Fiche Technique:Formation cybersécurité au Sénégal

Objectifs de la formation

Compétences immédiatement actionnables pour passer d'une posture réactive à proactive.

- Réaliser des analyses de risques ciblées et prioriser les plans d'action.
- Définir une politique de sécurité pragmatique et des normes internes.
- Déployer les contrôles essentiels (durcissement, segmentation, MFA, correctifs).
- Réduire la surface d'attaque et sécuriser les environnements hybrides.
- Mettre en place la détection et la réponse aux incidents (procédures, exercices).
- Piloter audits, indicateurs et communication avec les parties prenantes.

> Résultats visés : vulnérabilités réduites, temps de réaction amélioré, conformité renforcée, maturité accrue.

Population cible

- Dirigeants et directeurs de BU orientant la résilience et la croissance.
- DSI, RSSI, responsables IT et chefs de projet bâtissant le référentiel sécurité.
- Responsables opérations industrielles, maintenance, qualité (intégration sécurité/ processus).
- Équipes réseaux, systèmes, cloud, support (pratiques et réflexes d'intervention).
- Conformité, juristes, responsables des données (alignement règlementaire/contrôles).
- Managers métiers (logistique, transport, BTP, agro-industrie, services, secteur public).

Durée de la formation

Formats modulables : présentiel, distanciel synchrone ou hybride, inter/intra-entreprises selon sites au Sénégal.

Format	Durée indicative	Public	Livrables
Essentiel inter-entreprises	3 jours	Managers, équipes IT	Plan d'action 90 jours, check-lists
Parcours avancé hybride	6 à 8 semaines	RSSI, DSI, responsables risques	Roadmap sécurité, kits de sensibilisation
Intra sur site (sur-mesure)	2 à 5 jours + coaching	Équipes mixtes IT/OT/métiers	Procédures IR, matrices RACI, tableaux de bord
Ateliers sectoriels	1 à 2 jours	BTP, logistique, énergie, secteur public	Modèles de politiques et scénarios dédiés

Programme de la formation

Alternance d’apports structurés, cas d’usage sénégalais et ateliers pratiques, reliés à des objectifs business concrets.

Gouvernance et gestion des risques

- Rôles, comités, politiques, normes internes, indicateurs.
- Priorisation des risques, plans d’action, pilotage des audits et conformité.

Sécurité des infrastructures et du cloud

- Durcissement, segmentation, authentification forte, gestion des correctifs.
- Check-lists pour sites distants, chantiers et contextes à connectivité variable.

Protection des données et conformité

- Chiffrement, gestion des accès, journalisation, conservation, anonymisation.
- Registres, analyses d’impact, documentation et preuve de conformité.

Détection et réponse aux incidents

- Scénarios réalistes : ransomware, identifiants compromis, fraude, messagerie.
- Procédures pas-à-pas, communication de crise, matrices RACI, entraînements.

Culture cyber et sensibilisation

- Programmes ciblés pour agents, chantiers, entrepôts, maintenance, fonctions commerciales/administratives.
- Messages et exercices adaptés pour réduire durablement les comportements à risque.

Partenariats et benchmarks régionaux

- Appui sur des repères francophones et écosystèmes professionnels.
- Benchmarks adaptés au contexte sénégalais pour renforcer la gouvernance.
