https://latribunelibre.com/emploi/architecte-reseaux-et-cybersecurite-f-h-8

Architecte Réseaux et Cybersécurité F/H

Description

Architecture et Administration des Systèmes

- Concevoir, déployer et administrer les infrastructures serveurs (Windows, Linux).
- Gérer les environnements virtualisés (VMware, Hyper-V, Proxmox).
- Implémenter et maintenir les solutions de stockage et sauvegarde.
- Assurer la haute disponibilité et la performance des systèmes.

Gestion des Réseaux et Sécurité

- Déployer et administrer les équipements réseau (switches, routeurs, firewalls).
- Optimiser la performance et la sécurité du réseau (QoS, VLAN, VPN, Wi-Fi).
- Mettre en place des outils de monitoring et de supervision (Zabbix, PRTG, Centreon).
- Appliquer les politiques de sécurité (gestion des accès, segmentation, filtrage).

Gestion des Incidents et Support Niveau 3

- Diagnostiquer et résoudre les incidents complexes liés aux infrastructures IT.
- Assurer un support technique avancé aux équipes internes.

Analyse et Gestion des Risques

- Évaluer les vulnérabilités et menaces sur les systèmes et réseaux.
- Réaliser des analyses de risques selon les méthodologies (EBIOS RM, ISO 27005).
- Proposer des mesures de mitigation conformes aux normes (ISO 27001, II 901, NIST, ANSSI).

Organisme employeur
AEROJOB

Type de poste
Temps plein

Secteur
CONSEIL POUR LES AFFAIRES ET AUTRES CONSEILS DE GESTION

Lieu du poste
78440, LES MUREAUX, LES MUREAUX, France

Salaire de base
60000 € - **Salaire de base**
70000 €

Date de publication
21 septembre 2025 à 17:08

Valide jusqu'au
20.10.2025

Définition et Mise en Œuvre des Mesures de Sécurité

- Concevoir et déployer des solutions de protection (pare-feu, EDR, SIEM, segmentation réseau).
- Rédiger les politiques et procédures de sécurité en conformité avec les standards.
- Accompagner les équipes techniques dans l'implémentation des bonnes pratiques.

Surveillance et Détection des Menaces

- Mettre en place des outils de supervision et détection d'incidents.
- Analyser les alertes de sécurité et proposer des plans de réponse.
- Participer à la gestion des incidents et à la mise en œuvre de plans de remédiation.

Conformité et Sensibilisation

- Garantir la conformité aux réglementations en vigueur (RGPD, LPM, NIS2).
- Former et sensibiliser les collaborateurs aux bonnes pratiques de cybersécurité.

Veille Technologique et Amélioration Continue

- Assurer une veille sur les nouvelles technologies et menaces cyber.
- Proposer des évolutions pour améliorer la résilience et l'efficacité des infrastructures.
- Participer à l'élaboration de la stratégie IT et aux choix technologiques.

LIVRABLES ATTENDUS

- Schémas d'architecture et documentation technique des infrastructures.
- Rapports d'audit, d'analyse de risques et de conformité.
- Politiques, procédures de sécurité et plans d'actions techniques.
-

Qualifications

Maîtrise des environnements Windows et Linux.

- Expertise en administration réseau (Cisco, Stormshield, NAC, Palo Alto).
- Connaissance approfondie des protocoles et services réseau (TCP/IP, BGP, OSPF, DNS, DHCP).
- Expérience avec virtualisation et solutions de stockage.
- Sensibilisation forte aux enjeux et bonnes pratiques de cybersécurité.
- Maîtrise des normes et cadres réglementaires (ISO 27001, Il 901, NIST, ANSSI).
- Expérience avec les outils de cybersécurité (SIEM, IDS/IPS, EDR).
- Connaissances en architecture réseau et sécurité des systèmes d'information.
- Expérience en audit et tests d'intrusion (pentest, forensic).

PROFIL SOUHAITÉ

- Formation Bac+5 en informatique, systèmes et réseaux ou équivalent.
- Minimum 7 ans d'expérience dans un poste similaire.
- Certifications appréciées : CCNP, CISSP, ITIL, RHCE, VMware VCP, Veeam, CISM, CEH, ISO 27001, EBIOS RM.

LANGUES

- Anglais lu, parlé, écrit.