Fiche Technique:Formation cybersécurité à Abidjan

Objectifs de la formation

Résultats ciblés et mesurables pour renforcer la sécurité, la conformité et la continuité d'activité.

- Évaluer la posture de sécurité et prioriser les actions à fort impact.
- Cartographier les risques alignés sur les processus métiers.
- Déployer et vérifier les contrôles essentiels (MFA, sauvegardes, segmentation, EDR).
- Mettre en place une sensibilisation continue avec indicateurs de progrès.
- Structurer la réponse aux incidents (playbooks, tests) et préparer les audits avec preuves tangibles.

> Approche 100% terrain : cas réels, ateliers collaboratifs, livrables et modèles directement exploitables.

Population cible

Pour les organisations à Abidjan confrontées à des enjeux de disponibilité, intégrité et confidentialité.

- Dirigeants et managers souhaitant structurer une gouvernance cyber efficace.
- RSSI/DSI et équipes IT/OT en charge de systèmes critiques et hybrides.
- Responsables qualité, conformité, HSE et achats gérant la sous-traitance.
- Équipes projets (ERP, WMS, MES, cloud, IoT) intégrant la sécurité dès la conception.
- Opérationnels (finance, RH, logistique, maintenance, service client) exposés au phishing et à la fraude.

Durée de la formation

Modalité	Durée indicative
Intensif 3 jours	24 heures
Rythme 2+2+2	3 × 4 heures
Hybride terrain	2 jours + 2 ateliers

> Formats : présentiel intra sur site, distanciel synchrone ou hybride. Évaluations intermédiaires et certification interne.

Programme de la formation

Parcours structuré : diagnostiquer, prioriser, sécuriser, entraîner.

Module 1 — Cartographie des risques et gouvernance

- Inventaire des actifs, menaces et impacts métier.
- Matrice de risques et rôles/instances de gouvernance clairs.

Module 2 — Contrôles techniques essentiels

- MFA, correctifs, durcissement postes/serveurs, segmentation réseau.
- Protections mail/web, sauvegardes 3-2-1, supervision et journalisation.

Module 3 — Protection des données et conformité

- Registres de traitements, politiques de conservation, gestion des accès.
- Clauses contractuelles, analyses d’impact, procédures de violation.

Module 4 — Réponse aux incidents et continuité

- Playbooks (phishing, ransomware, compromission, exfiltration) et tests de sauvegardes.
- Coordination IT/métiers/juridique/direction et communication maîtrisée.

Module 5 — Chaîne d’approvisionnement et fournisseurs

- Critères de sélection, clauses sécurité, revues périodiques et chiffrement.
- Exigences de notification et preuves pour audits et grands comptes.

Module 6 — Sensibilisation avancée et culture cyber

- Parcours adaptés par métier avec indicateurs (taux de clics, incidents, MFA).
- Plan de formation continue et durable.
