https://latribunelibre.com/emploi/ingenieur-devops-cybersecurite-f-h-2

Ingénieur DevOps cybersécurité F/H

Organisme employeur
Sabena Technics

Type de poste
Temps plein

Secteur
CONSTRUCTION
AÉRONAUTIQUE ET SPATIALE

Lieu du poste
33281, MERIGNAC, MERIGNAC, France

Date de publication
8 janvier 2026 à 12:03

Valide jusqu'au
07.02.2026

Description

En tant qu'Ingénieur DevOps cybersécurité, vous êtes rattaché hiérarchiquement au Responsable de la Sécurité des Systèmes d'Information.
L'objectif central de l'ingénieur.e DevOps Cybersécurité est de façonner et maintenir un niveau élevé de résilience et de protection des données et des accès sur les environnements de l'équipe Cybersécurité et, suivant les demandes, les environnements d'autres équipes du groupe.
La cybersécurité est une composante fondamentale de toutes les missions de l'ingénieur.e DevOps Cybersécurité.
Ces missions comprennent principalement la conception, la construction, l'exploitation et l'amélioration continue des environnements virtualisés et conteneurisés de l'équipe Cybersécurité. Ces missions comprennent aussi, au besoin, la participation à la gestion d'incident de cybersécurité et l'accompagnement d'autres équipes sur les sujets DevOps.

Infrastructure | Réseaux | Virtualisation
- Installer, configurer et améliorer les environnements Proxmox, les VMs, les conteneurs (rootless, pods, images), les OS et les dépôts.
- Concevoir et mettre en place une architecture de segmentation réseau au sein et autour des différents environnements de l'équipe Cybersécurité en relation avec l'équipe infrastructure du Groupe.
- Configurer et maintenir les WAF (ModSecurity, OWASP-CRS) devant les applications exposées.
- Gérer le provisioning, le scaling et la mise à jour des hyperviseurs.

Authentification | Autorisation
- Mettre en oeuvre des solutions d'authentification forte et d'autorisations pour l'accès aux plateformes Proxmox, aux hôtes Linux, aux applications et aux services (MFA, LDAP, OIDC, OAUTH2, Certificats SSH, RBAC, ABAC, …).
- Gérer et contrôler les politiques d'autorisation sur la base des principes de moindre privilège et de confiance minimale.

Cybersécurité
- Appliquer les principes de défense en profondeur, de moindre privilège, de confiance minimale et les guides de durcissement de l'ANSSI, du BSI, du NIST et du CIS.
- Gérer rigoureusement les secrets et les configurations des environnements.
- Automatiser et planifier les audits et les contrôles réglementaires et internes des environnements ainsi que de l'infrastructure goupe exposée sur l'internet public.
- Prendre connaissance progressivement des réglementations, des normes et des référentiels sur la cybersécurité qui sont applicables aux activités du groupe (EASA Part IS, NIS2, IGI 1300, SecNumCloud, EUCS, ISO, EBIOS RM).

Orchestration IaC

Qualifications

Profil

Expérience :

- Expérience professionnelle de 5 ans ou plus.
- Expériences professionnelles avérées sur un poste de DevOps.
- Activités professionnelles récentes liées à la cybersécurité.

Formation :

- Master Informatique ou Cybersécurité
- Diplôme Ingénieur en Informatique ou Cybersécurité

Langues :

- Bonne maîtrise écrite et orale de l'anglais (B2 minimum).
- Bonne maîtrise écrite et orale du français.

Compétences

Compétences techniques

- Maitrise : Virtualisation, Conteneurisation, IaC, Proxmox, Administration linux, Scripting, CI/CD, Supervision,
- Expériences : OpenTofu/Terraform, Ansible, Podman, Réseau, Authentification, Autorisation, Durcissement, scan de vulnérabilités, gestion des secrets, WAF, Agilité, ITIL, SRE
- Connaissances : Standards, référentiels et guides de l'ANSSI, du CIS, de MITRE ATT&CK, du NIST

Capacités

- Esprit d'analyse et résolution de problème,
- Rigueur et méthode
- Travail en équipe multidisciplinaire, en autonomie et proactif
- Sens du service