FICHE DE POSTE

Titre poste	**Analyste cybersécurité Niveau 1**
Supérieur hiérarchique direct (1):	**SOC Manager**
Supérieur hiérarchique direct (2):	**Directeur Technique - DT**

Cyber Defense Africa

Issue d'un partenariat stratégique entre l'Etat Togolais et la société Asseco Data Systems S.A. (ADS) représentée 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 visant à 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 une personne talentueuse et enthousiaste pour rejoindre son équipe en tant qu'analyste cybersécurité.
L'analyste Niveau 1 sera chargé des activités de réponse aux incidents, en tirant parti de plusieurs technologies de sécurité, en guidant et en dirigeant les clients dans le traitement des incidents de sécurité et en examinant les systèmes informatiques et de sécurité à l'aide des méthodes d'investigation numérique les plus efficaces pour détecter, valider et atténuer les incidents liés à la sécurité informatique.

Responsabilités du poste

- Surveiller les outils d'alerte et traiter également les incidents remontés par les clients ;
- Trier les alertes au fur et à mesure qu'elles arrivent en menant les actions appropriées ;
- Répondre aux alertes communes de manière cohérente et reproductible à partir de plusieurs sources d'alerte, en veillant à recueillir le contexte et les informations nécessaires ;
- Assurer la remontée des menaces inconnues vers les analystes de niveau 2;
- Mener des tests de vulnérabilité ;
- Développer et maintenir la documentation spécifique aux incidents ;

- Soutenir les activités du SOC / CERT selon les besoins.

Conditions requises

- Connaissance de l'infrastructure réseau, des principes de sécurité de l'information ;
- Capacité à lire et à comprendre les données du système, y compris les journaux des événements de sécurité, les journaux du système, les journaux des applications et les journaux des équipements réseau ;
- Compréhension des technologies d'entreprise, notamment des systèmes d'exploitation, des bases de données et des applications Web ;
- Posséder une compréhension des technologies et des outils de sécurité ;
- Démontrer des capacités d'analyse du trafic réseau afin d'identifier les phases d'attaques.

Formation académique & expérience

- License en informatique, en ingénierie, en systèmes d'information et/ou dans un domaine connexe ou expérience équivalente ;
- Les certifications en gestion d'incident et/ou cybersécurité (CIH, CSA, Security+, CyberOps, CEH) seraient un avantage ;
- Bonne connaissance de l'anglais.

Aptitudes personnelles

- Très bonnes aptitudes à la communication, fortes capacités d'analyse et de résolution de problèmes ;
- Personne motivée, autogérée, capable de faire preuve de compétences analytiques exceptionnelles et de travailler de manière professionnelle avec ses pairs et les clients, même sous pression ;
- Capacité à travailler sans supervision, dans des situations potentiellement stressantes, avec peu ou pas de supervision immédiate ;
- Solides compétences écrites et verbales ;
- Solides compétences interpersonnelles avec la capacité de bien collaborer avec les autres.