



AVIS DE RECRUTEMENT

Type de contrat: **CDD 02 ans**

Disponibilité immédiate

ANALYSTE SOC_NIVEAU 2 (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	
Prendre en charge les incidents escaladés par le niveau 1, conduire les investigations approfondies, concevoir et maintenir les capacités de détection du bjCSIRT, mener des campagnes de chasse aux menaces et automatiser les traitements récurrents, tout en assurant l'encadrement technique des analystes de niveau 1.	
PRINCIPALES RESPONSABILITES	



- Prendre en charge les escalades de niveau 1, conduire l'investigation approfondie et statuer sur la qualification de l'incident (sévérité, périmètre, vecteur initial, impact)
- Reconstituer la chronologie de l'attaque à partir des journaux, de la télémétrie endpoint et réseau, et documenter la cartographie des techniques adverses selon MITRE ATT&CK
- Concevoir, tester, déployer et maintenir les règles de détection (Sigma, règles Wazuh, requêtes Elastic, SPL, YARA, Suricata) selon une approche detection-as-code versionnée
- Mesurer et améliorer la qualité de la détection : taux de faux positifs, couverture ATT&CK, délai de détection, non-régression après modification
- Conduire des campagnes de chasse aux menaces fondées sur des hypothèses, alimentées par le renseignement sur la menace, et documenter méthode, requêtes, résultats et pivots
- Piloter les actions de containment et d'éradication de niveau 2 en coordination avec les équipes techniques des entités concernées
- Concevoir et maintenir les playbooks d'orchestration et d'automatisation : enrichissement automatique, réponse assistée, intégrations API
- Encadrer techniquement les analystes de niveau 1 : revue des tickets, débriefs, transfert de compétences, mise à jour des procédures
- Participer aux exercices purple team et à la validation des détections par émulation d'adversaires
- Produire les rapports d'incident et les recommandations de durcissement à destination des entités bénéficiaires
- Contribuer à l'ingénierie des sources de données : intégration de nouvelles télémétries, normalisation, contrôle de complétude et de qualité des journaux.

FORMATION, EXPÉRIENCE, COMPETENCES ET LANGUES

FORMATION

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

EXPERIENCE ET CONNAISSANCES

- Avoir au minimum trois (03) ans d'expérience professionnelle ;
- Justifier de la conception et de la mise en production de règles de détection sur un SIEM ;
- Justifier d'une expérience d'investigation sur des incidents réels ;
- Justifier d'une expérience de chasse aux menaces fondée sur hypothèses ;
- Une expérience d'encadrement technique ou de mentorat serait un plus.

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 :
- Plateformes : SIEM ; SOAR ; EDR d'entreprise ; requêtes avancées et corrélation multi-sources
- Ingénierie de détection : Sigma, YARA, Suricata, Zeek, ES|QL/EQL, SPL ; detection-as-code (Git, revue par les pairs, CI/CD, tests automatisés)
- Analyse Windows : Journaux d'événements, Sysmon, PowerShell logging, Active Directory et Kerberos (kerberoasting, DCSync, abus de tickets), abus d'outils légitimes (LOLBAS)
- Analyse Linux / conteneurs : auditd, journald, persistance, escalade de privilèges, évocation de conteneur
- Analyse réseau : PCAP, Zeek, empreintes JA3/JA4, détection de balisage C2 (Cobalt Strike, Sliver), tunneling DNS, exfiltration
- Triage de code malveillant : Analyse statique de premier niveau, désobfuscation de scripts, exploitation de sandbox (CAPE), extraction d'indicateurs
- Cloud et identité : Journaux Microsoft 365 / Entra ID, abus d'OAuth, détection sur environnements cloud
- Automatisation : Python, PowerShell, API REST, Shuffle, Cortex XSOAR, conteneurisation Docker
- Référentiels : MITRE ATT&CK et Navigator, MITRE D3FEND, Diamond Model, pyramide de la douleur
- Avoir l'une des Certifications est un atout : CSA, GIAC GCIA ou GCIH, CompTIA CySA+, Blue Team Level 2 (BTL2), eCTHP, Microsoft SC-200, Elastic Certified Analyst, OSIR, OTH ou équivalent.
- 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-divulgaration



- 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.

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.