

Le Dépositaire Central / Banque de Règlement (DC/BR)

Lance un appel à candidatures pour le recrutement du poste suivant

Un(e) Chargé(e) de la Sécurité des Systèmes d'Information

Poste basé à Abidjan (CDI)

Attributions et responsabilités du poste :

Stratégie et Gouvernance en Cybersécurité :

- Élaborer et mettre en œuvre la politique de sécurité des systèmes d'information (PSSI) ;
- Définir et actualiser les stratégies de cybersécurité en conformité avec les normes et réglementations (ISO 27001, NIST, RGPD, directives AMF-UMOA, BCEAO) ;
- Assurer la veille réglementaire et technologique en matière de cybersécurité ;
- Piloter la gouvernance des risques liés à la cybersécurité et assurer leur intégration dans la stratégie globale du DC/BR.

Gestion des Risques et Conformité :

- Identifier, analyser et évaluer les risques liés à la sécurité des SI ;
- Mettre en place des plans d'actions correctifs et préventifs pour réduire les risques identifiés ;
- Assurer la mise en conformité avec les exigences légales et normatives ;
- Superviser les audits de sécurité et coordonner les actions de remédiation.

Protection des Données et Sécurisation des SI :

- Définir et mettre en œuvre des mesures de protection des données sensibles et de la confidentialité des informations ;
- Gérer les accès et les habilitations des utilisateurs en fonction des besoins métiers ;
- Superviser les politiques de sauvegarde et de restauration des données ;
- Déployer des solutions de protection (antivirus, firewall, SIEM, DLP, MFA, PAM).

Surveillance et Gestion des Incidents de Sécurité :

- Mettre en place un SOC (Security Operations Center) ou superviser les solutions de surveillance des menaces ;
- Détecter, analyser et répondre aux incidents de sécurité (cyberattaques, intrusions, fuites de données) ;
- Gérer les crises cyber et élaborer un plan de réponse aux incidents (PRA/PCA, tests d'intrusion, simulations de cyberattaques) ;
- Assurer le reporting des incidents auprès de la direction et des autorités compétentes.

Sensibilisation et Formation en Cybersécurité :

- Organiser des campagnes de sensibilisation à la cybersécurité pour les collaborateurs ;
- Rédiger des guides de bonnes pratiques et animer des formations internes ;
- Assurer la montée en compétences des équipes techniques sur les enjeux de cybersécurité.

Lien(s) hiérarchique(s)

- Gestionnaire des Risques.

Compétences techniques

Normes et réglementations :

- Maîtrise des référentiels de cybersécurité (ISO 27001, NIST, CIS, RGPD, PCI-DSS) ;
- Connaissance des réglementations locales et internationales en matière de protection des données.

Sécurité des Systèmes et Réseaux :

- Bonne connaissance des architectures réseaux et des protocoles sécurisés (TLS, IPsec, VPN, DNSSEC) ;
- Expérience dans la sécurisation des infrastructures cloud (AWS, Azure, Google Cloud) ;
- Maîtrise des outils de protection et de détection (firewalls, IDS/IPS, SIEM, SOC) ;
- Expertise en gestion des vulnérabilités et en tests d'intrusion.

Gestion des Identités et Accès (IAM) :

- Expérience dans la mise en place de solutions IAM (Active Directory, LDAP, SSO, MFA) ;
- Gestion des droits et des rôles selon les principes du moindre privilège (Zero Trust).

Supervision et Réponse aux Incidents :

- Utilisation d'outils de monitoring et de réponse aux incidents (Splunk, ELK, Wazuh, Sentinel ...) ;
- Expérience en forensic et analyse des menaces.

Qualifications

- Être titulaire d'un Diplôme de niveau Bac+5 en informatique, systèmes d'information, réseaux et télécommunications, Cybersécurité ou disciplines connexes ;
- Certifications appréciées : CISSP, CISM, CEH, ISO 27001 Lead Implémenter, CCSP ;
- Avoir un bon niveau en anglais.

Expérience Professionnelle

- 3 ans d'expérience dans la cybersécurité idéalement dans un environnement multiculturel dont trois (3) dans une fonction similaire dans une infrastructure de marché, dans une banque commerciale, dans une multinationale ou institution financière régionale ou internationale ;
- Expérience dans des environnements critiques nécessitant une haute disponibilité ;
- Expérience avérée dans la gestion des incidents et la mise en conformité réglementaire.

Nationalité

Être ressortissant d'un État Membre de l'UMOA.

Les candidat(e)s intéressé(e)s pourront télécharger les TDR sur le site web du DC/BR : www.dcbuemoa.org dans la rubrique « nous rejoindre » en bas du site web.

Le dossier de candidature doit être envoyé sous la référence **CSSI/DCBR/2026** à l'adresse recrutements@dcbuemoa.org au plus tard le 30 octobre 2026 à 12h00. Seul(e)s les candidat(e)s éligibles seront invité(e)s à participer à un entretien.