FICHE DE POSTE

Titre poste	**Analyste cybersécurité SOC / CERT Niveau 1**
Sup H. direct (1):	**SOC Manager**
Sup H. direct (2):	**Directeur Technique**

Cyber Defense Africa

Issue d'un partenariat stratégique entre l'État 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 une personne talentueuse et enthousiaste pour rejoindre notre 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

Les analystes de premier niveau constituent la première ligne de réponse aux incidents. L'équipe fonctionne 24h/24, 7j/7 et est la première ligne de traitement des événements / incidents de cybersécurité. L'analyste Niveau 1 effectue une surveillance des événements de cybersécurité en temps réel et détermine l'urgence des alertes ainsi que celles nécessitant une escalade au niveau 2. Sa tâche principale est le triage qui comprend :

- La vérification – Trouver la preuve technique que l'événement est un incident de sécurité, une erreur réseau ou de périphérique ou simplement une fausse alarme (false positive) ;
- La classification – Attribuer un type, une catégorie et une priorité d'action particulière liée à l'événement, sur la base d'une évaluation préliminaire de l'impact négatif potentiel sur la confidentialité, la disponibilité et / ou l'intégrité des informations ;
- Détermination de l'ampleur de l'attaque – Identifier et caractériser l'impact négatif de l'incident en se basant sur les systèmes informatiques affectés par l'événement ou l'incident. Évaluer la taille et l'étendue de l'incident en analysant les parties affectées de l'infrastructure, des services, des données et des business

units ;
- Le traitement – Suivre les procédures existantes pour traiter l'incident jusqu'à sa clôture ou l'escalade vers le niveau 2 ;
- La documentation – documenter toutes les mesures prises pour résoudre l'incident, à savoir les informations critiques collectées, les analyses effectuées, les mesures correctives et corrections appliquées.

Il aura aussi à :
- Mener des tests de vulnérabilité ;
- 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.

Formations & expériences

- Connaissances en informatique, en ingénierie, en systèmes d'information ou toutes expériences équivalentes ;
- Les certifications en gestion d'incident et/ou cybersécurité (CIH, CSA, Security+, CyberOps, CEH) seraient un avantage ;
- Bonne connaissance de l'anglais.

Aptitudes personnelles

- Passionné de cybersécurité, autodidacte, avec une forte capacité d'adaptation ;
- 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 ;
- Suivi et respect des procédures ;
- Aptitude à travailler en shift.

Si vous désirez nous rejoindre, envoyer votre CV à : jobs@cda.tg