https://latribunelibre.com/emploi/analyste-soc-splunk-f-h-2

Analyste SOC Splunk F/H

Organisme employeur
AGH CONSULTING

Type de poste
Temps plein

Secteur
INGÉNIERIE, ÉTUDES TECHNIQUES

Lieu du poste
92050, NANTERRE, NANTERRE, France

Date de publication
8 octobre 2025 à 11:06

Valide jusqu'au
07.11.2025

Description

Au sein du **CyberSOC** d'un grand groupe, vous intégrerez une équipe d'experts dédiée à la supervision, la détection et la réponse aux incidents de sécurité. Dans un contexte de forte montée en puissance des menaces et d'évolution constante des technologies, l'objectif est d'assurer une surveillance proactive et une amélioration continue des dispositifs de sécurité, en s'appuyant sur des outils et des méthodologies à la pointe de la cybersécurité.

Vous interviendrez dans un environnement exigeant, orienté vers la **performance, la réactivité et l'innovation**, au sein d'une cellule où la collaboration et le partage des connaissances sont au cœur des pratiques quotidiennes.

Missions principales

Rattaché(e) au responsable du CyberSOC, vous participerez activement à la détection, l'investigation et la résolution d'incidents de sécurité, tout en contribuant à l'amélioration des processus et des outils de surveillance. Vos principales missions incluront :

- **Analyse et traitement des incidents de sécurité :**
  - Surveiller en temps réel les alertes issues des outils de supervision (Splunk, SIEM, EDR, IDS/IPS, etc.).
  - Identifier, qualifier et prioriser les incidents selon leur niveau de criticité.
  - Réaliser des investigations approfondies sur les événements suspects à l'aide de **Splunk** et d'autres outils d'analyse.
  - Proposer et mettre en œuvre des mesures correctives ou préventives pour réduire les risques de récurrence.
- **Optimisation et automatisation :**
  - Améliorer en continu les règles de détection et les corrélations dans Splunk.
  - Développer des tableaux de bord, rapports et alertes adaptés aux besoins opérationnels et stratégiques.
  - Contribuer à des projets d'innovation autour de **Splunk Enterprise Security**, du **Risk-Based Alerting (RBA)** et du **Machine Learning Toolkit (MLTK)** pour renforcer la pertinence des détections et automatiser certaines tâches répétitives.

- **Threat Hunting et veille de sécurité :**
    - Mener des campagnes de **threat hunting** afin d'identifier les menaces avancées non détectées par les systèmes automatiques.
    - Exploiter les indicateurs de compromission (IoC) issus de différentes sources pour enrichir les scénarios de détection.
    - Effectuer une veille active sur les nouvelles vulnérabilités, techniques d'attaque et outils défensifs.
- **Documentation et capitalisation :**
    - Alimenter les bases de connaissances internes via **Confluence, Git ou SharePoint**.
    - Rédiger des rapports d'incidents détaillés et des comptes rendus d'investigation.
    - Participer à la mise à jour des procédures et à la formalisation des bonnes pratiques SOC.

Profil du candidat

Compétences clés : Splunk, SOC, CyberSOC, Splunk Power User, détection et réponse aux incidents, threat hunting, analyse de logs, corrélation d'événements, sécurité opérationnelle, reporting.

Qualifications

Profil recherché

De formation Bac+3 à Bac+5 en informatique ou cybersécurité, vous justifiez d'une première expérience significative (stage, alternance ou emploi) au sein d'un **SOC ou CyberSOC**. Vous êtes passionné(e) par la sécurité opérationnelle, l'investigation technique et la recherche de menaces.

Compétences techniques attendues :

- Maîtrise avancée de **Splunk** (requêtes SPL, tableaux de bord, corrélations, automatisations).
- Bonne compréhension des concepts de **SIEM**, **SOC**, **threat hunting** et **incident response**.
- Connaissances solides en **réseaux, systèmes, logs applicatifs** et protocoles de sécurité.
- Une certification **Splunk Power User** ou **Splunk Core Certified User** est un plus apprécié.
- Familiarité avec les outils de documentation (Confluence, Git, SharePoint).

Compétences comportementales :

- Esprit d’analyse, rigueur et sens du détail.
- Curiosité technique, goût pour l’innovation et le travail en équipe.
- Sens du service et de la confidentialité.