


# Ingénieur sécurité et réseau confirmé(e) (H/F)

75019 PARIS [Accéder à l'annonce en ligne](#) 

 CDI

 Temps plein

 Dès que possible

 Ouvert aux personnes en situation de handicap

## L'entreprise

Up Skills se positionne en tant que cabinet de recrutement spécialisé dans l'identification et la sélection de profils cadres, experts et managers de transition. Avec 14 bureaux implantés à travers la France 8 domaines métiers : IT, Ingénierie, Comptabilité/Finance, Fonctions Support, RH/Juridique, Commerce/Marketing, Immobilier/Construction, et Tourisme.

Notre division Informatique recherche un Ingénieur réseau et sécurité H/F en CDI basé à Paris pour son client un groupe international secteur tourisme dynamique et engagée d'environ 170 collaborateurs au sein de leur DSI, vous contribuerez à des projets innovants et stratégiques, tout en participant à la transformation digitale de l'entreprise.

En rejoignant cette organisation dynamique et engagée, vous serez au cœur de projets technologiques stratégiques visant à moderniser et sécuriser les infrastructures réseau et cloud, tout en contribuant à l'amélioration continue des services offerts.

**Prêt(e) à relever ce défi stimulant dans un secteur en pleine mutation ? Postulez dès maintenant !**

## Le poste

Ingénieur réseau et sécurité spécialisé(e) Cloud H/F

- Élaborer, examiner et documenter les exigences techniques et fonctionnelles des environnements réseau.
- Auditer l'infrastructure réseau pour détecter les vulnérabilités et établir des plans de remédiation.
- Gérer et atténuer les risques liés au réseau, y compris dans les environnements Cloud.
- Participer à l'évaluation du réseau afin d'en identifier les forces et faiblesses
- Bonne compréhension de la gestion des licences logicielles ( besoins et réglementations)
- Concevoir et mettre en œuvre des infrastructures sécurisées à clé publique.

**Connaissance des menaces et des attaques:** Identifier, analyser et répondre aux cybermenaces, notamment celles visant les environnements Internet.

**Maintenir la conformité:** Assurer le respect des normes de sécurité, comme la PCI DSS, et établir des plans de mise en conformité.

**Participer au déploiement et à la maintenance:** Déployer et maintenir les solutions de sécurité. Réaliser des mises à jour et tests de sécurité réguliers pour éliminer l'obsolescence.

### **Gérer les correctifs et incidents**

Effectuer le déploiement des correctifs de sécurité et assurer la surveillance des journaux pour détecter des anomalies. Participer activement à la gestion des incidents et aux interventions d'urgence.

**Administration des réseaux et équipements:** Administration des équipements réseau et de sécurité (LAN, WAN, firewall FortiGate, Juniper, Aruba, etc.).Gestion des accès distants et réseaux Cloud (Azure, GCP).Maintenance des services DNS, DHCP (Infoblox) et Load Balancers (F5, FortiADC).

**Support technique:** Assurer un support de niveau 2 et 3 pour les incidents liés aux services réseau et infrastructure.Collaborer avec les éditeurs pour le suivi et la résolution des problèmes complexes.

**Environnement technique** Technologies clés : LAN, WAN, VPN, Firewall (Fortinet), WAF, SDWAN, SASE (CATO), DNS/DHCP (Infoblox), GCP, Azure, F5 Load Balancer, automatisation (GIT).

## Le profil recherché

### Profil recherché :

- Diplôme : Bac+5 en réseaux et sécurité informatiques.
- Expérience : Minimum 5 ans hors alternance en réseau et sécurité
- Expertise en sécurité réseau (LAN, WAN, VPN, Fortinet).
- Connaissances avancées des **environnements Cloud (Azure, GCP)**.
- Bonne maîtrise des concepts ITIL (gestion des incidents, des fournisseurs, des changements).
- Expérience avec des technologies de sécurité avancées (cryptographie, HTTPS, SSL, etc.).
- Langues : **Anglais courant** à l'écrit comme à l'oral.
- Certifications en sécurité réseau et Cloud sont un plus (Fortinet, CISSP, etc.).