



Cybersécurité énergétique : protégez vos infrastructures critiques contre les cyberattaques

Lien :

<https://afrique-formation.com/formation/cybersecurite-energetique-protectez-vos-infrastructures-critiques-contre-les-cyberattaques>

 DURÉE
4 jours (28h)

 RÉFÉRENCE
DDE114

 CATÉGORIE
**Exploitation,
Maintenance et Smart
Energy**

OBJECTIFS DE LA FORMATION

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

- ✓ Comprendre les enjeux de la cybersécurité dans l'énergie
- ✓ Identifier les menaces et vulnérabilités
- ✓ Maîtriser les architectures IT/OT des infrastructures
- ✓ Mettre en place des stratégies de protection efficaces
- ✓ Gérer les incidents de cybersécurité
- ✓ Assurer la conformité aux normes et réglementations
- ✓ Protéger les données et systèmes critiques
- ✓ Développer une culture cybersécurité au sein des organisations

POUR QUI ?

- ✓ Ingénieurs en énergie et réseaux
- ✓ Experts en cybersécurité
- ✓ Responsables IT et OT
- ✓ Exploitants d'infrastructures énergétiques
- ✓ Chefs de projets énergie
- ✓ Consultants en sécurité informatique
- ✓ Toute personne impliquée dans la sécurité des systèmes énergétiques

Afrique Formation



Programme détaillé

1 / Introduction à la cybersécurité énergétique

- Définition et enjeux de la cybersécurité
- Spécificités des infrastructures énergétiques (réseaux, centrales, smart grids)
- Menaces et impacts sur la continuité de service

2 / Typologie des cybermenaces

- Malware, ransomware, attaques DDoS
- Intrusions et espionnage industriel
- Menaces internes et erreurs humaines

3 / Architecture des systèmes énergétiques

- Systèmes SCADA et ICS
- Réseaux OT (Operational Technology) vs IT
- Points de vulnérabilité

4 / Gestion des risques cyber

- Identification et cartographie des risques
- Évaluation des vulnérabilités
- Analyse d'impact sur les infrastructures critiques

5 / Normes et réglementations

- Standards internationaux (ISO 27001, NIST, IEC 62443)
- Réglementations sectorielles
- Exigences de conformité

6 / Stratégies de protection des infrastructures

- Sécurisation des réseaux et systèmes
- Gestion des accès et authentification
- Chiffrement des données

7 / Détection et réponse aux incidents

- Systèmes de détection d'intrusion (IDS/IPS)
- Gestion des incidents de cybersécurité
- Plan de réponse et de continuité d'activité

8 / Sécurité des données et des systèmes connectés

- Protection des données sensibles
- Sécurité des objets connectés (IoT énergétique)
- Gestion des mises à jour et correctifs

9 / Gouvernance et culture cybersécurité

- Sensibilisation des équipes
- Organisation de la sécurité
- Amélioration continue des dispositifs

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

 22 au 25 Sep. 2026

 Présentiel -

 24 au 27 Nov. 2026

 Présentiel -

 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>

Document généré le 22/07/2026 — Réf : DDE114

Afrique Formation — Tous droits réservés