

Group Officer – Cybersécurité

Supérieur hiérarchique : Group Manager – Assurance technologique & Auditeur cybersécurité

OBJECTIF DU POSTE

Le/la **Group Officer – Cybersécurité** assiste le/la Group Manager – Assurance technologique & Auditeur cybersécurité dans la réalisation d’une assurance indépendante de la posture de cybersécurité du Groupe dans plusieurs juridictions.

Le poste combine une expertise technique pratique dans les domaines des opérations de cybersécurité, de la sécurité du cloud, de la sécurité des infrastructures et de la sécurité des applications, avec des techniques d’assurance fondées sur les données et l’intelligence artificielle.

Le/la titulaire du poste est chargé(e) de réaliser des audits de cybersécurité fondés sur les risques, d’effectuer des tests et analyses techniques, de mettre en place des dispositifs de surveillance continue et de contribuer à la modernisation de l’assurance cybersécurité grâce à l’analyse de données, à l’automatisation et aux technologies émergentes.

Le poste joue un rôle important dans le renforcement de la résilience et de la gouvernance en matière de cybersécurité de la banque, en combinant la rigueur traditionnelle de l’audit avec des approches modernes fondées sur les données.

CONTEXTE DU POSTE

Le poste exige du/de la candidat(e) :

- une grande intégrité ;
- une forte curiosité technique ;
- une attention particulière aux détails ;
- une attitude proactive.

Le/la candidat(e) doit disposer de solides compétences techniques pratiques dans différents domaines de la cybersécurité, être capable de traduire les constats techniques en conclusions d’assurance claires et être disposé(e) à utiliser l’analyse de données et l’automatisation afin d’améliorer l’efficacité des audits.

Le/la titulaire contribuera au renforcement de la gouvernance, de la gestion des risques et de l'environnement de contrôle de la banque grâce à des travaux d'audit technique en cybersécurité associés à des solutions modernes d'assurance fondées sur les données.

PRINCIPALES RESPONSABILITÉS

1. Réalisation des audits de cybersécurité

- Réaliser des audits de cybersécurité fondés sur les risques couvrant les réseaux, les infrastructures, les plateformes cloud, les applications métier et les contrôles de sécurité.
 - Effectuer des revues techniques des opérations de cybersécurité et des processus des **Security Operations Centers (SOC)**, notamment l'ingénierie de détection, la préparation à la réponse aux incidents, l'efficacité de la surveillance de sécurité et les opérations de renseignement sur les menaces.
 - Réaliser des audits de sécurité cloud sur les environnements **AWS, Azure et Google Cloud Platform**, notamment sur les charges de travail cloud, les configurations, la gestion des identités et des accès (IAM), le chiffrement et les responsabilités partagées.
 - Effectuer des revues de sécurité des infrastructures, notamment de l'architecture réseau, des contrôles des terminaux, de la gestion des accès privilégiés, du durcissement des systèmes et de la gestion des correctifs.
 - Réaliser des audits de sécurité des applications, notamment des revues du **cycle de développement sécurisé (Secure SDLC)**, des évaluations de la sécurité des API, de la sécurité des conteneurs et de Kubernetes, ainsi que des pratiques **DevSecOps**.
 - Réaliser des évaluations des vulnérabilités, examiner les résultats des tests d'intrusion et évaluer l'adéquation et la rapidité des actions de remédiation.
 - Documenter les procédures d'audit, les éléments probants, les constats et les recommandations conformément à la méthodologie d'audit et aux normes de qualité.
 - Communiquer clairement les constats techniques aux entités auditées, au/à la Group Manager et aux parties prenantes de niveau supérieur, en veillant à ce que les problèmes soient clairement formulés et puissent donner lieu à des actions concrètes.
-

2. Gestion des risques cyber et conformité

- Évaluer les contrôles de cybersécurité au regard des cadres, normes et réglementations applicables, notamment :
 - **ISO 27001** ;
 - **NIST Cybersecurity Framework** ;
 - **CIS Controls** ;
 - **COBIT** ;
 - **PCI DSS** ;

- **SWIFT Customer Security Controls Framework (CSCF).**
 - Évaluer la conformité aux politiques, normes et procédures internes de cybersécurité, en identifiant les lacunes et les possibilités d'amélioration.
 - Examiner l'efficacité des dispositifs de réponse aux incidents, de continuité d'activité et de reprise après sinistre liés aux cybermenaces et aux actifs technologiques critiques.
 - Évaluer les risques cyber liés aux tiers, notamment l'adéquation des dispositifs d'assurance de sécurité des fournisseurs, les risques de concentration et les dépendances vis-à-vis des fournisseurs de services cloud.
 - Contribuer au reporting des risques cyber et au suivi des actions de remédiation, en veillant à la clôture dans les délais des constats d'audit.
 - Se tenir informé(e) des nouvelles cybermenaces, vulnérabilités, techniques d'attaque et de l'évolution du paysage des menaces applicable au secteur bancaire et aux services financiers.
-

