Sûreté et Malveillance pour Managers et Cybercriminalité

Lien :
https://afrique-formation.com/formation/srete-et-malveillance-pour-managers-et-cybercriminalite

DURÉE
10 jours (70h)

RÉFÉRENCE
GRC43

CATÉGORIE
Gestion des Risques et Plan de Continuité des Activités

🎯 OBJECTIFS DE LA FORMATION

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

- ✔ Comprendre les enjeux de la sûreté et de la malveillance en entreprise
- ✔ Identifier les différents types de menaces physiques et numériques
- ✔ Évaluer la vulnérabilité de son organisation face aux risques
- ✔ Déployer des mesures de sûreté adaptées au contexte de l’entreprise
- ✔ Mettre en œuvre un plan de prévention contre les actes malveillants
- ✔ Adopter les bons comportements managériaux en matière de sécurité
- ✔ Intégrer la cybersécurité dans les pratiques quotidiennes de l’entreprise
- ✔ Sensibiliser les équipes aux risques internes et externes
- ✔ Réagir efficacement face à une attaque physique ou cyber
- ✔ Renforcer la résilience de l’entreprise grâce à une approche globale
- ✔ Assurer la conformité réglementaire en matière de sûreté et cybersécurité
- ✔ Instaurer une culture de sécurité partagée au sein de l’organisation
- ✔ Collaborer efficacement avec les équipes sécurité, IT et juridiques
- ✔ Exploiter les retours d’expérience pour améliorer les dispositifs de protection
- ✔ Accompagner le changement organisationnel dans un contexte de menace croissante

POUR QUI ?

- Managers et cadres opérationnels en entreprise
- Responsables sécurité, sûreté ou HSE
- Responsables des ressources humaines
- Responsables informatiques et DSI
- Dirigeants de PME et responsables de site
- Responsables de la conformité ou du contrôle interne
- Responsables de la sécurité des systèmes d'information
- Chefs de projets stratégiques ou sensibles
- Membres de cellules de crise ou équipes d’intervention
- Personnels en charge de la prévention des risques
- Cadres dans les secteurs sensibles (industrie, énergie, transport, finance)
- Collaborateurs amenés à gérer des données confidentielles
- Toute personne exposée aux enjeux de sûreté et de cybercriminalité en milieu professionnel
- Acteurs de la gestion de crise ou de la communication institutionnelle

AFRIQUE FORMATION
La Référence en Afrique pour la Formation

Programme détaillé

1 / Introduction à la sûreté en entreprise

- Différence entre sécurité et sûreté
- Enjeux stratégiques pour les organisations
- Responsabilité managériale en matière de sûreté

2 / Typologie des actes de malveillance

- Intrusions, vols, sabotages, espionnage industriel
- Menaces internes : collaborateurs, sous-traitants
- Menaces externes : visiteurs, fournisseurs, hackers

3 / Diagnostic de la vulnérabilité d'un site

- Méthodes d'évaluation des risques
- Identification des points sensibles physiques et logiques
- Analyse des incidents passés

4 / Mesures physiques de sûreté

- Contrôle d'accès : badges, biométrie, surveillance
- Sécurisation des locaux : coffres, barrières, serrures
- Vidéoprotection : implantation, limites légales

5 / Sûreté humaine et organisationnelle

- Rôle des agents de sécurité et des rondes
- Procédures d’accueil et de filtrage des visiteurs
- Sensibilisation des salariés au comportement sécurisé

6 / Prévention de l’espionnage industriel

- Protection des données sensibles et stratégiques
- Comportements à risque en déplacement ou salons
- Bonnes pratiques en communication d’entreprise

7 / Gestion des conflits internes et actes hostiles

- Typologie des conflits et signaux faibles
- Conduite à tenir face aux comportements agressifs
- Collaboration avec les RH et la médecine du travail

8 / Plan de sûreté de l’entreprise

- Élaboration et mise à jour d’un plan de sûreté
- Scénarios de crise et réponses adaptées
- Coordination avec les forces de sécurité publique

9 / Introduction à la cybercriminalité

- Définition et typologie des cybermenaces
- Acteurs de la cybercriminalité : hackers, insiders, groupes organisés
- Conséquences pour l’entreprise : financières, réputationnelles, juridiques

10 / Menaces numériques internes

- Négligence, erreurs humaines, ingénierie sociale
- Fuite ou vol d’informations par les employés

- Mauvaise gestion des accès et mots de passe

11 / Menaces numériques externes

- Phishing, ransomwares, DDoS, intrusion réseau
- Exploitation des failles de sécurité
- Hameçonnage ciblé et attaques personnalisées

12 / Rôle du manager face à la cybermenace

- Vigilance managériale et posture numérique
- Signalement des incidents et remontée d’alerte
- Prise de décision en cas d’attaque informatique

13 / Politiques de cybersécurité d’entreprise

- Charte informatique et règles d’usage
- Protection des terminaux, sauvegardes, antivirus
- Gestion des accès, mises à jour et correctifs

14 / Réaction en cas d’incident de sécurité

- Procédures d’alerte, confinement, récupération
- Communication de crise et gestion de l’image
- Collaboration avec les équipes IT et légales

15 / Cas pratiques, jeux de rôle et retours d’expérience

- Études de cas réels d’attaques et malveillances
- Simulations de gestion de crise
- Bilan collectif des apprentissages

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

03 au 14 Août 2026	Présentiel -
05 au 16 Oct. 2026	Présentiel -
30 Nov. au 11 Déc. 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