

SOC & SIEM Specialist

Mission

Le/la SOC & SIEM Specialist est responsable de la gouvernance des capacités de détection et de monitoring de cybersécurité. Il/elle veille à ce que les capacités SOC/SIEM permettent à l'organisation de détecter, analyser et escalader efficacement les événements de sécurité et de répondre aux exigences NIS2.

Principales responsabilités

- Définir le framework de gouvernance SOC.
- Définir les exigences minimales en matière de monitoring et de détection.
- Gouverner la stratégie SIEM et la collecte des logs de sécurité.
- Définir les exigences de logging & monitoring pour les systèmes critiques.
- Définir les exigences de rétention, intégrité et protection des logs.
- Définir et suivre les use cases de détection.
- Assurer le suivi de la couverture des actifs critiques par le SOC/SIEM.
- Mettre en place des KPI/KRI sur la capacité de détection.
- Suivre les métriques telles que :
 - detection coverage
 - MTTD
 - MTTA
 - alert volume
 - false positive rate
 - critical use-case coverage
- Challenger la performance des prestataires SOC/MSSP.
- Assurer la gouvernance des processus d'escalade vers Incident Response et Crisis Management.
- Participer aux exercices de cyberdéfense et simulations d'incidents.
- Vérifier l'alignement des capacités SOC avec les exigences NIS2.
- Assurer le suivi des gaps et plans de remédiation.
- Contribuer aux audits et à la préparation des preuves de conformité.
- 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 SOC, SIEM, detection engineering ou cyber governance.

- Bonne compréhension des architectures SOC.
- Expérience avec des solutions SIEM, en particulier Splunk, et idéalement XDR/SOAR.
- Bonne connaissance de la détection basée sur les logs et événements.
- Connaissance de MITRE ATT&CK.
- Bonne compréhension des processus Incident Response.
- Expérience en gouvernance et gestion de fournisseurs SOC/MSSP.
- Connaissance de NIS2 et ISO 27001.
- Capacité à dialoguer avec des équipes SOC très techniques tout en restant orienté gouvernance.

Certifications appréciées

- CISSP
- CISM
- GIAC
- Splunk
- MITRE ATT&CK training/certification