FICHE DE POSTE

Titre poste	**Auditeur de sécurité des systèmes d'information**
Sup H. direct (1):	**Directeur Technique - DT**
Sup H. direct (2):	**Directeur Général - DG**

Cyber Defense Africa

Issue d'un partenariat stratégique entre l'Etat Togolais et la société Asseco Data Systems S.A. (ADS) représenté dans plus de 50 pays, Cyber Defense Africa S.A.S. (CDA) est la société de service en cybersécurité mandatée par l'Agence Nationale de la Cybersécurité (ANCy) pour assurer la sécurisation des systèmes d'information au Togo et par-delà ses frontières.
Nous fournissons des services de Security Operations Center (SOC) ainsi que de Computer Security Incident Response Team (CSIRT). Nous accompagnons les administrations et entreprises privées dans la sécurisation de leurs infrastructures, la protection des applications et la confidentialité de leurs données avec une large gamme de services allant du conseil à la mise en œuvre technique.

Cette structure soutient la stratégie de faire du Togo un leader régional en cybersécurité tout en créant un écosystème local d'emplois qualifiés avec un pôle de compétences spécialisées en cybersécurité au Togo capable de satisfaire la demande des entreprises togolaises et africaines.

Résumé du poste

Cyber Defense Africa recherche un Auditeur de Sécurité des Systèmes d'Information pour rejoindre son équipe.
L'auditeur de la sécurité des systèmes d'information sera responsable des questionnaires, de l'évaluation, des audits de contrôle du système d'information des clients de CDA. Il est chargé des rapports sur la posture sécurité et de la normalisation des politiques et des procédures.

Responsabilités du poste

- Développer des méthodes pour surveiller et mesurer les risques, la conformité et les efforts d'assurance ;
- Contrôler et évaluer la conformité d'un système aux exigences de sécurité, de résilience et de fiabilité des technologies de l'information (TI) ;
- Effectuer la validation par étapes, en comparant les résultats réels aux résultats attendus et en analysant les différences pour identifier l'impact et les risques ;
- Fournir des recommandations sur les améliorations et les mises à niveau possibles ;
- Examiner ou effectuer des audits de programmes et de projets de technologie de l'information (TI) ;
- Développer et mettre en œuvre des processus d'audit indépendant de la sécurité des TI pour les logiciels d'application/réseaux/systèmes ;
- Concevoir des procédures d'audit pour évaluer les contrôles de sécurité des TI et atteindre les objectifs d'audit ;
- Suivre les questions ouvertes nécessitant une résolution conformément aux contrôles de sécurité des TI et aux exigences du client ;
- Créer des rapports d'audit pour communiquer efficacement si les systèmes informatiques sont conformes aux politiques appropriées du cabinet, aux normes de l'industrie, aux réglementations gouvernementales et aux exigences contractuelles ;

- Participer périodiquement à d'autres projets relatifs aux risques informatiques.

Conditions requises

- Connaissance des concepts et des protocoles de réseaux informatiques, ainsi que des méthodologies de sécurité des réseaux ;
- Connaissance des processus de gestion des risques (par exemple, les méthodes d'évaluation et d'atténuation des risques) ;
- Connaissance des lois, des règlements, des politiques et de l'éthique en matière de sécurité informatique ;
- Connaissance des normes de sécurité des données relatives aux informations personnellement identifiables (PII) ;
- Connaissance des normes de sécurité des données relatives aux informations médicales personnelles (PHI) ;
- Connaissance de la norme ISO 27001 et du National Institute of Standards and Technology (NIST) ;
- Connaissance technique de plusieurs framework de conformité, SOC 2, PCI DSS ;
- Fortes connaissances en matière de pare-feu, VPN, prévention des pertes de données, IDS/IPS, Web-Proxy et audits de sécurité.

Formation académique & expérience requises

- Master en informatique, en ingénierie et/ou dans un domaine connexe. Un diplôme supérieur pertinent est un plus ;
- 3 à 5 ans d'expérience dans l'exécution de fonctions d'audit de la sécurité informatique ;
- Certifications souhaitées : Auditeur de systèmes d'information certifié (CISA), Certified Information Security Manager (CISM), Certified Information Systems Security Professional (CISSP) ;
- Bonne connaissance de l'anglais.

Aptitudes personnelles

- Excellentes aptitudes à la démonstration et à la présentation ;
- Capacité à travailler sous pression, à être multitâche, à se concentrer et à obtenir des résultats ;
- Bonnes capacités de communication et esprit d'équipe exceptionnel.