Fiche Technique:Audit Cybersécurité au Maroc

Objectifs de la formation

- Réaliser un état des lieux exhaustif de la sécurité informatique.
- Identifier vulnérabilités et failles potentielles.
- Évaluer la conformité réglementaire locale et internationale.
- Fournir un rapport clair pour la prise de décision.
- Définir un plan d'action pragmatique et priorisé.

Population cible

- Entreprises de tous secteurs souhaitant évaluer leur sécurité IT.
- Directions générales, responsables sécurité, informatiques, risques.
- Équipes opérationnelles en charge des infrastructures IT.
- PME et grands groupes dans secteurs critiques (finance, énergie, télécoms).
- Organisations implantées en zones industrielles et hubs économiques.

Durée de la formation

Phase	Description	Durée indicative
Diagnostic initial	Collecte d'informations et cadrage	1 semaine
Analyse documentaire	Vérification des politiques et conformité	1 à 2 semaines
Analyse technique	Tests d'intrusion et audit infrastructure	1 à 2 semaines
Recommandations et plan d'action	Remise du rapport et plan priorisé	1 semaine

Durée totale : 3 à 6 semaines selon taille et complexité. Formats présentiel, distant ou hybride possibles.

Programme de la formation

Étape 1 : Diagnostic initial

- Compréhension organisationnelle et collecte d'infos.

Étape 2 : Analyse documentaire et réglementaire

- Étude des politiques, conformité locale (Loi 09-08) et normes (ISO 27001).

Étape 3 : Analyse technique sur le terrain

- Tests d'intrusion, audit des systèmes et protection des données sensibles.

Étape 4 : Recommandations et plan d'action

- Rapport complet avec plan de remediation chiffré et priorisé.

Étape 5 : Suivi et accompagnement

> Mise en œuvre des mesures, formation et pilotage pour durabilité des bonnes pratiques.