3. Assurance cybersécurité fondée sur les données et l'IA

- Concevoir et maintenir des routines d'analyse de données et des tests automatisés de surveillance des contrôles de cybersécurité, en utilisant notamment :
 - **SQL ;**
 - **Python ;**
 - **Power BI ;**
 - **Power Automate ;**
 - **Audit Command Language (ACL).**
- Appliquer des techniques d'assurance fondées sur l'IA, notamment l'analyse prédictive, la détection des anomalies et l'audit assisté par l'IA, afin d'identifier les indicateurs de risque cyber, les faiblesses des contrôles et les menaces émergentes au sein du Groupe.
- Développer des dispositifs d'audit continu des contrôles de cybersécurité sur les plateformes critiques, les applications métier et les canaux numériques.
- Analyser d'importants volumes de données provenant :
 - des journaux de sécurité ;
 - des systèmes **SIEM/SOAR ;**
 - des analyses de vulnérabilités ;
 - des flux de renseignement sur les menaces,
- afin d'identifier les tendances, les anomalies et les événements nécessitant une attention particulière dans le cadre des audits.
- Contribuer au développement d'analyses réutilisables, de scripts, de tableaux de bord et de tests automatisés permettant de standardiser et de déployer à grande échelle les procédures d'audit cybersécurité.
- Appliquer, lorsque cela est pertinent, des techniques de science des données et d'apprentissage automatique afin de soutenir la surveillance intelligente des risques et l'assurance cybersécurité proactive.

- Collaborer avec le pôle **Continuous Data-Driven Assurance & Innovation** afin d'intégrer les approches fondées sur les données et les outils d'analyse dans les activités d'audit cybersécurité.
-

4. Relations avec les parties prenantes et soutien aux investigations

- Collaborer avec les parties prenantes des domaines de la cybersécurité, de l'IT et des métiers afin de comprendre les systèmes, les contrôles et les initiatives émergentes au sein du Groupe.
 - Participer à des investigations ponctuelles concernant des incidents cyber présumés, des fraudes, des comportements répréhensibles ou des irrégularités, au moyen d'analyses techniques, de l'examen de preuves numériques et de techniques d'investigation fondées sur les données.
 - Collaborer avec l'ensemble de l'équipe **GIAMS**, notamment les pôles :
 - Assurance technologique ;
 - Assurance continue fondée sur les données & Innovation ;
 - Investigations & Forensic.
 - Participer aux revues de suivi et à la vérification de l'efficacité des actions de remédiation relatives aux constats d'audit cybersécurité.
 - Contribuer à l'amélioration continue de la méthodologie, des outils et des méthodes de travail du pôle.
 - Se tenir informé(e) de l'évolution des techniques, outils et plateformes d'audit cybersécurité et partager les connaissances ainsi que les nouvelles pratiques au sein de l'équipe.
-

QUALIFICATIONS ET EXPÉRIENCE

Expérience professionnelle

- **5 à 8 ans d'expérience** dans les domaines de la cybersécurité, de l'audit de sécurité informatique ou de la gestion des risques technologiques, avec une solide expérience technique pratique.
- Expérience démontrable dans plusieurs domaines :
 - opérations de cybersécurité ;
 - sécurité cloud ;
 - sécurité des infrastructures ;
 - sécurité des applications.
- Expérience dans la réalisation d'audits cybersécurité fondés sur les risques et de revues des contrôles de sécurité, de préférence dans le secteur bancaire ou des services financiers.

