Fiche Technique:Formation cybersécurité au Cameroun

Objectifs de la formation

Acquis opérationnels, adaptés au contexte camerounais et aux exigences clients/partenaires.

- Diagnostiquer la surface d'attaque et prioriser les actions.
- Définir une feuille de route réaliste et chiffrée.
- Déployer les contrôles essentiels: pare-feu, EDR, MFA, sauvegardes.
- Structurer détection, réponse à incident et capitalisation (playbooks).
- Renforcer la culture sécurité et la lutte anti-phishing.
- Préparer audits et initier la conformité aux référentiels courants.

> Livrables fournis: gabarits, grilles, politiques, procédures et check-lists réutilisables.

Population cible

- DSI, managers IT, responsables sécurité/qualité/conformité, chefs de projet digital.
- Admins systèmes/réseaux, équipes support, DevOps, analystes SOC débutants.
- Directions métiers exposées aux risques numériques; organisations publiques.
- Secteurs: BTP, industrie, énergie, logistique, maintenance, transport, agro-industrie, services, secteur public.
- Établissements financiers, intégrateurs numériques, entités en transformation digitale.
- Directions générales et RH cherchant l'alignement gouvernance-technologies-conformité.

Durée de la formation

Formats flexibles: présentiel, distanciel ou mixte. Sessions fractionnables en demi-journées.

Parcours	Durée	Modalité	Public
Essentiels opérationnels	2 jours	Présentiel ou distanciel	Techniciens, administrateurs
Gestion de la sécurité	3 jours	Présentiel ou distanciel	Managers IT, responsables sécurité
Réponse à incident	2 jours	Présentiel	Équipes NOC/SOC, chefs de projet
Programme complet	5 à 8 jours	Mixte	Équipes pluridisciplinaires

> Évaluations selon le parcours: quiz, ateliers pratiques, études de cas, exercices de crise, plan d'action.

Programme de la formation

1. Cartographie des risques et priorités

- Méthodes, outils et gabarits réutilisables.

2. Gouvernance, politiques et plan de sécurité

- Traduire exigences clients/réglementaires en règles applicables.

3. Sécurisation des postes et serveurs

- Durcissement, EDR, MFA, correctifs, sauvegardes.

4. Protection réseau et accès distants

- Segmentation, VPN, filtrage, accès à privilèges, supervision.

5. Cloud et SaaS en contexte local

- Identités, chiffrement, journaux, configuration et posture.

6. OT/IoT: maintenance, énergie, logistique

- Mesures à faible impact, supervision, gestion des fournisseurs.

7. Réponse à incident

- Playbooks, coordination et remontée d’alerte.

8. Sensibilisation et ingénierie sociale

- Simulations de phishing, scénarios, indicateurs.

9. Continuité d’activité et PRA

- Scénarios réalistes adaptés aux contraintes de connectivité.

10. Métriques, tableaux de bord et audit

- Preuves, traçabilité et communication au comité de direction.

> Chaque module alterne théorie, démonstrations, cas pratiques et exercices de crise; livrables prêts à l’emploi fournis.
