

PAM & IAM Specialist

Mission

Le/la PAM & IAM Specialist est responsable de la gouvernance des identités et des accès, avec un focus particulier sur les comptes privilégiés. Il/elle définit les politiques et contrôles IAM/PAM, assure le suivi des risques et veille à leur alignement avec les exigences NIS2.

Principales responsabilités

- Définir et maintenir la politique IAM/PAM.
- Définir les principes de Least Privilege et Need-to-Know.
- Gouverner les processus de gestion du cycle de vie des identités.
- Définir les exigences relatives au Joiner/Mover/Leaver process.
- Gouverner les accès aux systèmes critiques.
- Définir les exigences relatives aux comptes privilégiés.
- Superviser le framework PAM et les contrôles associés.
- Définir les exigences concernant :
 - MFA
 - privileged accounts
 - service accounts
 - emergency/break-glass accounts
 - access reviews
 - segregation of duties
- Définir et suivre les campagnes de User Access Reviews.
- Assurer la gouvernance des comptes techniques et comptes de service.
- Identifier et suivre les risques liés aux privilèges excessifs.
- Définir les KPI/KRI IAM/PAM.
- Suivre la couverture PAM des systèmes critiques.
- Challenger les architectures IAM et PAM proposées par les équipes IT.
- Assurer l'intégration des exigences IAM/PAM dans les projets.
- Contribuer aux audits NIS2, ISO 27001 et aux contrôles internes.
- 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 IAM, PAM ou Information Security.
- Solide compréhension des architectures IAM modernes.

- Bonne connaissance de MFA, SSO, RBAC, ABAC, LDAP/AD, Entra ID/Azure AD,...
- Expérience de solutions PAM.
- Bonne compréhension du Zero Trust et du Least Privilege.
- Expérience en définition de politiques et standards de sécurité.
- Connaissance de NIS2 et ISO 27001.
- Capacité à travailler avec les équipes infrastructure, cloud, application et audit.

Certifications appréciées

- CISSP
- CISM
- CIAM
- CyberArk / BeyondTrust / Delinea certifications
- Microsoft Identity certifications