



AVIS DE RECRUTEMENT

Type de contrat: **CDD 02 ans**

Disponibilité immédiate

SPECIALISTE INVESTIGATION NUMERIQUE ET REPONSE A INCIDENT (DFIR)_(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

Conduire les investigations numériques et piloter techniquement la réponse aux incidents majeurs affectant les entités de la base d'utilisateurs du bjCSIRT, depuis l'acquisition des preuves jusqu'au rétablissement, en garantissant l'intégrité des éléments collectés et la qualité des conclusions produites.

PRINCIPALES RESPONSABILITES

- Piloter techniquement la réponse aux incidents majeurs (rançongiciel, compromission de domaine Active Directory, intrusion persistante, exfiltration de données, compromission de messagerie) sur site et à distance;



- Réaliser les acquisitions forensiques (disque, mémoire vive, journaux, cloud, équipements mobiles) en préservant l'intégrité des preuves: condensats cryptographiques, scellés, procès-verbaux et chaîne de custody documentée;
- Analyser les artefacts système Windows, Linux et macOS: MFT, journal USN, base de registre, prefetch, Amcache/Shimcache, journaux d'événements, shellbags, fichiers LNK, artefacts navigateur, persistance;
- Conduire l'analyse de mémoire vive (Volatility 3, MemProcFS): processus injectés, modules dissimulés, artefacts réseau, extraction de secrets;
- Construire la chronologie consolidée de l'incident et déterminer le vecteur initial, la progression latérale, la persistance et le périmètre réellement compromis;
- Réaliser le triage et l'analyse des codes malveillants collectés: analyse statique et dynamique en environnement isolé, extraction de configuration et d'indicateurs, rédaction de règles YARA;
- Définir et faire exécuter les mesures de containment, d'éradication et de recovery avec les équipes techniques des entités, puis valider la remédiation effective;
- Rédiger les rapports d'investigation techniques et exécutifs, distinguant strictement les faits observés, les hypothèses et les conclusions, et exploitables en contexte judiciaire;
- Assurer l'interface technique avec les autorités compétentes et les services d'enquête dans le respect strict du cadre légal en vigueur;
- Capitaliser sur chaque incident : versement des indicateurs dans MISP, des modes opératoires dans OpenCTI, retour d'expérience, post-mortem et amélioration des règles de détection avec le SOC ;
- Maintenir en condition opérationnelle le laboratoire forensique, les kits d'intervention, les procédures et les gabarits de rapport.

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 minimum trois (03) ans d'expérience professionnelle en cybersécurité ;
- Avoir une expérience d'intervention en environnement contraint (production, crise, délais courts);
- Justifier d'une expérience d'investigation sur des incidents réels;
- Avoir une expérience d'encadrement technique ou de mentorat est 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:



- Outillage forensique: Velociraptor, KAPE, Plaso/log2timeline, Timesketch, Autopsy/Sleuth Kit, FTK Imager, Volatility 3, MemProcFS, Hayabusa/Chainsaw, Eric Zimmerman tools
 - Forensique Windows : Systèmes de fichiers NTFS, artefacts d'exécution, artefacts d'accès, Active Directory, Kerberos, journaux de sécurité, ADCS
 - Forensique Linux et conteneurs: Artefacts système, persistance, journaux, images de conteneurs, environnements Docker et Kubernetes
 - Forensique cloud et messagerie: Microsoft 365 / Entra ID (journaux d'audit unifiés, MailItemsAccessed), AWS CloudTrail, compromission de messagerie professionnelle
 - Analyse de code malveillant : Triage, désobfuscation, sandbox CAPE, YARA, analyse de chargeurs et de balises C2 ; notions de rétro-ingénierie (Ghidra, x64dbg)
 - Normes et méthodes: RFC 3227, ISO/IEC 27037, chaîne de custody, NIST SP 800-61, préservation et intégrité de la preuve
 - Développement: Python pour l'analyse d'artefacts et l'automatisation des collectes; PowerShell; requêtes VQL Velociraptor
 - Rétro-ingénierie
- Avoir l'une des Certifications suivantes est un atout : GIAC GCFA, GCFE, GREM, GNFA, HTB CDSA, OSIR, OSDA, CHFI, 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 PARTICULIERES D'EXERCICE

- Disponibilité pour intervention d'urgence, y compris en dehors des heures ouvrables, et déplacements sur le territoire national ;
- Poste soumis à une enquête de moralité approfondie et à la signature d'un engagement de confidentialité renforcé ;
- Obligation de neutralité et d'objectivité : les conclusions d'investigation ne peuvent être influencées par aucune partie prenante.