- Une expérience dans l'utilisation de l'analyse de données, de l'automatisation et de techniques modernes d'audit appliquées à l'assurance cybersécurité constitue un avantage.
-

CONNAISSANCES ET COMPÉTENCES

Expertise technique

- Solides connaissances pratiques des opérations de cybersécurité, des processus SOC, des plateformes **SIEM/SOAR**, de la surveillance de sécurité, de l'ingénierie de détection et de la réponse aux incidents.
 - Bonne connaissance de la sécurité cloud sur **AWS, Azure et Google Cloud Platform**, notamment :
 - IAM ;
 - contrôles réseau ;
 - protection des charges de travail ;
 - chiffrement ;
 - modèles de responsabilité partagée.
 - Solide compréhension de la sécurité des infrastructures :
 - architecture réseau ;
 - sécurité des terminaux ;
 - gestion des accès privilégiés ;
 - durcissement des systèmes ;
 - gestion des correctifs.
 - Connaissance de la sécurité des applications :
 - Secure SDLC ;
 - sécurité des API ;
 - OWASP Top 10 ;
 - sécurité des conteneurs et de Kubernetes ;
 - pratiques DevSecOps.
 - Compréhension des cadres, normes et réglementations en matière de cybersécurité, notamment **ISO 27001, NIST Cybersecurity Framework, CIS Controls, COBIT, PCI DSS et SWIFT CSMF**.
 - Expérience pratique des outils d'analyse de données et d'automatisation, notamment **SQL, Python, Power BI, Power Automate et ACL**.
 - Connaissance des concepts d'IA et de machine learning et de leur application à la cybersécurité et à l'analyse des audits.
 - Connaissance des outils d'évaluation des vulnérabilités, des concepts de tests d'intrusion et des plateformes de renseignement sur les menaces.
 - Sensibilisation aux risques liés aux technologies émergentes, notamment à la gouvernance et à la sécurité de l'IA/du machine learning ainsi qu'aux contrôles liés à l'identité.
-

Gestion des risques et audit

- Bonne compréhension des principes de l'**audit fondé sur les risques (Risk-Based Audit)** et capacité à respecter les normes de l'**IIA (Institute of Internal Auditors)**.
 - Capacité à appliquer les concepts de risque et de contrôle dans le contexte de la cybersécurité et des technologies.
 - Bonne connaissance des bonnes pratiques en matière de gouvernance, de gestion des risques et de conformité IT, ainsi qu'une expérience dans l'évaluation des risques de cybersécurité.
-

Compétences analytiques et résolution de problèmes

- Solide esprit analytique, curiosité technique et capacité à approfondir l'analyse de systèmes et d'ensembles de données complexes.
 - Grande attention aux détails et capacité à identifier les faiblesses des contrôles, les anomalies et les indicateurs de compromission.
 - Orientation vers la résolution de problèmes et capacité à traduire les problèmes techniques en constats d'audit clairs et en recommandations concrètes.
-

Communication et relations interpersonnelles

- Bonnes compétences en communication écrite et orale, avec la capacité d'expliquer des problématiques techniques et de cybersécurité complexes à des interlocuteurs non techniques.
 - Fort esprit d'équipe et capacité à collaborer avec des auditeurs, des parties prenantes métier et des spécialistes techniques à travers le Groupe.
 - Attitude positive et volontaire, avec un engagement en faveur de l'apprentissage continu et du développement professionnel.
-

Autres exigences

- Haut niveau d'intégrité, de professionnalisme et d'éthique, avec un engagement à préserver la confidentialité et à traiter les informations sensibles avec discrétion.
 - Bonne compréhension de l'évolution du paysage des cybermenaces et capacité à se tenir à jour concernant les nouvelles menaces et les bonnes pratiques en matière de cybersécurité.
 - Volonté de maintenir un haut niveau d'expertise technique grâce à un apprentissage continu, à la pratique et à l'obtention de certifications pertinentes.
-

FORMATION ET CERTIFICATIONS

Formation

- **Licence/Bachelor** en :
 - informatique ;
 - ingénierie ;
 - systèmes d'information ;
 - cybersécurité ;
 - ou domaine connexe.
- Un **Master** constitue un avantage.

Certifications professionnelles

Une ou plusieurs des certifications suivantes sont attendues :

- **CISA** ;
- **CISSP** ;
- **CEH** ;
- **OSCP** ;
- Certification de sécurité **AWS** ;
- Certification de sécurité **Azure** ;
- Certification de sécurité **GCP** ;
- ou certification équivalente.

Des certifications supplémentaires constituent un avantage.

QUALITÉS PERSONNELLES

- Capacité à travailler efficacement sous pression et à respecter les délais.
- Forte curiosité technique et approche pratique (*hands-on*).
- Sensibilité culturelle et capacité à travailler efficacement dans un environnement panafricain diversifié.
- Bonnes capacités de communication écrite et orale.
- Excellentes capacités de gestion du temps et d'organisation.
- Bonnes aptitudes relationnelles.
- Solides capacités d'analyse et orientation vers les résultats, avec une grande attention aux détails et une discipline rigoureuse en matière de documentation.