Sarl au capital de FCFA 1.000.000
N°089-SE-OECCA BÉNIN
IFU: 320 181 041 7815
RCCM RB /COT/ 18 B 22394
Compte BOA N°0061 6850 0001

Tél: +229 67 86 62 62
01 BP 345 Cotonou
Îlot: 650 Maison DJOSSOU,
Qtier Jericho Nord, Cotonou-Benin
e-Mail: cabinetsecca.sarl@gmail.com

Le cabinet SECCA SARL recrute pour le compte d'une importante **société publique :**

Deux (02) Analystes en Cybersécurité

Lieu de travail : Cotonou, Bénin

Mission, attributions et profil recherché : Voir fiche de poste ci-après :

Le profil est-il le vôtre ?

Envoyez votre dossier par mail, en précisant en objet l'intitulé du poste à l'adresse : cabinetsecca.sarl@gmail.com

PIECES A FOURNIR :

1. Une lettre de motivation adressée au Directeur Général de SECCA SARL en précisant le poste (y inscrire votre disponibilité et votre prétention salariale) ;
2. Un Curriculum Vitae détaillé comprenant trois (03) références professionnelles ;
3. Une copie légalisée des diplômes ou titres à faire valoir ;
4. L'authenticité du diplôme ou titre à faire valoir (pourra être complétée avant la fin du processus de sélection) ;
5. Les preuves des expériences présentées par le candidat ;
6. Une copie de la pièce d'identité en cours de validité.

NB. :

En soumettant votre candidature, vous nous donnez également votre consentement pour la collecte, le stockage, le traitement de vos données personnelles.

Vous pouvez à toute étape du processus, exercer votre droit d'opposition.

Date limite de dépôt : **Vendredi 11 Avril 2025**

PROFIL DE L'ANALYSTE EN CYBERSECURITE

Mission

Les Analystes en Cybersécurité auront pour mission, sous la supervision du Responsable de la Sécurité du Système d'Information, de :

- analyser, interpréter et traiter les alertes de sécurité, ainsi que de prévenir les cyberattaques et autres menaces potentielles pesant sur le système d'information de la Société ;
- intervenir sur les incidents de cybersécurité et réaliser des tests de vulnérabilité sur le système d'information de la Société.

1. Tâches principales

Les Analystes en Cybersécurité auront la charge de :

- analyser les alertes de sécurité émises par les solutions de sécurité ;
- réaliser des tests de vulnérabilité périodiques conformément à la politique de gestion des vulnérabilités de la Société ;
- assurer une surveillance de tous les actifs du système d'information à l'aide des outils de sécurité déployés dans l'architecture de la Société ;
- réaliser des actions de forensic en cas de compromission d'un actif informatique ou de tentative d'intrusion ;
- collaborer avec le SOC externe pour évaluer l'étendue d'un incident dans l'infrastructure du de la Société ;
- appliquer les procédures de réponse aux incidents de sécurité de l'information ;
- isoler les systèmes compromis afin de limiter la propagation des menaces ;
- fournir un rapport détaillé sur les incidents et les actions entreprises ;
- communiquer régulièrement les rapports au RSSI et au DSI ;
- effectuer une veille constante sur les nouvelles vulnérabilités et les menaces ;
- coordonner avec l'équipe de la DSI pour s'assurer que les correctifs des vulnérabilités détectées sont appliqués ;
- se tenir informé des dernières évolutions en matière de cybersécurité.

2. Qualifications

Les candidats devront remplir les conditions ci-après :

- être titulaire d'une Licence (BAC+3) en sécurité informatique ;
- avoir une expérience significative dans l'analyse des incidents en se basant sur le cadre ATT&CK de MITRE ;
- justifier d'au moins deux (02) années d'expérience professionnelle dans le domaine de la sécurité informatique.

3. Savoirs

- avoir une bonne connaissance du Système d'Information des Sociétés Publiques ;
- avoir une connaissance de la gestion des incidents suivant les normes NIST et ISO 27005 ;
- avoir une bonne connaissance des outils d'analyse de sécurité de l'information et de forensic ;
- avoir une bonne connaissance des solutions de sécurité (Pare-feu de nouvelle génération NGFW, PAM Wallix, Solution XDR, Solution SIEM, Pare-feu d'application Web WAF) ;
- avoir une bonne connaissance des techniques d'attaque, de défense et les outils de sécurité de l'information.

4. Savoir-faire

- savoir travailler en équipe ;
- être passionné de cybersécurité, autodidacte, avec une forte capacitée d'adaptation ;
- avoir une bonne capacité rédactionnelle ;
- avoir une parfaite maitrise de l'utilisation des outils bureautiques (Word, Excel, Powerpoint, Outlook, Sharepoint, Firefox) ;
- avoir une excellente maitrise de la langue française aussi bien à l'oral qu'à l'écrit ;
- avoir une bonne capacité d'analyse ;
- avoir une bonne maitrise de l'anglais technique.

5. Savoir-être

- être impartiale, juste et précis dans les vérifications ;
- être courtois, communiquant et engagé ;
- avoir l'esprit d'écoute ;
- être méthodique, organisé, vigilant ;
- être disponible, dynamique et avoir le sens de la discrétion ;
- faire preuve de sérénité, d'adaptabilité et de capacité à trouver rapidement des solutions ;
- avoir le sens du respect de la hiérarchie ;
- savoir anticiper et porter des initiatives et innovations de qualité ;
- avoir le sens de responsabilité ;
- avoir un esprit analytique, curieux, rigoureux et organisé ;
- avoir un solide esprit de contrôle ;
- faire preuve de disponibilité;
- avoir une bonne capacité d'adaptation ;
- respecter la confidentialité des données ;
- faire preuve d'un grand sens d'intégrité et d'objectivité.