

## Fonction

# RESPONSABLE ANTICIPATION DETECTION ET REPONSE IV.A (H/F)

## Évolutions possibles

### Au sein du métier

- [RSSI IV.A \(H/F\)](#)
- [RSSI IV.B \(H/F\)](#)
- [ADMINISTRATEUR SOLUTIONS DE SECURITE III.3 \(H/F\)](#)
- [ADMINISTRATEUR SOLUTIONS DE SECURITE IV.A \(H/F\)](#)
- [ANALYSTE DE LA MENACE III.3 \(H/F\)](#)
- [ANALYSTE DE LA MENACE IV.A \(H/F\)](#)
- [ANALYSTE REPONSE INCIDENT III.3 \(H/F\)](#)
- [ANALYSTE REPONSE INCIDENT IV.A \(H/F\)](#)
- [ANALYSTE SOC III.2 \(H/F\)](#)
- [ANALYSTE SOC III.3 \(H/F\)](#)
- [ANALYSTE SOC IV.A \(H/F\)](#)
- [CORRESPONDANT SECURITE III.2 \(H/F\)](#)
- [CORRESPONDANT SECURITE III.3 \(H/F\)](#)
- [CORRESPONDANT SECURITE IV.A \(H/F\)](#)
- [EXPERT CYBER IV.B \(H/F\)](#)
- [PENTESTEUR III.3 \(H/F\)](#)
- [PENTESTEUR IV.A \(H/F\)](#)
- [RESPONSABLE ANTICIPATION DETECTION ET REPONSE IV.A \(H/F\)](#)
- [RESPONSABLE ANTICIPATION DETECTION ET REPONSE IV.B \(H/F\)](#)
- [RESPONSABLE PROJET DE SECURITE III.3 \(H/F\)](#)
- [RESPONSABLE PROJET DE SECURITE IV.A \(H/F\)](#)
- [EXPERT CYBER IV.A \(H/F\)](#)

## Raisons d'être

Le Responsable détection et réponse à incidents est responsable d'une équipe de réponse aux incidents de sécurité ciblant les systèmes d'information de l'organisation. Il est également en charge, lorsque applicable, de la gestion des activités d'un SOC (Security Operation Center).

Il s'assure de la bonne exécution des investigations et de la coordination des parties prenantes lors d'un incident de sécurité. Il contribue à la préparation de l'organisation pour garantir une réponse efficace. Lors d'incidents à fort impact, le Responsable détection et réponse à incidents est amené à interagir avec l'équipe de gestion de crise.

Il anime une équipe en charge de l'anticipation et de la veille sur les menaces cyber. Il contribue à l'amélioration du niveau de cybersécurité en recommandant les mesures techniques et organisationnelles à mettre en œuvre pour contrer ces menaces.

Il met également en place le service de détection de ces incidents de sécurité, valide la bonne exécution des processus de supervision et de gestion des événements de sécurité et assure un reporting complet et précis des indicateurs clés. Il définit et pilote le plan d'amélioration des services du SOC.

Dans le cadre de ses activités liées à la réponse à incidents, le Responsable détection et réponse à incidents peut être amené à contribuer à la gestion d'incidents liés à des raisons autres que la sécurité des SI, comme par exemple la fraude via des moyens informatiques.

Pour suivre l'évolution des tendances, il pourra être amené à développer des compétences en machine learning et en threat intelligence afin de renforcer les capacités de détection.

Dans le cadre de ses activités liées à la réponse à incidents, le Responsable détection et réponse à incidents peut être amené à contribuer à la gestion d'incidents liés à des raisons autres que la sécurité des SI, comme par exemple la fraude via des moyens informatiques.

