

**Hassan A.** - Né en 2000  
**59300 Valenciennes**  
**4 ans d'expérience**  
**Réf : 2402141437**

## Ingénieur cybersécurité

### Ma recherche

---

Je recherche tout type de contrat, sur toute la région Hauts-de-France, dans le Bâtiment.

### Formations

---

**2023** : Bac +5 à INSA Hauts-de-France  
Master Cyberdéfense et Sécurité de L'information (CDSI)

### Expériences professionnelles

---

#### **04/2023 - 10/2023** :

Analyste SOC chez Tiphereth Consulting

Qualification du niveau de criticité des vulnérabilités en fonction des CVE, CVSS.

Saisie d'incidents et escalade.

Analyse et vérification des vulnérabilités des systèmes.

Mise en place des Rapports et Dashboard sur SPLUNK.

Prévenir les nouvelles vulnérabilités en anticipant les mises à jour logicielles et les changements d'installation.

Évaluer la gravité des incidents de sécurité et, si nécessaire, effectuer des investigations complémentaires à l'aide d'outils tels que Virus Total et HybridAnalysis.

Effectuer des analyses de vulnérabilités et des audits de sécurité, comprenant :

Vérification des ports et des serveurs à l'aide d'outils comme Nmap.

Exploitation des vulnérabilités en utilisant Metasploit.

Analyser les e-mails de phishing et/ou les pièces jointes malveillantes.

Évaluation des vulnérabilités dans les instances EC2 à l'aide de Amazon Inspector

Environnement : Splunk, Defender, Crowdstrike, Phantom, Snort, Suricata, Servicenow, Jira

#### **03/2021 - 06/2021** :

Stagiaire en PENTEST chez Centre De Formation France

Identifier les vulnérabilités et leurs impacts sur l'ensemble du réseau.

Test d'exploitation des vulnérabilités.

Mettre en place des environnements de travaux pour réaliser les pentests.

Effectuez des tests d'intrusion (périmètres suivant votre expertise), en solo (pour les cibles simples) ou en équipe (pour les cibles vastes ou complexes).

Faire des recommandations sur les mesures immédiates.

Rédactions des rapports des audits

Environnements : VMware, Kali Linux, Linux (Ubuntu), LAN, WAN, Apache, HTTP Server, Docker, Metasploit, Wireshark, Nmap

#### **10/2019 - 01/2021** :

Administrateur système et Réseaux chez Airtel

Déployer et administrer les serveurs virtuels et physiques.

Assurer des prestations de régis (visites préventives, entretien de parc informatique et suivi des besoins utilisateurs).

Maintenir en conditions opérationnelles les infrastructures et traiter les incidents N2/N3.

Planifier et gérer les fonctions de mise à niveau, de migration, de maintenance, de sauvegarde, d'installation, de supervision et de configuration ;

Concevoir, installer et configurer des serveurs, des dispositifs de réseau et des pare-feu internes et destinés aux clients.

Gérer et entretenir de manière proactive les systèmes de serveurs, de réseaux et de pare-feu.

Assurer des prestations de régis (visites préventives, entretien de parc informatique et suivi des besoins utilisateurs).

Environnement : Linux (Ubuntu, CentOS), Microsoft (Windows Server, Windows Postes de travail), VMWARE, Switchs, Nexus, Cisco, Fortinet

## Langues

---

Français (Oral : courant / Ecrit : expérimenté)

## Atouts et compétences

---

Technologies : IDS/IPS, Firewall, SIEM.

Supervision et SIEM : Snort, Sucicata, Phantom, Splunk.

Réseaux et protocoles : TCP/IP, IPv6, NAT, DHCP, DNS, LAN, ARP, Ethernet, OSI Model.

Services Réseaux : FTP, HTTP(S), IPSec, LDAP, SMTP, SSH, Telnet, SSO.

Cloud : Microsoft Azure, AWS

Virtualisation et OS : Linux (CentOS), Windows, VMware, VirtualBox, Docker

Programmation et Scripting : Python, PowerShell, Perl, C, Python, Html, CSS, MySQL.

Outils d'analyses : VirusTotal, CyberChef, Wireshark, IPVoid, Cuckoo Sandbox.

Outils d'analyses de vulnérabilités : Nessus, Nmap.

Offensive : Kali Linux et les outils associés (Metasploit, SQLmap, Burp Suite, Nmap, Maltego, etc.)

## Permis

---

Permis B

## Centres d'intérêts

---

Roller, Football, découverte, voyage