

FINASDDEE
Credit Line

REJOIGNEZ

L'ÉQUIPE

RESPONSABLE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION (RSSI)

DOUALA

I. INDICATEURS CLÉS DE PERFORMANCE DU POSTE

✓ 100 % des alertes de sécurité critiques évaluées et escaladées dans les délais de réponse approuvés.
✓ 100 % des vulnérabilités critiques et à haut risque suivies jusqu'à une correction vérifiée ou un traitement du risque approuvé.
✓ 100 % des revues planifiées des contrôles de sécurité et des évaluations de vulnérabilités réalisées ; constats documentés et suivis.
✓ Suivi et reporting dans les délais des actions de remédiation assignées issues des recommandations de l'ANTIC, de la COBAC et de l'audit interne.
✓ Réalisation des actions de sensibilisation à la sécurité, des exercices de réponse aux incidents et de préparation à la reprise planifiés.
✓ Reporting dans les délais des risques et incidents de sécurité à la Direction Générale et appui à la supervision du BIISC.

II. PRINCIPALES RESPONSABILITÉS

▪ Élaborer et mettre en œuvre la stratégie de sécurité de l'information, les politiques, les normes et le programme de traitement des risques, alignés sur la norme ISO/IEC 27001 et les exigences réglementaires applicables.
▪ Mener des évaluations de vulnérabilités pratiques, des revues de configuration de sécurité et des tests de sécurité autorisés des réseaux, serveurs, applications et API ; coordonner les tests d'intrusion indépendants.
▪ Surveiller les événements de sécurité à l'aide des outils de sécurité Fortinet, des journaux centralisés et des solutions de supervision de la sécurité ; investiguer les menaces et coordonner le confinement des incidents, la réponse et la préservation des preuves.
▪ Évaluer les règles de pare-feu, les privilèges d'accès, la segmentation réseau, la protection des terminaux, la gestion des correctifs et la sécurité des sauvegardes ; vérifier les mesures correctives mises en œuvre par l'équipe informatique.
▪ Tenir à jour le registre des risques de sécurité de l'information et suivre la remédiation des constats de l'ANTIC, de la COBAC et de l'audit interne ; escalader les actions en retard et les risques résiduels.
▪ Évaluer les risques de sécurité des nouveaux projets, des changements applicatifs, des services tiers et du traitement des données ; promouvoir le développement sécurisé et la protection des informations clients.
▪ Coordonner la sensibilisation à la sécurité, les exercices de réponse aux incidents et l'assurance de la reprise après sinistre ; appuyer la déclaration réglementaire des incidents avec le service Risques et Conformité.
▪ Apporter un appui technique au Comité Informatique et Sécurité de l'Information du Conseil (BIISC), participer aux sessions élargies si nécessaire, et rendre compte directement au Directeur Général des risques de sécurité, des incidents, de l'efficacité des contrôles, de l'avancement des remédiations et des besoins en ressources.
▪ Travailler étroitement avec le Responsable IT sur les améliorations techniques de sécurité tout en maintenant une surveillance indépendante et en évitant l'auto-revue ; appuyer l'assurance indépendante de l'Audit interne.

III. PROFIL DU POSTE

Expérience	• Au moins cinq (5) ans d'expérience pertinente en cybersécurité, sécurité de l'information ou risques informatiques, dont au moins deux (2) ans dans un poste de direction ou de coordination en sécurité. • Expérience pratique avérée en évaluation de vulnérabilités, tests de sécurité, durcissement des systèmes, investigation d'incidents et analyse des menaces. • Connaissance pratique de FortiGate, FortiAnalyzer et FortiManager ; expérience des SIEM, de la protection des terminaux, des WAF et des outils de supervision de la sécurité. • Connaissance pratique de Windows Server, de la sécurité d'Active Directory, de la sécurité réseau, de la gestion des identités et des accès et de la protection des comptes à privilèges. • Expérience pratique de la sécurité des applications web et des API, de la vérification des corrections de vulnérabilités et des pratiques de développement sécurisé (OWASP). • Expérience de la mise en œuvre de politiques de sécurité de l'information, d'évaluations des risques, de contrôles alignés sur ISO/IEC 27001, de remédiation d'audit et de programmes de réponse aux incidents.

Expérience	• Une expérience dans la banque, la microfinance ou un autre secteur réglementé, y compris des exigences réglementaires de sécurité, est fortement souhaitée.
Formation	• Licence (Bachelor) en Cybersécurité, Informatique, Technologies de l'information, Ingénierie des réseaux ou domaine connexe. • Au moins une certification de sécurité reconnue (CISSP, CISM ou équivalent) est requise ; ISO/IEC 27001 Lead Implementer ou Lead Auditor est fortement souhaitée. • Les certifications pratiques de sécurité telles que OSCP, GIAC, Security+ ou les certifications Fortinet avancées constituent des atouts. • Un Master en Cybersécurité ou en Sécurité de l'information, ainsi qu'une certification ITIL, constituent des atouts.
Qualités personnelles	• Excellentes aptitudes d'analyse, techniques, d'investigation et de communication ; proactif et orienté résultats. • Grande intégrité, confidentialité, jugement professionnel et capacité à remettre en question de manière constructive les faiblesses de sécurité. • Bilingue anglais et français (oral et écrit).

Qualités personnelles	• Capacité à coordonner efficacement avec des parties prenantes techniques et non techniques.

Rattachement : Directeur Général

Postulez ici : cv.fcl@finasddee-creditline.com

Date limite de candidature : Lundi 7 décembre 2026