Red Teamer

LIEU	CONTRAT	DATE LIMITE
Siège social VEONE, Abidjan	**CDI**	**03/12/2026**

Description du poste

Dans le cadre du développement de notre offre de sécurité offensive, nous recherchons un Red Teamer expérimenté. Il simulera des attaques réalistes et ciblées, à la manière d'un attaquant réel, afin d'évaluer la capacité des organisations à prévenir, détecter et répondre aux menaces avancées.

Missions et responsabilités

Préparation des opérations

- Définir avec le client les objectifs, le périmètre, les scénarios d'attaque et les règles d'engagement.
- Réaliser la phase de reconnaissance et de collecte d'informations en sources ouvertes (OSINT).
- Préparer l'infrastructure d'attaque (serveurs C2, redirecteurs, domaines, charges utiles).
- Construire des scénarios d'attaque inspirés de menaces réelles (émulation d'adversaires basée sur MITRE ATT&CK).

Conduite des opérations Red Team

- Obtenir un accès initial par différents vecteurs : ingénierie sociale, phishing, exposition externe, accès physique si prévu au contrat.
- Mener les phases de post-exploitation : élévation de privilèges, mouvements latéraux, persistance, collecte d'identifiants.
- Compromettre les environnements Active Directory et Azure AD / Entra ID.
- Contourner les mécanismes de défense (antivirus, EDR, filtrage réseau, journalisation) de façon discrète.
- Atteindre les objectifs définis (« trophées ») tout en évaluant le niveau de détection du SOC.

Restitution et amélioration de la défense

- Rédiger des rapports détaillés : chronologie de l'attaque, chemins de compromission, faiblesses identifiées et recommandations.
- Présenter les résultats aux équipes techniques et à la direction.
- Animer des exercices Purple Team avec les équipes SOC et Blue Team pour améliorer les capacités de détection.
- Développer des outils, scripts et charges utiles adaptés aux missions.
- Assurer une veille permanente sur les techniques d'attaque, les groupes de menaces (APT) et les outils offensifs.

Profil recherché

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

Expérience : Minimum 5 ans en sécurité offensive (tests d'intrusion internes, Active Directory), dont au moins 2 ans sur des missions Red Team.

Compétences techniques

- Maîtrise approfondie des attaques Active Directory (Kerberoasting, AS-REP Roasting, délégations, ADCS, Pass-the-Hash / Pass-the-Ticket, DCSync…).
- Maîtrise des frameworks de Command & Control : Cobalt Strike, Sliver, Mythic, Havoc, Brute Ratel.
- Outils offensifs : BloodHound, Impacket, Rubeus, Mimikatz, CrackMapExec / NetExec, Responder, Certipy.
- Techniques de contournement des EDR et antivirus (obfuscation, injection de processus, exécution en mémoire).
- Ingénierie sociale et campagnes de phishing (GoPhish, Evilginx).
- Connaissance des environnements cloud (Azure / Entra ID, AWS) et de leurs vecteurs d'attaque.
- Bonne maîtrise du framework MITRE ATT&CK et de l'émulation d'adversaires.
- Développement et scripting : Python, PowerShell, C / C#, notions de Go ou Rust appréciées.
- Bonne compréhension des mécanismes de détection (SIEM, EDR) pour mieux les contourner et conseiller la défense.

Ce qui fera la différence

- Contributions à des outils open source, publications, CVE ou participation à des CTF.
- Expérience d'exercices Purple Team ou d'émulation d'adversaires (TIBER-EU, CBEST ou équivalent).

Certifications appréciées

CRTO / CRTL (Certified Red Team Operator / Lead), OSEP, OSCP, CRTE, CRTP, GXPN, eCPTX).

Qualités personnelles

- Créativité, persévérance et capacité à penser comme un attaquant.
- Éthique irréprochable et strict respect des règles d'engagement.
- Discrétion et sens de la confidentialité.
- Excellente capacité rédactionnelle et aisance à l'oral.
- Esprit d'équipe et goût du partage avec les équipes de défense.

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 03/11/2026. Candidatures reçues jusqu'au 03/12/2026 inclus. Référence RE - RED - TM- 2026.