



<https://latribunelibre.com/emploi/soc-analyst-f-h-6>

## SOC Analyst F/H

### Description

#### Analyste Sécurité Opérationnelle / SOC Analyst

- Date de démarrage : 01/12/2025
- Localisation Paris (75)
- Télétravail 3 fois/semaine

### Objectif du poste

Intégré(e) au sein de l'équipe Sécurité Opérationnelle, vous contribuez à la surveillance, à la détection et au traitement des incidents de sécurité.

Vous intervenez sur l'ensemble du périmètre du groupe (solutions SaaS, infrastructures internes, environnements Cloud et On-Prem) à travers les outils du SOC : EDR/MDR CrowdStrike, SIEM et vulnérabilités Rapid7 (InsightIDR / InsightVM), proxy/ZTNA Netskope, DLP et gouvernance des données Varonis, sécurité Active Directory Semperis, et PAM Wallix.

Votre rôle vise à renforcer la détection, la corrélation, et la réponse opérationnelle aux menaces, tout en contribuant à la cyber-résilience du groupe.

### Responsabilités principales

#### 1. Détection et analyse des événements de sécurité

- Surveillance continue des alertes issues des solutions : EDR/MDR CrowdStrike, SIEM Rapid7, Netskope, Varonis, Semperis, Wallix, DLP, IDS/IPS, logs Cloud.
- Corrélation des événements et identification des patterns d'attaque multi-vecteurs.
- Qualification et priorisation des alertes (faux positifs / réels incidents).
- Investigation technique et remontée d'IOC, indicateurs de compromission, tendances.
- Participation à la chasse aux menaces (« threat hunting ») en lien avec le MSSP/MDR.

#### 2. Gestion des incidents

- Prise en charge et documentation des incidents jusqu'à leur résolution.
- Coordination avec les équipes internes (infra, réseau, dev, produit) et le MSSP.
- Contribution à la communication interne (reporting, post-mortem, indicateurs).
- Application des playbooks de réponse à incident et proposition d'améliorations.

### Organisme employeur

NATAN CONSULTING

### Type de poste

Temps plein

### Secteur

CONSEIL EN SYSTÈMES ET LOGICIELS INFORMATIQUES

### Lieu du poste

France

### Salaire de base

57000 € - **Salaire de base**

65000 €

### Date de publication

19 octobre 2025 à 13:06

### Valide jusqu'au

16.11.2025

### 3. Amélioration continue du SOC

- Enrichissement des règles de détection et des tableaux de bord Rapid7 / Netskope.
- Proposition et intégration de nouveaux cas d'usage SIEM / DLP / EDR.
- Participation à la construction de la base de connaissance du SOC (retours d'expérience, procédures, lessons learned).
- Contribution à l'automatisation via scripts, APIs ou intégration SOAR.

### 4. Support à la conformité et à la gouvernance sécurité

- Contribution à la démonstration de conformité ISO 27001, DORA et exigences clients.
- Documentation des incidents, alertes et indicateurs pour les audits internes/externes.
- Veille sur les menaces et vulnérabilités affectant le périmètre SaaS et Cloud.

## Qualifications

### Compétences techniques recherchées

- Maîtrise des environnements : CrowdStrike Falcon, Rapid7 InsightIDR / InsightVM, Netskope NG-SWG & ZTNA, Varonis DLP, Semperis Directory Services Protector, Wallix Bastion, AWS Security Hub (apprécié).
- Bonne compréhension des logs Windows, Linux, Active Directory, Cloud et réseau.
- Connaissance des frameworks MITRE ATT&CK, NIST IR, ISO 27035.
- Scripting (Python, PowerShell ou équivalent) pour automatiser l'analyse.
- Compréhension du fonctionnement des pipelines CI/CD et des risques DevSecOps (bonus).

### Compétences méthodologiques et relationnelles

- Autonomie, rigueur, capacité à travailler dans un environnement exigeant.
- Aisance dans la communication technique et la vulgarisation auprès des équipes métiers.
- Capacité à prioriser, synthétiser et documenter efficacement.
- Esprit d'équipe, proactivité et curiosité technique.