

Vulnerability & Incident Management Specialist

Mission

Le/la Vulnerability & Incident Management Specialist est responsable de la gouvernance des processus de gestion des vulnérabilités et des incidents de sécurité dans le cadre de NIS2. Il/elle définit le cadre de contrôle, assure le suivi des risques et plans de remédiation et veille à ce que les processus opérationnels soient alignés avec les exigences réglementaires et les politiques de sécurité de l'entreprise.

Principales responsabilités

- Définir et maintenir le framework de gouvernance de la gestion des vulnérabilités.
- Définir les exigences en matière de scanning, identification, qualification, priorisation et remédiation des vulnérabilités.
- Mettre en place une gouvernance basée sur le risque et la criticité des actifs.
- Définir et suivre les SLA de remédiation des vulnérabilités.
- Produire des KPI/KRI à destination du CISO et du management.
- Gouverner le processus de gestion des incidents de cybersécurité.
- Définir les exigences relatives à la détection, qualification, escalade, traitement et clôture des incidents.
- S'assurer que les processus d'incident management permettent de répondre aux obligations NIS2 en matière de notification et de reporting.
- Participer aux exercices de crise et de cyber incident.
- Assurer le suivi des lessons learned et des plans d'amélioration.
- Contrôler la bonne application des politiques et standards de sécurité.
- Préparer les éléments nécessaires aux audits internes, externes et réglementaires.
- 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, idéalement en vulnerability management, incident management ou cyber governance.
- Connaissance des frameworks NIS2, ISO 27001.
- Compréhension des processus de vulnerability management et incident response.
- Expérience dans un environnement complexe/international.

- Capacité à travailler avec les équipes SOC, infrastructure, cloud, IT et métiers.
- Excellentes capacités d'analyse et de reporting.
- Très bonnes capacités de communication avec des interlocuteurs techniques et exécutifs.

Certifications appréciées

- CISSP
- CISM
- ISO 27001 Lead Implementer / Lead Auditor
- GIAC / GCIH / GCIA
- Certifications liées au vulnerability management