



AVIS DE RECRUTEMENT

Type de contrat: **CDD 02 ans**

Disponibilité immédiate

ANALYSTE SECURITE OFFENSIVE (H/F)	
Employeur	Agence des Systèmes d'Information et du Numérique (ASIN)
Entité de rattachement	Pôle Sécurité Numérique / Département Cybersécurité
Relation fonctionnelle	Équipes du bjCSIRT
Lieu d'affectation	Cotonou
Candidature	Postuler en ligne sur le portail national des services publics https://service-public.bj/public/services/service/PS01334 en joignant un CV actualisé, une lettre de motivation, la copie des diplômes et une pièce d'identité au plus tard le 19 octobre 2026 à 20h00 (heure de Cotonou).
INFORMATIONS GENERALES	
La République du Bénin a lancé un programme ambitieux de développement de l'économie numérique visant à positionner le pays comme la référence en matière de plateforme de services numériques en Afrique de l'Ouest et de faire des Technologies de l'Information et de la Communication le principal levier de son développement socio-économique. L'Agence des Systèmes d'Information et du Numérique (ASIN) est une agence gouvernementale sous la double tutelle du Ministère de l'Économie et des Finances et du Ministère de la Transformation Digitale et de l'Innovation, chargée d'assurer la mise en œuvre opérationnelle des programmes et projets entrant dans le cadre des stratégies de développement des services et systèmes d'information sécurisés au Bénin. À ce titre, elle conçoit, déploie et maintient les plateformes nationales de services publics numériques, les référentiels et les briques d'interopérabilité qui permettent aux administrations d'échanger leurs données et de servir les usagers de manière simple, sécurisée et continue. Le bjCSIRT, un service du Département Cybersécurité, est l'équipe nationale de réponse aux incidents de sécurité informatique. Il assure la veille sur les menaces, la détection et la qualification des incidents, la réponse et la coordination nationale en cas de crise cyber, la gestion des vulnérabilités, la production de renseignement sur la menace, l'accompagnement technique des administrations publiques et des opérateurs d'importance vitale, ainsi que la coopération avec les réseaux de confiance régionaux et internationaux.	
OBJECTIFS ET PORTEE DE LA MISSION DU POSTE	
Évaluer par la voie offensive le niveau de sécurité réel des systèmes d'information des entités relevant de la base d'utilisateurs du bjCSIRT: tests d'intrusion, audits techniques, émulation d'adversaires et exercices purple team, avec pour finalité l'amélioration mesurable de la posture défensive nationale.	
PRINCIPALES RESPONSABILITES	



- Conduire les tests d'intrusion (externe, interne, applicatif web, API, mobile, Wi-Fi, Active Directory, cloud) sur les périmètres autorisés, exclusivement selon des règles d'engagement formalisées
- Réaliser les audits de configuration, d'architecture et les revues de code de sécurité sur les plateformes et eServices nationaux
- Conduire des opérations d'émulation d'adversaires et de Red Team fondées sur les modes opératoires réellement observés (MITRE ATT&CK)
- Animer les exercices purple team avec les équipes SOC : rejeu contrôlé de techniques, mesure de la couverture de détection, amélioration conjointe des règles
- Développer et maintenir l'outillage offensif interne : scripts, charges de test, infrastructure de commande et contrôle dédiée aux exercices
- Conduire les campagnes autorisées d'hameçonnage simulé et d'évaluation de la sensibilisation, dans le respect du cadre éthique et réglementaire
- Documenter chaque action réalisée (horodatage, machine source, commande, effet) afin de permettre la corrélation avec les journaux des entités testées
- Rédiger les rapports d'évaluation : constats étayés par des preuves, scoring, chemins d'attaque, impact métier et plan de remédiation priorisé ; restituer aux équipes techniques et aux décideurs
- Réaliser les contre-tests après remédiation et attester du traitement effectif des constats;
- Contribuer à l'évaluation de la sécurité des projets nationaux en amont de leur mise en production, et alimenter les référentiels de durcissement de l'ASIN
- Transférer les enseignements offensifs aux équipes défensives: indicateurs, techniques, angles morts de détection et recommandations d'instrumentation.

FORMATION, EXPÉRIENCE, COMPETENCES ET LANGUES

FORMATION

Être titulaire d'un diplôme de niveau BAC + 3 à BAC + 5 en informatique, cybersécurité ou toute autre formation de niveau équivalent.

EXPERIENCE ET CONNAISSANCES

- Avoir au moins trois (03) ans d'expérience professionnelle en tests d'intrusion, audit technique de sécurité ou opérations offensives
- Justifier de la conduite autonome d'au moins une (1) mission de test d'intrusion documentées
- Justifier d'une expérience de rédaction et de restitution de rapports auprès d'équipes techniques et de décideurs
- Une expérience d'exercices purple team ou de collaboration structurée avec une équipe de détection serait un atout majeur.



