COMMISSARIAT GENERAL

COMMISSARIAT DES SERVICES GENERAUX

DIRECTION DES RESSOURCES HUMAINES
ET DE LA FORMATION PROFESSIONNELLE

TERMES DE REFERENCE

Titre du poste	*Grade*	*Lieu de travail*
Professionnel Technique (Analyste SOC)	P1	Lomé et sur toute l'étendue du territoire national

Nom du titulaire du poste	*Supérieur hiérarchique*
A déterminer	Chef de la section d'affectation

Objectif principal du poste

Sous la supervision du chef hiérarchique, l'analyste SOC est responsable de la surveillance et de la sécurité du système d'information de l'Office Togolais des Recettes (OTR). Il/elle détecte et évalue les activités suspectes ou malveillantes, propose des plans d'action pour résoudre les incidents de sécurité et contribue à l'amélioration continue des méthodes de détection de prévention au sein de l'Office en fonction des objectifs stratégiques ainsi que des évolutions technologiques et réglementaires. Il doit faire preuve de vigilance quant à la gestion des risques liés à l'utilisation de l'informatique.

Tâches & Responsabilités principales

Sous la supervision du supérieur hiérarchique, l'agent contribue à :

1. Surveiller le système d'information pour détecter les activités suspectes ou malveillantes ;
2. Analyser et interpréter les alertes de sécurité émises par le centre des opérations de sécurité (SOC) ;
3. Évaluer les dommages subis en cas d'intrusion et proposer des solutions techniques pour rétablir les services ;
4. Coordonner avec les équipes d'administration informatique et de réponse aux incidents (CSIRT) pour résoudre les incidents de sécurité ;
5. Faire l'escalade des incidents de sécurité de niveau supérieur ;
6. Participer à la prévention des incidents de sécurité en amont ;
7. Analyser des protocoles réseau ;
8. Détecter et gérer les vulnérabilités du système d'information ;
9. Faire la veille technologique sur les vulnérabilités et menaces courantes (CVE) fournies par les CERT et les sources de bases de données d'intelligence sur les menaces (Threat Intelligence)

CV

Qualifications	*Expérience*
Essentielle 1. Avoir au minimum une Licence (BAC+3) en Sécurité des Systèmes d'Information, Réseau Système, Génie Logiciel ou équivalent ;	Essentielle 2. Justifier d'une expérience professionnelle pertinente d'au moins trois (03) ans dans le domaine de la sécurité des systèmes d'information comme Analyste SOC ; Souhaitable 3. Avoir une certification cyber sécurité (par exemple, CEH, CompTIA Security+, CISSP...) serait un atout ;

Connaissances Spéciales	***Habiletés Spéciales***
Essentielles 4. Connaissance et mise en œuvre des systèmes de supervision de la sécurité (SIEM, sondes, honeypots, équipements filtrants) ; 5. Connaissance approfondie de QRadar ; 6. Connaissance approfondie de Cisco ESA et de Cisco Umbrella, FortiWAF, FortiMail, FortiWeb, FortiSandbox... 7. Connaissance des EDR, NDR, Antivirus ; 8. Maîtrise de langage de Scripting (python, C, Powershell); 9. Connaissance des outils de Pentest ; 10. Connaissance des outils de ticketing ; 11. Bonne connaissance en sécurité applicatif système et Réseau ; 12. Maitrise des systèmes d'exploitation (Windows, Linux, Unix); 13. Notions de base sur les configurations usuelles, systèmes et outils bureautiques ; 14. Connaissance approfondie des réseaux informatiques ; 15. Connaissance approfondie des systèmes d'information et des technologies de sécurité ;	*Essentielles* 16. Parler couramment le français ; 17. Capable de gérer les conflits de manière diplomatique. *Souhaitables* 18. Connaissances de base en anglais ; *19.* Excellentes compétences rédactionnelles.

Qualités personnelles

Essentielles	*Souhaitables*
20. Intègre et d'une moralité irréprochable. 21. Esprit analytique développé ; 22. Disposé (e) à suivre un cycle de formation d'amélioration des compétences ; 23. Personne dotée d'un sens d'écoute ; 24. Bonnes qualités interpersonnelles et sociale/diplomatique dans les relations avec les parties prenantes et le personnel ; 25. Discret et digne de confiance 26. Ordonné, discipliné et rigoureux dans le travail	27. Capable d'exécuter simultanément plusieurs tâches ; 28. Capable de travailler en situation d'urgence ; 29. Soins à son image professionnelle ; plein d'assurance et confiant ; 30. Ouvert d'esprit, stratégique, penseur conceptuel, innovateur.