ASIN AGENCE DES SYSTÈMES D'INFORMATION ET DU NUMÉRIQUE
RÉPUBLIQUE DU BÉNIN

01 BP 8088 Cotonou
+ 229 21 31 10 13
contact@asin.bj

AVIS DE RECRUTEMENT

Type de contrat : CDD 02 ans **Disponibilité immédiate**

INGENIEUR(E) SECURITE INFRASTRUCTURE DEFENSIVE (H/F)	
Employeur	Agence des Systèmes d'Information et du Numérique (ASIN)
Direction	Pôle Sécurité Numérique – Service RSSI
Superviseur Hiérarchique	RSSI
Superviseur fonctionnel	Directeur de l'Exploitation et de l'Appui aux Sectoriels (coordination opérationnelle)
Lieu d'affectation	Cotonou
Candidature	Postulez en ligne sur le portail national des services publics https://service-public.bj/public/services/service/PS01334 en joignant CV détaillé, lettre de motivation, références et attestations, au plus tard le 27 novembre 2026 à 18h00 (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 de l'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 tutelle 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. Dans ce contexte, l'ASIN recherche un **profil confirmé**, directement **opérationnel** et capable d'intervenir de manière autonome sur des environnements techniques hétérogènes et à forts enjeux de sécurité.

CONTEXTE ET PORTEE DE LA MISSION DU POSTE

Rattaché(e) au Responsable de la sécurité des systèmes d'information (RSSI) et mis(e) à disposition de la direction de l'Exploitation et de l'Appui aux Sectoriels, l'ingénieur(e) sécurité infrastructure défensive est le/la représentant(e) opérationnel(le) de la fonction RSSI au sein des équipes techniques et garant(e) de la sécurité et de la conformité des infrastructures de l'agence. Sa mission principale est d'assurer l'intégration des exigences de cybersécurité dans les projets d'infrastructure et d'exploitation afin de garantir la mise en œuvre d'environnements sécurisés, durcis et conformes aux standards de sécurité de l'ASIN. Les équipes Infrastructure appliquent les exigences de sécurité ; le/la titulaire les outille, les forme et les contrôle.

PRINCIPALES RESPONSABILITES

Intégration de la sécurité dans les projets d'infrastructure

- Participer aux projets d'évolution des infrastructures, des systèmes et des plateformes techniques.
- Accompagner les équipes Infrastructure dans l'application du principe « Security by Design ».
- Veiller à l'intégration des exigences de cybersécurité lors de la conception et du déploiement des solutions techniques.
- Participer aux comités projets, revues d'architecture et revues techniques afin de garantir la prise en compte des exigences de sécurité dès les phases de conception.

Sécurisation et durcissement des infrastructures

- Définir, maintenir et faire appliquer les standards de durcissement des systèmes, serveurs,

01 BP 8088 Cotonou
+ 229 21 31 10 13
contact@asin.bj

équipements réseau et plateformes cloud.
- Concevoir des modèles de déploiement durcis intégrant par défaut les outils de sécurité, la journalisation et la sauvegarde.
- Réaliser des contrôles de conformité et des audits techniques de sécurité.
- Réaliser des tests d'intrusion et identifier les vulnérabilités sur les infrastructures de l'ASIN.
- Superviser la mise en œuvre des solutions de protection de l'infrastructure.
- Accompagner la mise en œuvre des outils de sécurité (EDR, scanners)
- Accompagner la correction des vulnérabilités et des écarts de sécurité identifiés.

Contrôle de la conformité et gestion des risques
- Vérifier la conformité des infrastructures aux politiques et standards de sécurité de l'ASIN.
- Participer aux analyses de risques sur les projets techniques et les infrastructures sensibles.
- Instruire et suivre les demandes de dérogation aux exigences de sécurité.
- Participer aux validations de sécurité avant la mise en service des infrastructures.
- Évaluer le niveau de sécurité du parc existant et piloter sa mise à niveau par priorité.

Gouvernance et reporting
- Assurer le suivi des risques et écarts de sécurité liés aux infrastructures.
- Assurer un reporting périodique au RSSI sur les projets suivis, les écarts identifiés, les risques résiduels et les plans de remédiation.
- Escalader sans délai au RSSI les écarts critiques.
- Sensibiliser et former les équipes techniques aux bonnes pratiques de sécurisation
- Assurer la remontée des journaux vers la supervision et appuyer le RSSI et le SOC dans le traitement des incidents.
- Contribuer à l'amélioration continue du niveau de sécurité des infrastructures de l'ASIN.

FORMATION, EXPÉRIENCES ET LANGUES

FORMATION
- Être titulaire au minimum d'un BAC+3 en informatique ou cybersécurité.

Certification (ou équivalent, serait un atout) :
- CompTIA Security+, CEH ou OSCP

Connaissances & Compétences
- Maîtrise de l'administration et du durcissement de Windows Server et de Linux.
- Maîtrise de la sécurité Active Directory et connaissance des environnements ESXi et Hyper-V.
- Bonne connaissance des réseaux, des pares-feux, du cloisonnement et des VPN.
- Bonne connaissance des solutions EDR, SIEM, IAM/PAM et des scanners de vulnérabilités.
- Bonne connaissance des techniques de tests d'intrusion sur les infrastructures.
- Maîtrise du Scripting PowerShell, Bash ou Python et pratique d'Ansible ou équivalent.
- Connaissance des guides de durcissement (CIS Benchmarks).
- La connaissance de la PSSIE, de la PPIIC et des environnements cloud 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 à l'oral et à l'écrit est un atout.

EXPERIENCES
- Avoir minimum deux (02) années d'expérience en administration systèmes et réseaux ou en sécurité des infrastructures, dont au moins une (01) en sécurisation d'environnements de production.

01 BP 8088 Cotonou
+ 229 21 31 10 13
contact@asin.bj

ETHIQUE, LEADERSHIP ET MANAGEMENT
▪ Être passionné(e) de la sécurité des technologies de l'information et avoir la volonté d'apprendre. ▪ Être capable de travailler en équipe et sous pression. ▪ Avoir le sens de la communication, être pédagogue, avoir le sens du dialogue et la capacité à convaincre sans lien hiérarchique. ▪ Avoir le sens de la rigueur, de l'autonomie et être force de proposition. ▪ Avoir le sens de la discrétion et un sens élevé de la confidentialité. ▪ Avoir un esprit de synthèse et d'analyse ainsi que la capacité de rédaction de rapports techniques. ▪ Avoir la capacité de respecter les délais et de rendre compte. ▪ Avoir le sens de l'éthique et de l'intégrité dans le traitement de tous les sujets sous sa responsabilité.