Spécialiste - Sécurité de l'information

Cotonou, Bénin
À propos de nous

Africa Valley SARL (https://www.africavalley.ca), entreprise béninoise en développement rapide recherche dans le cadre de l'expansion de ses activités avec des partenaires étrangers des ressources spécialisées en technologie de l'information (TI).
Sous la responsabilité du directeur général, le spécialiste sécurité de l'information aura à intervenir à distance sur les plateformes technologiques de partenaires et de clients pour le compte de l'entreprise Africa Valley SARL.
Il agit en tant que spécialiste en sécurité dans des mandats d'envergures; accomplit ses fonctions, entre autres, en mettant en place des outils et/ou des méthodes assurant le maintien et la saine gestion de cette spécialisation chez le client.

Plus précisément sans être limitatif, il aura à effectuer les activités suivantes.

Activités générales attendues :

- Agir comme spécialiste dans l'installation, la configuration et la maintenance de solution de type SIEM;
- Agir comme spécialiste dans l'installation, la configuration et la maintenance de solution de type IDS/IPS;
- Agir comme spécialiste dans l'installation, la configuration et la maintenance de solution d'analyse et de gestion de vulnérabilités;
- Agir comme spécialiste dans l'installation, la configuration et la maintenance de solution de type WAF (Web Application Firewall);
- Agir comme spécialiste dans l'installation, la configuration, la maintenance et la gestion des règles de pare-feux de nouvelles générations;
- Agir comme spécialiste dans l'installation, la configuration et la gestion de consoles Antivirus;
- Agir comme spécialiste dans l'identification et le traitement des menaces;
- Intervenir dans la conception ou la révision d'architecture de sécurité devant intégrer des solutions de sécurité qu'il devra proposer;
- Encadrer (« coacher »), au besoin, les intervenants ciblés pour assurer le transfert des connaissances techniques requises;
- Réaliser la documentation de procédures et de configuration pour assurer le respect des normes, des spécifications pertinentes et de qualité requises;

- Préparer la documentation et les supports requis pour produire ou alimenter des tableaux de bord de sécurité;

- Animer des programmes de formation à l'interne et auprès des clients;

- Assurer toute autre tâche connexe à la demande du directeur général.

Qualifications requises

Générale

- Diplôme d'études universitaire avec spécialisation en technologie de l'information (TI), informatique, Réseaux ou l'équivalent;
- Niveau d'études Bac +5, Bac +3 avec au moins 5 années d'expérience (souhaitable)
- Certification de sécurité CISSP, CEH, OSCP, CSSLP, GCIH, ECSA, GREM, CPEN ou équivalent (un atout);
- Capacité à interagir avec des représentants de milieux différents;
- Excellent sens de l'organisation, d'esprit d'analyse, d'initiative et de synthèse;
- Rigueur et excellente attitude;
- Capacité à être autonome rapidement dans un environnement changeant et à faire preuve d'innovation;
- Capacité à rédiger des documents de façon claire et structurée;
- Capacité à travailler en équipe et à agir comme « coach »;
- Bilinguisme français et anglais, parlé et écrit.

Technique

- Expérience pratique dans la manipulation de produits type SIEM, SOAR, IDS/IPS, etc.
- Expérience pratique dans la gestion de SOC;
- Expérience pratique dans la manipulation d'outils de type EDR, MDR, xDR;
- Expérience pratique dans la corrélation de données non structurées provenant de divers types de journaux et de flux d'évènements (pare-feux, IPS, IDS, EDR, serveurs, routeurs, etc.);
- Expérience pratique dans la programmation de script en powershell et/ou en python ou équivalent;
- Expérience dans la gestion d'incidents de sécurité;
- Excellente connaissance des technologies Web;
- Excellente connaissance des systèmes Linux ou Unix;
- Excellente connaissance des concepts Zero Trust, threat Intelligence et de la sécurité en profondeur;
- Excellente connaissance des concepts d'architecture de sécurité;

- Excellente capacité à rédiger de la documentation fonctionnelle et technique;
- Bonne Connaissance des outils type Elastisearch, Sentinel, QRadar, Rapid7, LogRythm, Tenable, SolarWinds Security EventLog Analyzer, Splunk, etc.;
- Bonne connaissance des environnement MS AD 2008 ou plus, Azure AD;
- Connaissance de solutions d'authentification multi-facteurs, solution de PAM;
- Connaissance des concepts de durcissements (Hardening)
- Connaissance de la sécurité des environnements infonuagiques (AWS, Azure, Google, etc.);
- Connaissance du framework MITRE ATT&CK et d'outils de tests d'intrusion.

Informations complémentaires:

- Poste permanent à plein temps;
- Rémunération attractive;
- Bonus mensuel et annuel;
- Paiement par l'employeur de formation(s) et/ou certification(s) en lien avec le poste;
- Candidature à adresser avant le 17 avril 2023 à contact@africavalley.ca
- **Horaire de travail de 12h à 21h**