https://latribunelibre.com/emploi/ingenieur-cybersecurite-f-h-42

Ingénieur cybersécurité F/H

Organisme employeur
RECRUTONSENSEMBLE

Type de poste
Temps plein

Secteur
CONSEIL POUR LES AFFAIRES ET AUTRES CONSEILS DE GESTION

Lieu du poste
83137, TOULON, TOULON, France

Salaire de base
30000 € - **Salaire de base**
56000 €

Date de publication
20 octobre 2025 à 09:07

Valide jusqu'au
19.11.2025

Description

Expert(e) en cybersécurité ayant une forte expérience sur les infrastructures cloud (AWS), les infrastructures on-prem (VMWare, Palo Alto, Cisco, Fortinet, F5), les stack applicatives (Java, Php, Angular).

Une connaissance des meilleures pratiques de l'ISO 2700x est attendue afin d'accompagner les équipes dans l'alignement du système de management de la sécurité avec les directives NIS2.

Les activités de sécurité opérationnelle sont les suivantes :

1. **Surveillance et monitoring :** Supervision du système d'information, analyse des logs de sécurité, monitoring des SIEM et outils de détection, veille technologique sur les nouvelles menaces.
2. **Détection et analyse d'incidents :** Triage des alertes et classification par criticité, analyse des IOCs, corrélation d'événements suspects, investigation approfondie des incidents.
3. **Réponse aux incidents :** Isolement des systèmes compromis, éradication des menaces identifiées, restauration des services, communication avec les parties prenantes.
4. **Threat hunting proactif :** Recherche active de menaces non détectées, analyse comportementale des utilisateurs/systèmes, exploitation du threat intelligence, développement d'hypothèses de compromission.
5. **Gestion et amélioration :** Maintenance des outils de sécurité, tuning des règles de détection, documentation des procédures, formation continue des équipes, reporting, post-mortem et amélioration continue.
6. **Activités transverses :** Coordination avec les équipes IT, support aux autres métiers, tests de sécurité et validation des contrôles, conformité réglementaire et audits (PGSSI, NIS2, Agréments)

Expériences pratiques souhaitées :

- F5, Palo Alto (dont Prisma et Cortex XDR), Fortinet, Cisco
- AWS (IAM, WAF, Guard Duty, Cloud Trail)
- VMWare 8
- MicroSoft (Windows, AD, ADFS, WSUS)
- Linux (Debian, CentOs, Kali)
- Tenable CS&IO, Qualys, CyberWatch, HarfangLab

Expériences théoriques souhaitées :

- Sécurité d'une infra cloud, SASE
- Normes ISO 27001, NIS2, RGPD

Qualifications

- Diplômé d'une école d'ingénieur, vous possédez une expérience réussie dans la cybersécurité d'environ 5 ans dans un environnement industriel et technique (Défense si possible).
- Vous faites preuve d'initiative pour savoir mettre en places les bonnes méthodes ainsi que les bons outils pour compléter l'état actuel des développements en termes d'infra et de Cyber.
- Connaissance des Règles de cybersécurité et de leur application logicielle : Expérience technique sur projets à logiciels prépondérants (dans l'industrie si possible).
  Spécification, cycle de développement, installation, debug, méthodes agiles.
- Connaissance des outils : IriusRisk (ou équivalent), JIRA en tant que bug tracker, sonarqube, git.
- Utilisation de la suite Microsoft.
- Connaissance de systèmes complexes dronisés serait un plus.