SWA TECH

Offres et services

Cybersécurité et digitalisation sécurisée

France et Afrique francophone

Audit · Conformité · SOC · Infrastructure · Développement sécurisé · Formation

CONTACT

Meyan Traoré

Experte en cybersécurité et fondatrice

E-mail	traore.meyan.m@gmail.com
LinkedIn	https://www.linkedin.com/in/meyan/
Site	swa-tech.fr
Tél.	+33 6 88 78 26 28

SWA Tech - Offres et services

Table des matières

SWA Tech - Offres et services 1

Qui sommes-nous 2

1. Audit de sécurité et tests d'intrusion 2

2. Gouvernance, risques et conformité (GRC) 3

3. Supervision de sécurité (SOC) et réponse aux incidents 3

4. Sécurité réseau et infrastructure 4

5. Développement web et applicatif sécurisé 4

6. Sensibilisation et formation 5

Notre méthode d'intervention 5

Modalités et contact 5

Qui sommes-nous

SWA Tech accompagne les TPE, PME, indépendants, associations et institutions dans la sécurisation et la digitalisation de leurs activités, en France et en Afrique francophone.

Notre force : une offre numérique de bout en bout, de l'audit de sécurité au développement d'applications sécurisées, portée par une expertise technique (SOC, tests d'intrusion) et en gouvernance (ISO 27001, gestion des risques).

1 Audit de sécurité et tests d'intrusion

> Objectif : mesurer votre niveau de sécurité réel et identifier les failles avant qu'elles ne soient exploitées.

Prestation	Contenu	Livrable
Diagnostic de sécurité	Entretiens, revue de l'organisation, des accès, des sauvegardes et des postes de travail	Note de maturité et plan d'actions priorisé
Audit du système d'information	Analyse de l'architecture, des configurations et des pratiques de sécurité	Rapport d'audit : forces, vulnérabilités, recommandations
Scan et gestion des vulnérabilités	Recherche automatisée de failles, qualification, suivi des corrections	Rapport de vulnérabilités classées par criticité
Test d'intrusion externe	Simulation d'attaque depuis Internet sur vos sites, serveurs et services exposés	Rapport technique + synthèse pour la direction
Test d'intrusion interne	Simulation d'un attaquant déjà présent sur le réseau (poste compromis, prestataire)	Scénarios d'attaque et remédiations
Audit d'application web	Tests sur vos sites et applications	Vulnérabilités applicatives et correctifs

Chaque audit se conclut par une restitution orale et un plan d'actions concret, adapté à vos moyens.

2 Gouvernance, risques et conformité (GRC)

> Objectif : structurer votre sécurité, maîtriser vos risques et répondre aux exigences réglementaires et contractuelles.

Prestation	Contenu	Livrable
Analyse de risques	Identification des actifs critiques, des menaces et de leur impact	Cartographie des risques et plan de traitement
Politique de sécurité (PSSI)	Rédaction ou révision du cadre de gouvernance sécurité	PSSI validée par la direction
Charte informatique	Règles d'usage des outils numériques pour les collaborateurs	Charte prête à diffuser
Accompagnement ISO 27001	Mise en place du système de management de la sécurité (SMSI), préparation à l'audit de certification	Documentation SMSI, déclaration d'applicabilité
Protection des données	RGPD en France ; loi malienne n° 2013-015	Registre des traitements, procédures
Plan de continuité et de reprise	Stratégie de sauvegarde, scénarios de crise, reprise d'activité	PCA / PRA documentés et testés

Notre démarche suit les cinq fonctions de référence : identifier, protéger, détecter, répondre, restaurer.

3 Supervision de sécurité (SOC) et réponse aux incidents

> Objectif : détecter les attaques en temps réel et réagir vite pour limiter leur impact.

- **Supervision SOC** : surveillance de vos journaux et équipements, détection, analyse et qualification des menaces, alertes. Formules en heures ouvrées ou 24 h/24, 7 j/7.
- **Procédures d'escalade** : définition de qui alerter, quand et comment, selon la gravité de l'incident.
- **Réponse à incident** : confinement, investigation (analyse forensique), éradication et retour à la normale.
- **Retour d'expérience** : rapport d'investigation et mesures pour éviter que l'incident se reproduise.
- **Pilotage** : rapport mensuel d'activité et comité de suivi avec vos équipes.

4 Sécurité réseau et infrastructure

> Objectif : disposer d'une infrastructure fiable, cloisonnée et protégée.

- **Audit et durcissement réseau** : revue des pare-feu, du Wi-Fi, de la segmentation et des accès distants (VPN).
- **Conception et sécurisation d'architecture** : réseaux LAN/WAN, interconnexions sécurisées entre sites.
- **Serveurs et virtualisation** : installation, configuration sécurisée, consolidation.
- **Sauvegarde et stockage sécurisé** : stratégie de sauvegarde, archivage, tests de restauration.
- **Gestion des accès** : comptes à privilèges, authentification forte, revue des droits.

Les travaux d'infrastructure sur site au Mali sont réalisés avec notre partenaire spécialisé en réseaux et systèmes.

5 Développement web et applicatif sécurisé

> Objectif : des outils numériques performants, conçus dès le départ pour résister aux attaques.

- **Sites web sécurisés** : sites vitrines et e-commerce, optimisés pour le référencement.
- **Applications web et mobiles** : développement sur mesure, intégrant la sécurité à chaque étape (authentification, chiffrement, protection des données).
- **Migration et optimisation** : modernisation de sites existants, hébergement sécurisé, performances.
- **DevSecOps** : mise en production automatisée et contrôles de sécurité intégrés au cycle de développement.
- **Maintenance et support mensuel** : mises à jour, sauvegardes, surveillance et assistance.

6 Sensibilisation et formation

> Objectif : faire de vos collaborateurs la première ligne de défense.

- **Sensibilisation des utilisateurs** : ateliers sur l'hameçonnage (phishing), les mots de passe, les bons réflexes au quotidien.
- **Campagnes de faux phishing** : mesure du niveau de vigilance et suivi des progrès.
- **Sensibilisation des dirigeants** : enjeux, responsabilités et décisions clés en cas de crise.
- **Formation à la création web** : pour les équipes qui souhaitent gérer leur site en autonomie.

Les contenus sont adaptés au niveau et au secteur de chaque public, en présentiel ou à distance.

Notre méthode d'intervention

1. **Échange initial** : compréhension de votre activité, de vos enjeux et de vos contraintes.
2. **Diagnostic** : état des lieux de votre sécurité, sur site ou à distance.
3. **Proposition** : plan d'actions priorisé et devis détaillé.
4. **Mise en œuvre** : réalisation des prestations retenues, avec un suivi régulier.
5. **Suivi dans la durée** : accompagnement, mesures d'amélioration et points de contrôle périodiques.

Modalités et contact

- **Tarifs** : sur devis, établi après l'échange initial selon le périmètre et la durée de l'intervention.
- **Paiement** : modalités flexibles.
- **Interventions** : en France et en Afrique francophone, sur site ou à distance.
- **Confidentialité** : engagement de confidentialité sur toutes les informations recueillies.