Fiche Technique:Formation sécurité systèmes et réseaux au Maroc

Objectifs de la formation

- Cartographier actifs, flux et dépendances; définir criticités et segmentation.
- Établir une politique de sécurité et un modèle de menace adaptés au contexte.
- Concevoir une architecture réseau cloisonnée avec filtrage, journalisation et supervision (SOC/SIEM).
- Durcir Windows/Linux, standardiser les configurations et automatiser le patch management.
- Renforcer identités et accès: MFA, moindre privilège, PAM, traçabilité et revues périodiques.
- Protéger connexions et transferts (VPN, SSH, SFTP), chiffrer les échanges et limiter l'exposition; structurer la détection et la réponse aux incidents via playbooks.

> Résultats attendus: réduction de la surface d'attaque, baisse des accès excessifs, accélération des correctifs, meilleure visibilité grâce à des tableaux de bord et indicateurs.

Population cible

- DSI, RSSI, chefs de projet IT pilotant conformité et défense en profondeur.
- Administrateurs systèmes/réseaux (pare-feu, durcissement, politiques d'accès).
- Architectes techniques, ingénieurs cloud et DevOps (industrialisation des configurations).
- Auditeurs internes, responsables conformité et risk managers (gouvernance/risques).
- Équipes support/exploitation (supervision fiable, alertes pertinentes, réaction aux incidents).

> Prérequis recommandés: socle en administration systèmes, réseaux ou cloud; intérêt pour la sécurité opérationnelle.

Durée de la formation

Format	Durée	Modalités
Intensif (Bootcamp)	5 jours	Présentiel/Distanciel, ateliers quotidiens
Étendu (Hebdomadaire)	6 à 8 semaines	2 sessions/sem., coaching inter-sessions
Hybride (Projet)	8 à 12 semaines	Formation + accompagnement projet

> Évaluation: quizz, exercices pratiques et évaluation finale; environnements de test et scénarios guidés.

Programme de la formation

Parcours alternant apports, démonstrations et ateliers, avec guides de configuration, matrices de risques et modèles prêts à l'emploi.

Module 1 — Gouvernance, réglementation et gestion des risques

- Référentiels (ISO 27001, NIST, CNDP), rôles et responsabilités.
- Politique de sécurité, classification, registre de risques et indicateurs.

Module 2 — Architecture réseau sécurisée et défense en profondeur

- Segmentation par zones et niveaux de confiance; politiques de pare-feu auditées.
- Journalisation et surveillance pour limiter les mouvements latéraux; DMZ.

Module 3 — Durcissement des systèmes Windows et Linux

- Hardening, patch management, baselines et contrôles automatisés.
- Gestion des écarts; standardisation des rôles critiques.

Module 4 — Identités, habilitations et privilèges

- MFA, moindre privilège, sessions privilégiées traçables.
- Revues périodiques; rôles/groupes et demandes outillées.

Module 5 — Connexions sécurisées et transferts chiffrés

- VPN, SSH, SFTP; accès distants conditionnels, segmentation des tunnels.
- Protection endpoints, rotation des clés, supervision des flux.

Module 6 — Cloud sécurisé: AWS, Azure, GCP

- IAM, journalisation, réseau, chiffrement, gestion des secrets.
- Revues de comptes et alertes de posture pour éviter les erreurs de configuration.

Module 7 — Supervision, SOC, SIEM et réponse aux incidents

- Cas d'usage, alertes utiles, architectures de supervision pragmatiques.
- Playbooks: détection, confinement, remédiation et reporting.

Module 8 — Conformité, audit, PRA/PCA et amélioration continue

- Cycles d'audit et de revue; tests PRA/PCA.
- Tableaux de bord, feuilles de route et registres de preuves.