

FICHE MÉTIER : Responsable de la Sécurité des Systèmes d'Information (CISO)

1. Synthèse du poste

Le **Chief Information Security Officer (CISO)** est le garant de la protection des données et de la disponibilité des systèmes d'information de l'entreprise. Il définit, met en œuvre et pilote la politique de sécurité (PSSI) tout en assurant un rôle de conseil stratégique auprès de la Direction Générale.

2. Missions Principales

Définir, piloter et garantir la stratégie de sécurité des systèmes d'information afin de protéger les actifs numériques, les données sensibles et la continuité des opérations de l'organisation.

Stratégie et Gouvernance

- Élaborer et maintenir la **Politique de Sécurité des Systèmes d'Information (PSSI)**.
- Assurer la veille technologique et réglementaire (RGPD, NIS2, ISO 27001, etc.).
- Définir les indicateurs de performance (KPI) et de risque (KRI) pour le reporting Board.

Gestion des Risques et Incidents

- Réaliser des analyses de risques sur les projets métiers.
- Piloter le **Plan de Continuité d'Activité (PCA)** et le **Plan de Reprise d'Activité (PRA)**.
- Diriger la cellule de crise en cas de cyberattaque ou de fuite de données.
- Représenter l'entreprise auprès des autorités (ANSSI, CNIL, ACPR, etc.).
- Négocier avec les assureurs cyber et optimiser le transfert de risque

Culture et Sensibilisation

- Concevoir des programmes de formation pour les collaborateurs (phishing, bonnes pratiques).
- Promouvoir la "Security by Design" auprès des équipes de développement et IT.

3. Profil et Formation

- Formation : Bac+5 (École d'ingénieur ou Master spécialisé en cybersécurité).
- Expérience : Généralement 5 à 10 ans d'expérience en IT/Sécurité ou Audit.
- Certifications (un plus) : CISSP, CISM, CISA ou certifications ISO 27001 Lead Implementer/Lead Auditor, ISO 27005 Risk Manager, EBIOS RISK Manager.
- Parcours le plus fréquent : Ingénieur systèmes/réseaux → pentest / SOC → consultant senior → RSSI → CISO

4. Compétences Requises

Hard Skills (Techniques)	Soft Skills (Comportementales)
Audit & Normes : ISO 27001, EBIOS RM, NIST.	Communication : Capacité à vulgariser le risque technique en risque business.
Technique : Cloud Security, Réseaux, Cryptographie.	Leadership : Influence et diplomatie auprès des directions métiers.
Droit : Maîtrise du cadre juridique lié aux données.	Gestion du stress : Réactivité et sang-froid en situation de crise.

5. Indicateurs de Succès (KPIs)

- Taux de conformité aux audits internes/externes.
- Temps moyen de détection et de réponse aux incidents (MTTD / MTTR).
- Pourcentage de collaborateurs sensibilisés à la cybersécurité.

6. Positionnement hiérarchique

Rattachement possible à : Direction Générale, DSI, Direction des Risques, Direction Conformité

Interaction forte avec : IT, Juridique, Audit interne, Métiers, Direction.

7. Débouchés

CISO Groupe, Directeur Cybersécurité, Risk & Security Director, Consultant CISO / Virtual CISO, Expert GRC.

8. Secteurs les plus demandeurs

Banque / Assurance, Industrie (surtout OT/ICS), Luxe, Énergie, Santé, Retail & e-commerce, SaaS / Scale-up, Secteur public / OIV/OSE, cabinets de conseil & ESN spécialisés cyber.