Fiche Technique:Audit Cybersécurité en Guinée

Objectifs de la formation

- Diagnostiquer la sécurité informatique des entreprises guinéennes.
- Identifier vulnérabilités techniques et organisationnelles.
- Vérifier conformité aux normes locales et internationales.
- Proposer un plan d’action stratégique adapté au contexte.
- Évaluer la gestion des incidents et contrôles d’accès.
- Renforcer la sensibilisation et outiller la direction.

Population cible

- Entreprises de tous secteurs sensibles (finance, télécoms, administrations, extractives, agroalimentaires).
- Directeurs des systèmes d’information et responsables sécurité IT.
- Équipes opérationnelles en gestion des réseaux et conformité.
- PME souhaitant renforcer leur posture de sécurité et conformité.
- Spécifiquement établissements bancaires, opérateurs télécoms, zones économiques et industrielles guinéennes.

Durée de la formation

Phase	Objectifs	Durée estimée
Diagnostic initial	Comprendre contexte, recueil et périmètre	1 à 2 semaines
Analyse documentaire	Contrôle conformité réglementaire et procédures	1 semaine
Recommandations et plan d’action	Mesures adaptées et priorisées	1 semaine
Suivi et accompagnement	Mise en œuvre et évaluation continue	Variable selon besoins

Programme de la formation

Étape 1 : Diagnostic initial

- Analyse du contexte et des actifs critiques.
- Entretiens et examen des infrastructures.

Étape 2 : Analyse documentaire et réglementaire

- Examen des politiques, procédures et audits précédents.
- Vérification de conformité légale et réglementaire.

Étape 3 : Recommandations et plan d’action

- Rapport avec mesures techniques et organisationnelles.

- Mesures priorisées selon risques et ressources.

Étape 4 : Suivi et accompagnement

- Suivi de la mise en œuvre des recommandations.
- Rapports réguliers et interventions ciblées.

> Ce programme permet d’adapter l’audit aux spécificités guinéennes et d’assurer une sécurité adaptée aux enjeux locaux.
