Fiche Technique:Formation cybersécurité à Tanger

Objectifs de la formation

Synthèse des acquis concrets visés à l’issue de la formation.

- Bâtir une feuille de route cyber alignée sur les enjeux métiers et la conformité locale.
- Cartographier les actifs critiques et dépendances; prioriser les mesures par scénarios de menace.
- Déployer les contrôles essentiels: MFA, segmentation réseau, durcissement postes, supervision, sauvegardes testées, PCA/PRA.
- Structurer la gouvernance et clarifier les rôles du COMEX aux équipes terrain.
- Prévenir fraudes et ingénierie sociale via des actions de sensibilisation métier.
- Organiser la détection et la réponse à incident; piloter par indicateurs (MTTD, MTTR, patchs, sauvegardes).

> Approche pragmatique: ateliers, scénarios d’attaque réalistes et livrables immédiatement exploitables.

Population cible

- Dirigeants et DAF souhaitant maîtriser impacts financiers et légaux.
- DSI, RSSI, responsables IT/OT des environnements industriels et logistiques.
- Chefs d’exploitation, responsables maintenance et QHSE, équipes opérationnelles.
- Managers RH et responsables formation pour les plans de sensibilisation.
- PME industrielles, opérateurs logistiques, sociétés de maintenance et établissements publics de la région de Tanger.

Durée de la formation

Formats modulables selon vos contraintes d’exploitation.

Format	Détails
Intensif	3 jours pour condenser l’essentiel et structurer la feuille de route.
Étalé	6 demi-journées pour intégrer chaque bloc sans interrompre l’activité.
Modalités	Intra-entreprise (sur vos processus) ou inter-entreprises (vision comparée locale).
Lieu / Rythme	Présentiel à Tanger ou à distance; exercices concrets, outils réutilisables et suivi post-formation.

Programme de la formation

Modules orientés résultats, adaptés aux réalités industrielles et logistiques de Tanger.

Cartographie des risques et priorisation des actions

- Analyse contextualisée; matrice de risques et cartographie des actifs pour orienter les contrôles.

Hygiène numérique et sécurisation des postes de travail

- Durcissement, correctifs, contrôles d’accès; procédures compatibles BTP/industrie/logistique.

Protection des systèmes industriels et des réseaux OT

- Segmentation, inventaire OT, supervision de trafic, correctifs et confinement sans arrêt de production.

Supervision, détection et réponse à incident

- Playbooks adaptés (ransomware, phishing, compromission, arrêt de ligne); coordination IT–opérations–direction.

Conformité, protection des données et responsabilité

- Registres, notices et procédures de notification; conformité au service du business et des partenaires.

Exercices et simulations

- Rapports d’exercice et plans d’amélioration; apprentissage expérientiel.
