Pentester / Testeur d'intrusion Senior

LIEU	CONTRAT	DATE LIMITE
Siège social VEONE, Abidjan	**CDI**	**02/12/2026**

Description du poste

Dans le cadre du renforcement de notre pôle cybersécurité, nous recherchons un Pentester Senior capable d'accompagner nos clients et nos équipes projets dans la sécurisation de leurs applications web, mobiles et API, de la conception jusqu'à la mise en production.

Missions et responsabilités

Tests d'intrusion

- Piloter et réaliser des tests d'intrusion sur des applications web, mobiles (Android / iOS) et API (REST, GraphQL), en boîte noire, grise et blanche.
- Définir le périmètre, les règles d'engagement et le plan de test avec le client.
- Appliquer une méthodologie rigoureuse et reconnue (OWASP WSTG, OWASP MASTG, PTES, OSSTMM).
- Réaliser des revues de code source orientées sécurité (Java, Kotlin, Swift, JavaScript/Node.js, PHP, .NET… selon les projets).

Restitution et accompagnement

- Rédiger des rapports clairs : synthèse managériale, détail technique des vulnérabilités, niveau de criticité (CVSS), preuves et recommandations.
- Présenter les résultats aux équipes techniques et à la direction.
- Accompagner les équipes de développement dans la remédiation et réaliser les contre-audits.
- Participer à la sécurisation dès la conception (Security by Design, revues d'architecture, analyses de risques).
- Contribuer à l'intégration de contrôles de sécurité dans le cycle de développement (DevSecOps, SAST/DAST).

Encadrement et expertise

- Encadrer et former les pentesters juniors (revue de leurs travaux, montée en compétences).
- Faire évoluer la méthodologie, les modèles de rapports et les outils internes.
- Assurer une veille offensive sur les nouvelles vulnérabilités et techniques d'attaque (OWASP, MITRE ATT&CK, CVE).

Profil recherché

Formation : Bac+4/5 en informatique, spécialisation cybersécurité.

Expérience : Minimum 5 ans en tests d'intrusion, dont une part significative sur des applications web et mobiles.

Compétences techniques

- Maîtrise des référentiels OWASP Top 10, OWASP API Security Top 10, ASVS, MASVS et Mobile Top 10.
- Exploitation des vulnérabilités applicatives (injections, contrôle d'accès, authentification, logique métier, désérialisation…).
- Analyse d'applications mobiles : reverse engineering, contournement de protections (root/jailbreak detection, SSL pinning), analyse statique et dynamique.
- Outils : Burp Suite Pro, OWASP ZAP, Frida, Objection, MobSF, Jadx, Postman, sqlmap, Nuclei, Nmap ; outils SAST (SonarQube, Checkmarx, Fortify…).
- Bonne compréhension des architectures applicatives, du cloud et des mécanismes d'authentification (OAuth2, OpenID Connect, JWT).
- Capacité à écrire des scripts (Python, Bash…).

Certifications appréciées

OSCP, OSWE, BSCP (Burp Suite Certified Practitioner), eWPTX, eMAPT, GMOB, GWAPT.

Qualités personnelles

- Excellente capacité rédactionnelle et pédagogique.
- Rigueur, éthique et sens de la confidentialité.

- Aisance relationnelle face aux clients et aux équipes techniques.
- Leadership et goût de la transmission.

Conditions et avantages

- **Rémunération** : selon profil et expérience, précisée pendant le processus de recrutement.
- **Assurance santé.**

Comment postuler

Déposez votre candidature en ligne sur notre espace recrutement, rubrique *Offres d'emploi*. Vous y suivrez ensuite l'avancement de votre dossier et y recevrez vos convocations d'entretien.

VEONE · Cocody, Riviera 2 Bonoumin, lot 302 ilot 23 · Abidjan · infos@veone.net · http://www.veone.net
Offre publiée le 02/11/2026. Candidatures reçues jusqu'au 02/12/2026 inclus. Référence RE - PENT - SE - 01.