

## Fonction

# ANALYSTE REPONSE INCIDENT 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

L'analyste réponse aux incidents de sécurité intervient généralement au sein d'un CERT (Computer Emergency Response Team) ou CSIRT (Computer Security Incident Response Team).

En cas de soupçons sur une activité malveillante ou d'attaque au sein du système d'information, l'analyste réponse aux incidents de sécurité analyse les symptômes et réalise les analyses techniques sur le système d'information.

Il identifie le mode opératoire de l'attaquant et qualifie l'étendue de la compromission. Il fournit des recommandations de remédiation pour assurer l'assainissement et le durcissement des systèmes attaqués

Un analyste réponse aux incidents de sécurité peut être spécialisé en tant que :

- Analyste système
- Analyste réseau
- Analyste de codes malveillants

Une évolution professionnelle est possible vers les fonctions d'Expert Cyber - Analyste SOC - Pentesteur - Administrateur Solution Sécurité - Correspondant Sécurité de projet

## Missions

### Anticipation

- Réaliser une veille sur les nouvelles vulnérabilités, sur les nouvelles technologies et sur les méthodes des attaques relatives aux différents composants du SI
- Alimenter les bases de renseignement sur les menaces (« threat intelligence »)
- Maintenir et développer des outils d'investigation

## Analyse des incidents

- Collecter les informations techniques d'un large ensemble de systèmes d'information, réaliser la recherche d'indicateurs de compromission
- Analyser les relevés techniques réalisés, afin d'identifier le mode opératoire et l'objectif de l'attaquant et de qualifier l'étendue de la compromission
- Aider à évaluer les risques et les impacts métiers associés
- Collecter les preuves en vue d'un dépôt de plainte
- Rédiger des rapports d'investigation

## Conseil

- Préconiser des mesures de contournement et de remédiation de l'incident (assainissement et durcissement)
- Préconiser des mesures d'amélioration des capacités d'analyse (extraction des indicateurs de compromission)
- Préparer des rapports

# 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

## Politiques de cybersécurité

Créer, intégrer et appliquer des politiques qui répondent aux objectifs de sécurité de l'organisation. Maitriser le corpus documentaire cybersécurité existant.

## 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.)

## 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.

## **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.

### **Cartographie, principes et composants de l'architecture technique et de production**

Maîtriser les cartographies, principes et composants de l'architecture technique et de production : - Cartographie réseaux, impression, services de messagerie, bus applicatif... - Architecture de partage, serveurs et outils distribués, implémentation CCU et RSE - SI internes/externes et cartographies des déploiements des services sur le Cloud - Référentiels d'entreprise - Urbanisation à l'échelle de l'entreprise, vision globale - Coexistence des processus internes et de l'outsourcing (BPO, ITO)

### **Cartographie, principes et composants de l'architecture fonctionnelle et applicative**

Maîtriser la cartographie, les principes et composants de l'architecture fonctionnelle et applicative : - Cartographies : fonctionnelles, applicatives, de flux, de référentiel et d'utilisateurs - Couverture fonctionnelle d'un domaine Métier et des éléments communs aux autres domaines - Référentiels de données et applications partagées par plusieurs domaines

## **Famille**

---

## **Filière**

---

## **Métier**

---

## **Répartition des effectifs**

- □

Groupe - siège

## **Effectif de la fonction**

De 10 à 49