Une évolution professionnelle est possible vers les fonctions de RSSI – Expert Cyber

## Missions

## Conduite d'équipe

### Donner du sens aux missions

- Piloter l'équipe avec des objectifs et indicateurs de performance pertinents
- Développer les compétences individuelles et collectives au sein de l'équipe
- Assurer l'employabilité des collaborateurs

## Pilotage des opérations

- Planifier et organiser les opérations quotidiennes de la cellule de réponse à incidents et du SOC
- Assurer un appui opérationnel à la gestion de crise de sécurité en cas d'incidents de sécurité majeurs
- Assurer et coordonner les relations entre les équipes de réponse à incidents et les équipes du SOC, notamment en situation de crise pour coordonner les différentes équipes de sécurité opérationnelle

## Anticipation

- S'appuyer sur les services de veille sur les menaces (« threat intelligence ») pour tenir compte des groupes d'attaquants existants, de leurs méthodes d'attaques et de leurs motivations
- Informer les équipes en charge de la sécurité des nouvelles menaces importantes et recommander des mesures tactiques pour les contrer
- Construire et maintenir des relations de confiance et d'échange avec les réseaux de CSIRT français et étrangers ainsi qu'avec les organismes gouvernementaux
- Participer aux exercices de préparation à la gestion de crise de cybersécurité

## Réponse à incident

- Élaborer et tenir à jour le processus d'intervention en cas d'incident majeur de sécurité ainsi que toutes les ressources nécessaires (outillage, procédure, etc.), vérifier que les prérequis techniques et documentaires sont en place et tenus à jour
- S'assurer que les parties prenantes connaissent leur rôle dans la gestion des incidents de sécurité
- S'assurer la bonne exécution du processus de réponse à incident depuis la détection jusqu'à la résolution de l'incident ; suivre et coordonner les actions de remédiation
- Organiser les retours d'expérience concernant les incidents pour capitaliser et définir des actions d'amélioration

## Stratégie de prévention et de détection

- Définir la stratégie du SOC, assurer la cohérence technique, prendre en compte les exigences réglementaires
- Définir et mettre en œuvre les outils du SOC pour la collecte des évènements, l'accès aux plateformes de sécurité, la recherche d'évènements suspects, la gestion des alertes, les workflows de suivi d'incidents de sécurité
- Alimenter la stratégie de détection à partir d'une vision globale de la nature et du niveau de vulnérabilité du SI
- Définir les cas d'usages de détection et les intégrer dans les outils de détection
- Définir et mettre en place les processus de notification et d'escalade
- Évaluer et valider l'efficacité des outils déployés dans le SOC et conduire les plans d'action correctifs nécessaires le cas échéant
- Créer des synergies avec les autres équipes de sécurité en partageant les informations sur les menaces identifiées (en interne comme en externe)

## Compétences

### Comportementales Socles

#### Orientation client

Enrichir l'expérience client en adoptant une posture de service et de conseil et développer une relation de confiance durable. Anticiper, analyser, comprendre les besoins et attentes de ses clients pour apporter des réponses personnalisées. S'appliquer à améliorer la satisfaction client et mesurer son niveau de satisfaction.

#### Culture du changement et de l'innovation

Encourager et accompagner le changement et les initiatives d'amélioration dans un environnement complexe et incertain. Expérimenter, tester, évaluer en s'appuyant sur de nouvelles méthodes, y compris numériques. Comprendre et susciter l'innovation en remettant en question les usages et en osant être pionnier. Etre dans une dynamique d'identification et d'apport de nouveautés dans son

activité en osant sortir du cadre pour penser le problème en dehors de ses limites et de ses moyens lorsque la situation le demande.

#### Coopération et ouverture

Construire et faire vivre des réseaux informels ou structurés d'individus ou de groupes en s'appuyant sur les outils collaboratifs comme les réseaux sociaux internes. Participer individuellement à l'atteinte d'un résultat collectif en favorisant l'entraide et le partage de connaissances. Savoir fédérer les parties prenantes d'un projet autour d'un objectif commun et établir des partenariats. Faire preuve d'écoute active vis-à-vis de ses interlocuteurs et prendre en compte leurs problématiques et les objections émises dans ses actions et prises de décision. Etre ouvert(e) d'esprit et curieux(se) au sein de son environnement.

