APPEL A CANDIDATURE
D'UN SPECIALISTE DE CYBER SECURITE

La Guinéenne de Monétique (GuiM) est un Groupement d'intérêt économique qui regroupe la Banque Centrale de la République de Guinée et l'ensemble des établissements de crédit, ayant son siège à Conakry, République de Guinée.

Elle a pour objet, la mise en place, la gestion et l'exploitation du Switch monétique et digital.

Dans ce cadre, la GuiM recrute :

- **Spécialiste de Cyber Sécurité**.

Conditions Générales :

Pour être éligible, les candidats doivent remplir les conditions suivantes :

- Être disponible immédiatement,
- Être âgés de 35 ans au plus,
- Avoir la nationalité Guinéenne.

Le candidat retenu sera engagé sous un Contrat à Durée Indéterminé (CDI), assorti d'une période d'essai de trois (3) mois.

Les dossiers de candidatures (lettre de motivation CV, diplôme et/ou attestations, attestations de travail, prétentions salariales, etc.…) devront parvenir au siège de la Guinéenne de Monétique au plus tard le **28 février 2025 à 12 h 00 TU.**

Seuls les candidats présélectionnés seront contactés.

Pour les envois par mail, toutes les pièces demandées, doivent être scannées puis transformées en PDF. Les originaux vous seront réclamés lors de l'entretien.

Les candidatures peuvent être transmises par voie électronique à : **recrutement@guim-gn.com**

TERMES DE REFERENCE DU POSTE

Référence	**SCS**
Poste proposé	Spécialiste de Cyber Sécurité
Contrat	CDI avec période d'essai de trois (3) mois.
Employeur	Guinéenne de Monétique (GuiM)
Position	D1
Localisation	Poste basé à Conakry, République de Guinée

MISSION PERMANENTE DU POSTE

CONDITIONS GENERALES :

Missions	- Responsable de la définition de la politique de sécurité du système d'information le cas échéant (prévention, protection, défense, résilience/remédiation) et de son application.

	Il assure son rôle de conseil, d'assistance, d'information, de formation et d'alerte, en particulier auprès des directeurs métiers, DG ; - Il préconise, voire prend, toute décision d'intervention sur les systèmes d'information et télécoms de son périmètre, en cas d'attaques potentielles ou avérées.
Description des activités principales	- Analyser et évaluer les risques associés à la sécurité du SI ; - Définir et faire évoluer la politique de sécurité des systèmes d'information de l'entreprise (PSSI) ; - Etablir un plan de prévention des risques informatiques et un plan de continuité d'activité (PCA) ; - Participer à la définition at au contrôle de la gestion des habilitations ; - Mettre en place les méthodes et outils de sécurité adaptés, et accompagner leur implémentation auprès des utilisateurs ; - Assurer une veille technologique et règlementaire pour garantir la sécurité logique et physique du SI dans son ensemble ; - Responsabiliser ses équipes en leur définissant des objectifs clairs, en les challengeant et en validant les plans d'actions proposés par ces derniers ; - Identifier et traiter les flux d'évènements de sécurité suspects ou malveillants affectant les actifs et les périmètres supervisés du système d'information, de diligenter la réponse aux incidents de sécurité, réglages des infractions, intégration et support sur les solutions de sécurité ; - Procéder aux scans des vulnérabilités/tests d'instruction et à la remédiation ; - Veiller à la supervision, l'exploitation des indicateurs de disponibilité des éléments critiques de l'infrastructure IT sur les différents sites ; - Suivre les incidents majeurs IT pour permettre la mise en place de dispositifs sécurisés de prévention et de correction ; - Contribuer au maintien de toute norme sécuritaire applicable et apporter les preuves de conformité aux exigences de la norme ; - Fournir les preuves nécessaires d'alignement sur les exigences des normes de sécurité ; - Développer les compétences des collaborateurs sous sa responsabilité ; - Veiller à la rédaction et mise à jour des procédures ; - Veiller au respect des procédures, normes et standards de travail de la GuiM ; - Veiller à la mise à jour des fiches de postes de son périmètre.
Relations intérieures et extérieures	- Ensemble du personnel ; - Membre de la GuiM, Clients, consultants, prestataires, partenaires (nationaux et étrangers), commissaires aux comptes, organisations sociales, assurances, structures de santé.
Qualifications requises	**Formation académique** Avoir un Bac+5 Ingénieur, informatique. Une certification en sécurité technique IT serait un atout. **Expériences professionnelles pertinentes** - Avoir au moins 5 ans d''expérience professionnelle dans un poste similaire ou dans un domaine équivalent de la sécurité informatique ; - Avoir des certifications de types CISA, CISM, CISSP ;

	- Bonne connaissance des principaux prestataires de la cybersécurité ; - Bonne connaissance des normes et procédures classique en termes de sécurité (antivirus, firewall, cryptographie, etc.) ; - Bonne connaissance de réseau et système ; - Bonne connaissance des outils d'évaluation et maîtrise des risques (EBIOS, MEHARI, etc.) ; - Bonne connaissance des normes et standards de sécurité (ISO27001, PCI-DSS, NIST CSF, CIS20, etc.) ; - Bonne connaissance des méthodologies d'audit (e g. OWASP, OSSTMM, etc.) ; - Connaissance juridique de base et de droit informatique. **Compétences et qualités requises** - Capacité de motivation et de management d'équipe ; - Pilotage par objectifs ; - Gestion du stress ; - Réactivité, relationnel, communication ; - Ethique, sens et respect de la confidentialité ; - Planification et organisation du travail ; - Aisance relationnelle ; - Ecoute, compréhension des autres, Esprit de médiateur ; - Esprit d'initiative ; - La maîtrise de l'Anglais est un atout.

NB : le candidat doit mentionner l'intitulé du poste à pourvoir dans l'objet de son message comme suit : **SPECIALISTE DE CYBER SECURITE.**

La Direction Générale