

Cryptography & Data Protection Specialist

Mission

Le/la Cryptography & Data Protection Specialist est responsable de la gouvernance de la cryptographie et de la protection des données sensibles. Il/elle définit les politiques, standards et contrôles cryptographiques de l'organisation et s'assure de leur conformité avec les exigences NIS2 et les standards de sécurité du Groupe.

Principales responsabilités

- Définir et maintenir la politique de cryptographie de l'organisation.
- Définir les standards relatifs au chiffrement des données at rest, in transit et, lorsque pertinent, in use.
- Définir les exigences concernant les algorithmes, protocoles, clés cryptographiques et certificats.
- Gouverner le cycle de vie des clés cryptographiques.
- Superviser la gouvernance des PKI, certificats et mécanismes de gestion des secrets.
- Définir les exigences de sécurité pour TLS, VPN, chiffrement applicatif, bases de données et infrastructures.
- Identifier et gérer les risques liés à l'utilisation d'algorithmes ou technologies cryptographiques obsolètes.
- Définir une roadmap de migration vers des mécanismes cryptographiques modernes.
- Suivre les risques liés à la cryptographie post-quantique (Post-Quantum Cryptography).
- Participer à la définition des exigences de sécurité dans les projets IT, cloud et applicatifs.
- Réaliser ou coordonner des cryptographic assessments.
- Assurer le suivi des exceptions et dérogations à la politique cryptographique.
- Produire les KPI/KRI cryptographiques à destination du CISO.
- Contribuer aux audits et aux preuves de conformité NIS2/ISO 27001.
- Contribution à la mise en œuvre et au maintien du NIS2 Cybersecurity Framework.
- Mapping des contrôles avec les exigences NIS2.
- Participation aux *NIS2 gap assessments*.
- Définition et maintenance des politiques, standards et procédures.
- Suivi des exceptions et risques acceptés.
- Définition des KPI/KRI.
- Reporting régulier au CISO.
- Coordination avec IT, Infrastructure, Cloud, Engineering, Risk, Legal, Compliance et Internal Audit.
- Gestion des plans de remédiation.
- Préparation et maintien des preuves d'audit.
- Contribution aux exercices de résilience et de gestion de crise.
- Veille réglementaire et adaptation du framework aux nouvelles exigences.

Profil recherché

- 5+ ans d'expérience en cybersécurité, avec une spécialisation en cryptographie, PKI ou data protection.
- Très bonne connaissance de la cryptographie appliquée en entreprise.
- Bonne compréhension de TLS, PKI, certificats, HSM, secrets management et key management.
- Expérience en définition de politiques et standards de sécurité.
- Connaissance de NIS2 et ISO 27001.
- Capacité à traduire des sujets techniques complexes en exigences de gouvernance.
- Bonne capacité de communication avec les équipes architecture, infrastructure, cloud et développement.

Certifications appréciées

- CISSP
- CCSP
- GIAC
- ISO 27001
- Certifications PKI / cryptographie