- Une contribution reconnue à la communauté (CVE, publications, outils, plateformes de bug bounty, plateformes d'entraînement, programmes de divulgation) serait un atout.

LANGUES

- Une excellente maîtrise de la langue française aussi bien à l'oral qu'à l'écrit est exigée;
- Une bonne maîtrise de l'anglais technique est exigée (documentation, advisories, échanges avec les réseaux de confiance internationaux).

COMPETENCES

- Maîtrise confirmée des domaines et technologies suivants:
 - Méthodologies: PTES, OWASP WSTG et ASVS, OSSTMM, MITRE ATT&CK, TIBER-like adversary emulation
 - Applicatif: OWASP Top 10, Burp Suite Pro, tests d 'API REST et GraphQL, OAuth2/OIDC, SAML, désérialisation, SSRF, injections, logique métier, mobile (Android/iOS)
 - Active Directory: Cartographie des chemins d'attaque (BloodHound), Impacket, relais NTLM, délégations Kerberos, abus d'ADCS, Group Policy, persistance de domaine
 - Systèmes et réseau: Escalade de privilèges Windows et Linux, pivotement, tunneling, sécurité réseau et contournement de segmentation, Wi-Fi
 - Post-exploitation: Frameworks C2 (Sliver, Havoc, Cobalt Strike), développement de charges, contournement des mécanismes de protection dans un cadre de test autorisé
 - Cloud et conteneurs: Entra ID / Microsoft 365, AWS, évacion de conteneur, sécurité Kubernetes
 - Développement: Python, PowerShell, Bash, Go ou C# pour l'outillage offensif
- Certifications appréciées: avoir l'une des certifications suivantes est un atout: CEH, OSCP, OSEP, OSWE, CRT0, CRTP, PNPT, GIAC GPEN/GXPN ou équivalente.
- Avoir participé au Hackerlab serait un atout.

ETHIQUE, MANAGEMENT ET LEADERSHIP

- Rigueur, esprit de synthèse et d'analyse
- Capacité à travailler de manière autonome et sous pression, y compris en situation de crise
- Capacité d'écoute, communication orale et écrite, capacité à vulgariser un sujet technique auprès de non-spécialistes
- Capacité à gérer les priorités et à répondre aux changements de priorités
- Esprit d'équipe, culture du partage d'information et de la capitalisation
- Sens aigu de l'éthique, de la transparence, de l'intégrité et de la discrétion professionnelle
- Respect strict de la confidentialité des informations traitées, du protocole TLP (Traffic Light Protocol) et des engagements de non-divulgation
- Respect de la réglementation en vigueur en matière de protection des données à caractère personnel et de confidentialité des données publiques.



USAGE RESPONSABLE DE L'INTELLIGENCE ARTIFICIELLE

- N'utiliser que les outils d'IA explicitement autorisés par l'ASIN et dans les conditions définies
- Ne soumettre aucune donnée d'incident, donnée à caractère personnel, preuve numérique ou information classifiée à un service d'IA externe non autorisé
- Soumettre à revue humaine toute analyse, tout code ou toute règle de détection produits avec l'assistance de l'IA, et en assumer la responsabilité technique
- Tracer l'usage de l'IA dans les travaux d'investigation et ne jamais présenter une sortie de modèle comme un fait observé.

CADRE LÉGAL ET RÈGLES D'ENGAGEMENT

- Aucune action offensive ne peut être engagée sans mandat écrit préalable définissant le périmètre, les adresses et systèmes concernés, les fenêtres d'intervention, les actions interdites et les points de contact d'urgence
- Interdiction absolue de toute action hors périmètre, de toute exfiltration de données réelles au-delà de la preuve minimale nécessaire, et de toute action susceptible de dégrader un service en production sans autorisation explicite
- Journalisation exhaustive et horodatée de toutes les actions menées, conservée et communicable à l'entité testée et à la hiérarchie
- Destruction sécurisée des données collectées à l'issue de la mission, selon la procédure de rétention définie
- Notification immédiate à la hiérarchie et à l'entité en cas de découverte d'une compromission préexistante, avec bascule vers le processus de réponse à incident
- Interdiction d'utiliser les compétences, les accès, l'outillage ou les informations obtenus dans le cadre du poste à toute autre fin ; engagement de non-divulgaration permanent, y compris après la fin du contrat
- Poste soumis à une enquête de moralité approfondie et à la production d'un extrait de casier judiciaire.

CONDITIONS PARTICULIÈRES D'EXERCICE

- Interventions possibles en dehors des heures ouvrables en cas de crise ou afin de limiter l'impact sur les services en production, et déplacements sur le territoire national.