



<https://latribunelibre.com/emploi/expert-e-securite-f-h-3>

Expert-e securite F/H

Description

Au sein de l'équipe CERT/SOC de CDC Informatique, vous intégrerez l'activité outillage du SOC (composée de 3 internes). Vous serez en charge de l'administration ainsi que de l'amélioration des outils au profit de la détection et le traitement des incidents de cybersécurité.

RESPONSABILITES :

Votre objectif sera d'assurer, maintenir et améliorer dans le temps l'outillage du SOC, via notamment les activités suivantes :

Administration des outils comprenant Splunk Enterprise, Palo Alto Cortex XSOAR avec les montées de version, l'intégration de contenu, les revues de droits, le débogage, etc. ;

Création et revue de scénarios (alertes) liés à la surveillance de l'outillage et leur automatisation ;

Création et suivi des procédures de traitement et de la documentation associée ;

Développement CI/CD pour une gestion efficace des outils ;

Amélioration continue de nos outils et procédures ;

Reporting au management.

ENVIRONNEMENT FONCTIONNEL ET TECHNIQUE :

Expertise sur la solution Splunk Enterprise

Maîtrise des expressions régulières

Développement en Python

Connaissances de Git et des principes de » versioning «

Connaissances en automatisation et CI/CD

Connaissances sur Ansible

Qualifications

Formation : Bac +5 en école d'ingénieur ou université spécialisé informatique

Le candidat devra démontrer d'une expérience significative de 3 ans minimum en tant que :

- Administrateur Splunk

- Ou expert technique cumulant plusieurs des autres aspects attendus avec un fort intérêt pour Splunk.

Une maîtrise ou expérience d'administration de la solution Palo Alto XSOAR sera un plus.

Une bonne connaissance de l'anglais écrit et oral dans un environnement technique est nécessaire.

Organisme employeur

CDC Informatique

Type de poste

Temps plein

Secteur

ACTIVITÉS DES SIÈGES
SOCIAUX

Lieu du poste

92007, BAGNEUX, BAGNEUX,
France

Salaire de base

50000 € - **Salaire de base**
55000 €

Date de publication

4 mars 2026 à 12:03

Valide jusqu'au

03.04.2026