EXPERT SÉCURITÉ SIEM – SPLUNK

Nous recherchons un Expert Sécurité SIEM pour renforcer notre dispositif de supervision sécurité. Vous serez en charge de l'ingénierie, de la configuration et de l'optimisation de la plateforme Splunk, ainsi que de l'analyse des logs et de la mise en place de règles de détection pertinentes.

Vos responsabilités

- Installation, configuration et maintien de la solution Splunk
- Conception et optimisation des requêtes de recherche et tableaux de bord
- Création et affinage de règles de détection de menaces (notamment via SPL)
- Analyse qualitative des logs (contenu, pertinence, verbosité)
- Intégration de nouvelles sources de données de sécurité
- Automatisation des déploiements et configurations via Ansible / Python
- Support aux équipes SOC ou clients dans la compréhension et l'exploitation de la solution

Lieu de travail : IDF
Ambiance conviviale et bienveillante

Votre profil

- Formation Bac+5 en cybersécurité, informatique ou systèmes/réseaux
- Expérience confirmée dans la gestion ou l'ingénierie SIEM (Splunk)
- Solide expertise en analyse de logs et détection d'incidents
- Bonne maîtrise de Splunk Search Processing Language (SPL)
- Pratique de l'automatisation avec Ansible / Python
- Certifications Splunk (ex. Splunk Core Certified Power User, Admin, Architect) appréciées
- Rigueur, capacité d'analyse, autonomie et sens de l'amélioration continue

Environnement technique :

- Splunk
- Ansible
- Python
- Environnements logs : multi-sources (réseaux, endpoints, serveurs, cloud…)

En bref…

Formind, leader français indépendant en cybersécurité avec plus de 300 consultants, a connu une croissance soutenue depuis sa création en 2010. Qualifié PASSI, Formind accompagne ses clients dans toutes les problématiques de cybersécurité avec une approche axée sur le risque, un pragmatisme fort, et des valeurs d'engagement. Basé à Paris, Formind s'est étendu dans plusieurs villes en France, au Maroc, en Espagne et au Canada. Formind est également fier d'être reconnu Happy@Work pour la 8e année consécutive.

Envoyez votre candidature à **recrutement@formind.fr**