Fiche Technique:Formation cybersécurité en entreprise au Maroc

Objectifs de la formation

Résultats attendus et compétences opérationnelles.

- Réduire les incidents évitables et améliorer la conformité.
- Transformer les bonnes pratiques en habitudes: MFA, politiques d'accès, procédures de réponse, contrôle des tiers.
- Identifier, prévenir et réagir aux phishing, BEC, rançongiciels et erreurs de configuration.
- Mettre en place des KPI/KRI, tableaux de bord et boucles d'amélioration continue.
- Renforcer la défense technique: EDR/antivirus, patch management, durcissement, supervision des accès à privilèges.
- Aligner gouvernance, risques et priorités métiers pour accélérer la décision.

> Focus résultats: baisse mesurable des incidents, activation MFA, amélioration continue par indicateurs.

Population cible

Publics concernés et prérequis.

- Dirigeants/Comex, DAF, DRH, DSI, responsables risques, conformité et métiers.
- Profils IT/sécurité et administrateurs systèmes (volets d'approfondissement).
- Équipes support: achats, finance, juridique, relations fournisseurs.
- Organisations multi-sites/distribuées: harmonisation siège/filiales/partenaires.
- Prérequis: aucun requis technique pour la sensibilisation; formats présentiel, distanciel ou hybride.

Durée de la formation

Parcours modulables: 1 à 5 jours, consécutifs ou fractionnés, en présentiel, distanciel ou hybride.

Parcours	Durée indicative	Pédagogie	Livrables
Socle de sensibilisation	1 jour	Ateliers, quiz, simulations	Fiches réflexes, supports, plan d'action
Gouvernance & décision	0,5 à 1 jour	Cas d'usage, tableaux de bord	KPI/KRI, matrice de risques, feuille de route
Hygiène technique	1 à 2 jours	Démos, check-lists, guides	Checklist EDR/MFA, modèles de politiques
Réponse aux incidents	1 jour	Table-top, scénarios, exercices	Playbooks, canevas de communication

> Diagnostic initial, évaluations pré/post-formation et rapport de recommandations (feuille de route 30/60/90 jours).

Programme de la formation

Parcours modulaire et progressif; modules suivables indépendamment ou intégrés.

> Ressources: fiches réflexes, check-lists, scénarios d’attaque, guides de décision, canevas prêts à l’emploi.

Parcours de sensibilisation et d’initiation

- Concepts clés, risques majeurs au Maroc, réflexes à adopter.
- Volets dirigeants (priorisation/budget/crise) et collaborateurs (quiz, simulations) pour ancrer les comportements.

Bonnes pratiques utilisateurs et hygiène numérique

- Gestes du quotidien: verrouillage, pièces jointes, outils collaboratifs, classification, contrôle d’accès.
- Postes de travail: mises à jour, EDR/antivirus, gestion des périphériques, chiffrement.

Mots de passe, authentification et protection des accès

- Politiques robustes: gestionnaire de mots de passe, MFA adapté, surveillance des connexions.
- Accès à privilèges: moindre privilège, segmentation, journalisation, PAM et alertes temps réel.

Phishing, ingénierie sociale et fraudes

- Cas locaux et simulations pour détecter phishing et manipulations.
- SMS, messageries, appels, réseaux sociaux; validation renforcée (RIB, factures, fraude au président).

Réponse aux incidents et continuité d’activité

- Préparation, détection, confinement, communication, retour d’expérience.
- Exercices table-top, simulations ransomware; indicateurs MTTD/MTTR pour améliorer la résilience.