Référence : AS/DSI/2025
Date limite de candidature : 21/10/2025

1 ARCHITECTE CYBERSECURITE (H/F)

(Poste(s) basé(s) à SALÉ)

Mission :

Rattaché(e) à la DIRECTION SYSTÈME D'INFORMATION, votre mission consiste à définir les architectures, les normes et les feuilles de route technologiques afférentes à la cybersécurité en vue d'assurer la protection du système d'information de la Banque, et ce, en alignement avec sa stratégie, sa politique d'appétence aux risques et les exigences réglementaires.

Responsabilités et Activités principales :

Définir, en concertation avec les autres parties prenantes dont le RSSI :
- L'architecture de sécurité (applications, données, infrastructures, cloud...)
- Les principes directeurs et les architectures de référence en cybersécurité (Zero Trust, segmentation, cryptographie, IAM…) et en piloter l'adoption ;

Assurer l'intégration des architectures dans les opérations (cloud, Dev, réseau, CERT, exploitation…) ;
Garantir, en coordination avec le RSSI, que les choix technologiques et les orientations d'architecture de sécurité s'inscrivent de manière cohérente dans la posture de sécurité et la stratégie cybersécurité de la Banque ;
Accompagner la revue et la validation des architectures et des choix techniques de sécurité en conciliant maîtrise des risques et efficience ;
Assurer l'intégration des cadres de contrôle (NIST, ISO 27001…) et des exigences de résilience de la Banque (PCA, PRA, …) dans la conception des architectures de sécurité ;
Accompagner la conception de sécurité des intégrations (flux internes et écosystème) et la définition des besoins et solutions liés au chiffrement des données et à la gestion des clés ;
Soutenir les démarches DevSecOps et la sécurisation des pipelines CI/CD (SAST/DAST/IAST) ;
Apporter un appui aux équipes de la Banque en charge de la sécurité des tiers et du cloud, de la protection des données, de la réponse aux incidents et de la gestion des vulnérabilités.

Qualifications :

Titulaire d'un Bac+5 en informatique/sécurité (ou équivalent), vous justifiez d'une expérience pertinente au poste d'au moins 8 ans.

CISSP, CISM, CCSP, SABSA et certifications sécurité du cloud seraient un atout.

Compétences et Qualités :

Architecture technique
- Sécurité applicative & API, SDLC sécurisé, gestion des secrets
- Sécurité cloud & conteneurs (hardening, posture management)
- Threat modeling & évaluation des risques , sécurité pour systèmes HA/latence faible
- Architecture Zero Trust et défense en profondeur , micro-segmentation, accès sécurisé
- IAM (RBAC/ABAC, fédération, PAM)
- Cryptographie & gestion de clés (PKI, HSM, rotation, chiffrement au repos/en transit)
- Plans de continuité d'activité et de reprise post incident et plans de continuité des opérations

Développement & Coding
- Infrastructure as a Code et policy as a code (ex. OPA) pour l'automatisation des contrôles
- Intégration/automatisation de sécurité , sécurisation des pipelines CI/CD

Sécurité Opérationnelle et supervision
- Supervision continue, cas d'usage SIEM/SOAR, patch/vulnérabilités

Infrastructures techniques
- Fiabilité & résilience, PRA/PCA, sécurité réseau & endpoint

Fondamentaux métiers
- Connaissance du secteur financier serait un atout
- Gestion du risque, orientation parties prenantes (ex : opérations, supervision, paiements, …), résolution de problèmes

Gestion de projets & programmes
- Approche systémique , pilotage de programmes sécurité

Compétences interpersonnelles & leadership
- Capacités de communication, négociation/priorisation, rédaction synthétique

- Les candidats intéressés, doivent obligatoirement remplir le formulaire de recrutement ouvert pour ce poste et disponible sur notre site web www.bkam.ma dans la rubrique « carrières», et ce, avant la date limite de dépôt de candidature mentionnée ci-dessus.
- Les candidats, dont les dossiers seront retenus lors de la phase de présélection, seront informés de la date et du lieu de l'entretien par mail.
- Les candidats doivent être de nationalité marocaine et âgés de moins de 40 ans.