ANNONCE DE VACANCE

BACM/DRH/26-06-2024

Intitulé du poste	: **Responsable Sécurité des Systèmes d'Information (RSSI)**
Direction	: **Générale**
Lien fonctionnel	**: Directeur Générale Adjoint – Support**
Lieu de fonction	: **Douala**
Statut	: **Cadre**
Contrat	: **CDI**
Zone de publication	: **Interne et externe**

Mission principale **: Assurer un rôle de conseil, d'assistance technique, d'information, de formation et d'alerte auprès du personnel par rapport aux systèmes d'information, afin de garantir la sécurité logique et physique du système d'information dans son ensemble.**

ACTIVITÉS PRINCIPALES

Gouvernance, risques et conformité cybernétiques

- S'assurer que les pratiques de l'entreprise respectent les régulations légales et les normes internes et externes via la veille réglementaire ;
- Développer la culture de la cybersécurité auprès des collaborateurs de la BACM en mettant en œuvre le programme annuel de sensibilisation AFG ;
- Maintenir des reportings réguliers sur l'état de la sécurité de l'information, analyser les tendances des incidents de sécurité et fournir des recommandations stratégiques à la Direction Générale.

Cyber Risk Management

- Identifier et évaluer les actifs informationnels critiques ; classer les risques selon leur probabilité et leur impact potentiel sur l'organisation ;
- Utiliser des techniques et/ou méthodologies afin d'évaluer les menaces existantes et émergentes ; analyser les vulnérabilités dans les systèmes et les processus ;
- Développer des stratégies pour atténuer les risques identifiés, y compris l'adoption de technologies de sécurité appropriées et la révision des politiques et procédures.

Identity and Access Management / Privileged Access Management (IAM / PAM)

- Participer à la mise en œuvre du programme IAM/PAM d'AFG sur son périmètre ;
- Gérer l'accès des utilisateurs de la BACM aux systèmes, applications et données, en se servant de la plateforme IAM ;
- Effectuer une surveillance en temps réel pour détecter les utilisations anormales ou non autorisées des accès, générer des rapports détaillés pour les audits ;
- Former régulièrement les utilisateurs aux politiques d'accès, aux risques associés aux négligences, et renforcer la conformité aux procédures de sécurité.

Sécurité opérationnelle

- Mettre en application et décliner opérationnellement la politique de sécurité de l'entreprise ;
- Conseiller le Top Management sur les solutions de sécurité adaptées à leurs besoins tout en rationalisant les différents outils de sécurité présents sur le marché et, ainsi, garantir une meilleure interopérabilité des systèmes ;
- Piloter sur son périmètre la sécurité des réseaux, des terminaux (postes de travail, appareils mobiles, etc.), et contribuer à la mise en œuvre de la sécurité périmétrique (firewall, proxy) ;
- Assurer l'intégration de la sécurité dès la conception (Security by Design) dans tous les projets informatiques, garantissant que les mesures de protection des données et les contrôles de sécurité sont intégrés de manière proactive dans l'architecture des systèmes, des applications et des infrastructures dès les premières étapes de développement ;
- Scanner régulièrement l'environnement dans le but de détecter des vulnérabilités ;
- Piloter et traiter les alertes et incidents de sécurité ;
- Construire des tableaux de bord et des indicateurs de mesure du niveau de sécurité opérationnelle de l'entreprise.

Cyber résilience

- Élaborer et maintenir des plans de continuité d'activité et de reprise après sinistre pour minimiser l'impact des incidents de sécurité sur les opérations commerciales ;
- Conduire des revues après chaque incident majeur pour identifier les lacunes dans les politiques et les procédures, et recommander des améliorations pour prévenir les récurrences ;
- Organiser régulièrement des tests de pénétration et des simulations d'attaques pour évaluer la robustesse des infrastructures et des réponses aux incidents, et pour former le personnel à la réactivité face aux crises.

QUALIFICATIONS ET EXPÉRIENCE REQUISES	COMPÉTENCES REQUISES

• Ingénieur / Master en Sécurité Informatique ou autre discipline apparentée ;
• Avoir une expérience professionnelle d'au moins 5 ans à un poste similaire ;
• Les certifications ci-dessous sont recommandées :
  ◦ Certified Ethical Hacker (CEH) ;
  ◦ Cisco Certified Network Associate (CCNA);
• Le bilinguisme (français – anglais) serait un atout.
	✓ **Savoir**
	• Bonnes connaissances de l'environnement bancaire ;
	• Bonne connaissance de la réglementation bancaire ;
	• Connaissance approfondie des normes de sécurité (ISO 27001, RGPD, ISO 27005, NIS2).
	
	✓ **Savoir-faire**
	• Maîtrise des outils de sécurité informatique : pare-feux, antivirus, systèmes de détection d'intrusion, etc.
	• Maîtrise des méthodes de reporting ;
	• Maîtrise des techniques de communication orale et écrite
	• Utilisation des outils de bureautique ;
	• Exploitation de Flexcube.
	
	✓ **Savoir-être**
	• Intégrité / probité
	• Aisance relationnelle / capacité d'écoute / esprit d'équipe
	• Organisation / méthode / rigueur

Dépôt des Candidatures

Envoyez votre curriculum vitae à **rh.recrutement@banqueatlantique.cm** au plus tard **le jeudi 04 juillet 2024**, en précisant en objet **« Responsable Sécurité SI ».**

Toute candidature reçue par un canal autre que celui indiqué ne sera pas considérée.

Trois semaines après cette date, si vous n'avez pas été contacté(e), merci de considérer que votre candidature n'a pas été retenue.

Direction des Ressources Humaines	Direction Générale