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) DevSecOPS (H/F)	
Employeur	Agence des Systèmes d'Information et du Numérique (ASIN)
Direction	Pôle Sécurité Numérique – Service RSSI
Superviseur Hiérarchique	RSSI
Superviseur Fonctionnel	Responsable Equipe Développement de la Direction des Systèmes d'Information et de la Digitalisation
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 numériquevisant 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 l'équipe Développement de la Direction des Systèmes d'Information et de la Digitalisation, l'ingénieur(e) DevSecOps 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 applications développées par les équipes DSID pour le compte du Gouvernement béninois. Sa mission principale est d'assurer l'intégration des exigences de cybersécurité tout au long du cycle de vie des applications de l'ASIN afin de garantir la conception, le développement, les tests et le déploiement d'applications sécurisées, conformes aux standards de sécurité de l'organisation. Les équipes projets appliquent les exigences de sécurité ; le/la titulaire les outille, les forme et les contrôle.

PRINCIPALES RESPONSABILITES

Intégration de la sécurité dans les projets

- Participer aux projets applicatifs dès les phases d'étude, de conception et d'architecture.
- Accompagner les équipes de développement dans l'application du principe « Security by Design ».
- Veiller à la prise en compte des exigences de sécurité dans les spécifications fonctionnelles et 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.
- Encadrer la sécurité des développements confiés à des prestataires.

Sécurisation du cycle de développement

- Définir et mettre en œuvre les pratiques DevSecOps au sein des chaînes CI/CD.

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

- Automatiser les contrôles de sécurité dans les processus de développement et de déploiement.
- Mettre en œuvre les outils d'analyse de code, de détection des vulnérabilités et de contrôle des dépendances logicielles.
- Identifier les vulnérabilités dans les applications et le code source, ainsi que les faiblesses de configuration et de développement.
- Accompagner la correction des vulnérabilités identifiées avant la mise en production.
- Sécuriser la gestion des secrets, des dépendances, de l'authentification et de la journalisation applicative.
- Encadrer l'usage de l'IA dans le développement : règles d'utilisation, revue du code généré, protection des données et des secrets.
- Accompagner la mise en place d'environnements de développement sécurisés.

Contrôle et validation sécurité

- Réaliser ou coordonner les revues de sécurité applicatives.
- Réaliser ou coordonner les tests d'intrusion applicatifs avant les mises en production majeures.
- Évaluer les risques liés aux nouvelles applications ou aux évolutions majeures.
- Vérifier la conformité des applications avec les politiques et standards de sécurité de l'ASIN.
- Participer aux validations de sécurité préalables aux mises en production.
- Veiller au déploiement des applications sur des environnements durcis.
- Tenir l'inventaire de sécurité des applications, évaluer celles en production et suivre leur remise à niveau.

Gouvernance et reporting

- Assurer le suivi des risques et écarts de sécurité identifiés sur les projets applicatifs.
- 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, former et accompagner les équipes de développement aux bonnes pratiques de cybersécurité.
- Appuyer le RSSI et le SOC dans le traitement des incidents de sécurité applicatifs.
- Contribuer à l'amélioration continue des processus de développement sécurisé.

FORMATION, EXPÉRIENCES ET LANGUES

FORMATION

- Être titulaire au minimum d'un BAC+3 en informatique ou cybersécurité (BAC+5 apprécié).

Certification (ou équivalent, serait un atout) :

- Certified DevSecOps Professional (CDP) ou CSSLP
- GIAC GWEB ou OSWE

Connaissances & Compétences

- Bonne pratique du développement (Python, Java ou JavaScript/TypeScript) et de Bash.
- Maîtrise de Git et des pipelines CI/CD GitLab ou équivalent.
- Maîtrise de l'audit de code, des tests de sécurité applicative et des outils SAST, SCA et DAST.
- Bonne connaissance des risques du développement assisté par IA et de leur encadrement.
- Maîtrise des référentiels OWASP (Top 10 Web, API et LLM, ASVS).
- Bonne connaissance de la sécurité des API et des applications mobiles.
- Bonne connaissance de Docker, de Kubernetes et de l'IaC (Terraform, Ansible).
- Bonne connaissance d'OAuth 2.0, d'OpenID Connect, du SSO et de la gestion des secrets.
- Connaissance du durcissement Linux et conteneurs et des environnements cloud.
- La connaissance de la PSSIE et de la PPIIC 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.

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

EXPERIENCES

- Avoir minimum trois (02) années d'expérience en développement, DevOps ou sécurité applicative, dont au moins deux (01) en sécurité applicative ou DevSecOps.

ETHIQUE, MANAGEMENT ET LEADERSHIP

- 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.

USAGE RESPONSABLE DE L'INTELLIGENCE ARTIFICIELLE

- Recourir aux outils d'IA uniquement parmi ceux autorisés par l'Agence et selon les règles d'usage en vigueur ;
- Assumer l'entière responsabilité du code livré : le recours à l'IA ne dispense ni de la compréhension du code, ni des tests, ni du respect des standards ;
- Faire preuve d'esprit critique face aux productions de l'IA (erreurs, failles de sécurité, dépendances obsolètes, code non conforme à l'architecture) ;
- Signaler en revue les portions de code produites avec l'assistance de l'IA lorsque la charte interne l'exige ;
- Respecter la réglementation en vigueur en matière de protection des données à caractère personnel et de confidentialité des données publiques.