✔ Sécuriser les données sensibles et les chaînes d’approvisionnement
- ✔ Développer une culture de cybersécurité au sein des organisations
- ✔ Réaliser des audits et des exercices de résilience
- ✔ Renforcer la capacité des organisations africaines à faire face aux cybermenaces
- ✔ Assurer la continuité des services essentiels
- ✔ Déployer une stratégie durable de cyberrésilience

👥 POUR QUI ?

- ✔ Responsables de la cybersécurité (RSSI/CISO)
- ✔ Directeurs des systèmes d’information (DSI)
- ✔ Responsables des infrastructures critiques
- ✔ Administrateurs réseaux et systèmes
- ✔ Experts en cybersécurité et en gestion des risques
- ✔ Opérateurs des secteurs de l’énergie, de l’eau, des transports et des télécommunications
- ✔ Cadres des administrations publiques et agences nationales de cybersécurité
- ✔ Responsables de la continuité d’activité et de la gestion de crise
- ✔ Forces de défense et de sécurité impliquées dans la cyberdéfense
- ✔ Auditeurs et contrôleurs des systèmes d’information
- ✔ Toute personne impliquée dans la protection des infrastructures critiques en Afrique

Afrique Formation

AFRIQUE FORMATION
La Référence en Afrique pour la Formation



Programme détaillé

1 / FONDAMENTAUX DE LA CYBERRÉSILIENCE DES INFRASTRUCTURES CRITIQUES

- Compréhension des concepts de cybersécurité et de cyberrésilience
- Identification des infrastructures critiques en Afrique
- Analyse des enjeux stratégiques, économiques et de souveraineté numérique

2 / GOUVERNANCE ET CADRE RÉGLEMENTAIRE

- Élaboration d’une stratégie de cyberrésilience
- Cadres législatifs et réglementaires nationaux et internationaux
- Rôles et responsabilités des acteurs publics et privés

3 / IDENTIFICATION ET ANALYSE DES RISQUES CYBER

- Cartographie des actifs critiques et des vulnérabilités
- Évaluation des menaces internes et externes
- Analyse des impacts opérationnels, financiers et réputationnels

4 / PROTECTION DES SYSTÈMES D’INFORMATION CRITIQUES

- Mise en œuvre des contrôles de sécurité
- Gestion des accès, des identités et des privilèges
- Sécurisation des réseaux, serveurs et infrastructures cloud

Afrique Formation

5 / SÉCURITÉ DES SYSTÈMES INDUSTRIELS (OT/ICS/SCADA)

- Protection des systèmes de contrôle industriel
- Sécurisation des réseaux OT et des automates industriels
- Gestion des risques liés aux infrastructures énergétiques, hydrauliques et de transport

6 / DÉTECTION, SURVEILLANCE ET RÉPONSE AUX INCIDENTS

- Mise en place d'un Centre des Opérations de Sécurité (SOC)
- Détection des cyberattaques et analyse des événements
- Gestion des incidents et coordination des réponses

7 / CONTINUITÉ D'ACTIVITÉ ET REPRISE APRÈS SINISTRE

- Élaboration d'un Plan de Continuité d'Activité (PCA)
- Mise en œuvre d'un Plan de Reprise d'Activité (PRA)
- Gestion des crises et restauration des services essentiels

8 / PROTECTION DES DONNÉES ET CONFORMITÉ

- Gouvernance des données sensibles
- Chiffrement, sauvegarde et gestion des accès
- Respect des exigences réglementaires en matière de protection des données

9 / GESTION DES RISQUES LIÉS À LA CHAÎNE D'APPROVISIONNEMENT

- Sécurisation des fournisseurs et partenaires critiques
- Gestion des risques liés aux prestataires numériques
- Évaluation de la résilience des écosystèmes technologiques

10 / SENSIBILISATION ET DÉVELOPPEMENT D'UNE CULTURE CYBER

- Formation des collaborateurs aux bonnes pratiques
- Prévention du phishing et de l'ingénierie sociale

Afrique Formation

- Développement d’une culture de vigilance organisationnelle

11 / AUDIT, TESTS DE RÉSILIENCE ET AMÉLIORATION CONTINUE

- Réalisation d’audits de cybersécurité
- Organisation d’exercices de simulation et de tests d’intrusion
- Suivi des indicateurs de performance et amélioration continue

12 / CAS PRATIQUES ET STRATÉGIES DE CYBERRÉSILIENCE EN AFRIQUE

- Analyse de cyberattaques visant des infrastructures critiques
- Élaboration d’une feuille de route de cyberrésilience
- Simulation de gestion de crise cyber dans un contexte africain

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
01 au 10 Fév. 2027	Présentiel - Casablanca
29 Mars au 07 Avr. 2027	Présentiel - Casablanca
24 Mai au 02 Juin 2027	Présentiel - Casablanca
19 au 28 Juil. 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

Document généré le 13/11/2026 — Réf : GRC65
Afrique Formation — Tous droits réservés

Afrique Formation