Fiche Technique:Audit Cybersécurité à Agadir

Objectifs de la formation

- Fournir un diagnostic complet et fiable de la sécurité informatique.
- Identifier vulnérabilités et analyser les risques.
- Vérifier la conformité aux normes internationales et régulations.
- Établir un rapport clair, actionnable et priorisé.
- Sensibiliser les équipes internes aux bonnes pratiques.
- Optimiser la gestion des incidents et réduire le risque de cyberattaque.

Population cible

- Entreprises et organismes situés à Agadir et environs (PME, grandes entreprises, secteur public).
- Services IT, responsables sécurité, DSI, chefs de projet, directions générales.
- Secteurs industriels, tertiaires, logistiques, commerciaux.
- Gestionnaires des risques, conformité réglementaire, continuité d'activité.
- Infrastructures critiques, notamment réseaux SCADA et radio industrielles ou portuaires.

Durée de la formation

Type d'audit	Durée estimée	Intervention
Diagnostic initial rapide	1 à 2 semaines	Sur site / Télétravail
Audit complet avec tests	4 à 6 semaines	Sur site majoritairement
Audit spécialisé réseaux radio et SCADA	3 à 5 semaines	Sur site et télétravail

> La durée dépend de la taille, complexité et périmètre audité. Formats flexibles adaptés aux contraintes opérationnelles.

Programme de la formation

Étape 1 : Diagnostic initial

- Collecte d'informations sur SI et environnement.
- Entretiens avec responsables IT.
- Analyse des infrastructures et dispositifs de sécurité.

Étape 2 : Analyse documentaire et réglementaire

- Revue des politiques, procédures, référentiels de conformité.
- Évaluation conformité normes ISO 27001, RGPD, exigences sectorielles locales.

Étape 3 : Recommandations et plan d’action

- Rédaction rapport détaillé avec classement des risques.
- Plan d’action clair et adapté à l’entreprise.

Étape 4 : Suivi et accompagnement

- Assistance mise en œuvre mesures correctives.
- Audits de contrôle et mise à jour procédures.
- Préparation aux audits de conformité futurs.