#### Orientation résultats

Engager des actions et mobiliser en toute autonomie des ressources (financières, matérielles, techniques, numériques et humaines) pour atteindre des performances durables dans le respect des principes éthiques, de qualité de vie et de RSE. Savoir être proactif et fixer, pour soi et/ou pour d'autres, des objectifs ambitieux et exploiter des opportunités pour aller au-delà des attendus.

### Cyber Sécurité

#### Gestion de crise cyber

Elaborer, mettre à l'essai et mettre en oeuvre les plans permettant à l'entreprise de se préparer et de faire face à la survenance d'une crise cyber (ex : rôles et responsabilités, organisation d'exercices de crise, pilotage effectif de crise cyber, etc.)

#### Vulnérabilités des environnements

Maitriser les principes, méthodes et outils d'évaluation des vulnérabilités et identifier les contre-mesures appropriées

#### Techniques d'attaque et d'intrusion

Maitriser les techniques employées par les attaquants pour compromettre un Système d'Information (ex : phishing via les réseaux sociaux, exploitation d'une vulnérabilité de l'OWASP), à toutes les étapes de la kill chain (reconnaissance, intrusion, exploitation, augmentation de priviléges, mouvement latéral, persistance, exfiltration, etc.)

#### Sécurité des systèmes d'exploitation

Maitriser la sécurité des systèmes d'exploitation (poste de travail, serveur, mobile) connus sur le marché (Windows, Linux, iOS, Android, etc.) : méthodes de durcissement, connaissance des outils de sécurité natifs, connaissance des principales attaques.

#### Sécurité des réseaux et protocoles

Mettre en place, maintenir et améliorer les pratiques établies en matière de sécurité des réseaux (ex : NIPS, anti-malware, restriction/empêchement dispositifs externes, filtres anti-spam) et des protocoles.

Maitriser des outils d'analyse de réseau pour identifier les vulnérabilités (ex : fuzzing, nmap, etc.).

Reconnaitre et interpréter une activité réseau malveillante dans le trafic. Maitriser l'utilisation d'analyseurs de protocoles. Maitriser la configuration et l'utilisation des composants de protection des réseaux (par exemple, pare-feu, VPN, systèmes de détection des intrusions dans les réseaux)

#### Investigation cyber

Maitriser les techniques et la démarche opérationnelle d'une investigation cyber au service de la détection ou de la réponse à incidents, permettant de mettre en évidence des preuves d'une attaque cyber en cours ou passée (analyse post-mortem, analyse de flux réseaux, analyse de journaux).

S'assurer du respect du cadre légal, ainsi que de l'intégrité et la confidentialité des données à chaque investigation

### Efficacité professionnelle

#### Synthèse

Savoir trier, analyser et isoler les informations essentielles des informations accessoires. Consolider des informations pour réaliser une synthèse.

#### Veille / innovation / tendances

Se tenir informé(e) des tendances, des évolutions technologiques et des innovations en vigueur dans son domaine d'intervention en lien avec les enjeux de l'entreprise et attentes des clients / partenaires et à les intégrer dans son activité.

### Techniques SI

#### Gestion des incidents et des problèmes

Identifier et qualifier les incidents et les problèmes. Maîtriser la méthode ITIL / GDI. Gérer la résolution des incidents (Priorisation/arbitrage, mobilisation des moyens et compétences nécessaires, escalade, activation mode dégradé...). Réaliser un rapport sur les incidents et les problèmes dans le cadre des processus et contrats définis.

#### Gestion des situations de tension organisationnelle ou humaine

Gestion des situations de tension organisationnelle ou humaine

## Famille

---

### Filière

---

### Métier

---

### **Répartition des effectifs**

- 
- 

Groupe - siège

### **Effectif de la fonction**

De 1 à 9