FICHE DE POSTE

Titre poste	**Spécialiste de la réponse aux incidents et des investigations numériques**
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 une personne talentueuse et enthousiaste pour rejoindre notre équipe en tant que spécialiste de la réponse aux incidents et des investigations numériques. Si vous avez une forte connaissance et un intérêt pour la réponse aux incidents et/ou aux investigations numériques, ce poste est le bon pour vous. Le spécialiste de la réponse aux incidents et des enquêtes numériques sera chargé des activités de réponse aux incidents sur site et hors site et des engagements avec les clients, 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

- Diriger les missions de réponse aux incidents jusqu'à ce que toutes les menaces soient éliminées ;
- Développer des plans de réponse aux incidents personnalisés liés à des environnements spécifiques et aux situations des clients ;
- Examiner et analyser les journaux/données d'une grande variété de technologies de sécurité, telles que les antivirus, les IDS/IPS, les pares-feux, les commutateurs, les VPN et d'autres sources de données sur les

menaces de sécurité ;

- Effectuer des investigations numériques sur différents artefacts, notamment la mémoire vive, les captures de paquets, les journaux et les images de disque ;
- Réaliser la rétro-ingénierie de logiciels malveillants et développer des signatures et des indicateurs de compromission.

Conditions requises

- Une bonne connaissance des meilleures pratiques en matière de sécurité informatique, des types d'attaque courants et des méthodes de détection/prévention ;
- Une expérience démontrable dans l'analyse et l'interprétation des journaux de système, de sécurité et d'application ;
- Expérience démontrable dans l'utilisation des outils, techniques et concepts de Digital Forensics, y compris la création et l'utilisation d'outils et de scripts personnalisés ;
- Démontrer une expérience dans le traitement des missions de réponse aux incidents en se basant sur une méthodologie standard telle que SANS Incident Response ou similaire;
- Solide formation ou expérience équivalente dans les domaines suivants : Analyse des menaces et des événements de sécurité, opérations ou ingénierie de sécurité réseau, rétro-ingénierie, analyse des logiciels malveillants, criminalistique Windows/Linux/OSX, tests de pénétration, administration Active Directory et Azure ;
- Expérience en tant qu'analyste principal ou expérience équivalente consistant à guider, à encadrer et à enseigner à d'autres analystes/professionnels de la sécurité comment gérer les incidents de sécurité ;
- Expérience significative dans le domaine de la cybersécurité, des meilleures pratiques en matière de développement de logiciels, connaissance de la revue de code et des tests de pénétration ;
- Rétro-ingénierie statique et analyse de logiciels malveillants écrits dans différents langages (X86/X64/C/C#, Go, etc.), élaboration de signatures et de règles Yara/Snort/Sigma ;
- Connaissance approfondie des tactiques de l'équipe rouge et capacité à trouver les traces de l'adversaire à l'échelle de l'entreprise.

Formation académique & expérience requises

- Master en informatique, en ingénierie, en systèmes d'information et/ou dans un domaine connexe. Un diplôme supérieur pertinent est un plus.
- Minimum 3 ans d'expérience en sécurité de l'information, dans des domaines tels que les opérations de sécurité, la détection des intrusions, l'analyse des incidents, le traitement des incidents, l'analyse des journaux, l'analyse des logiciels malveillants, la rétro-ingénierie ou la détection des menaces.
- Les certifications CISSP, GCIA, GCIH, CHFI, GCFA, GCFE, GREM, OSCP 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