






# Kilian Jeny Alternant Systèmes, Réseaux & Cybersécurité

 kilian.jeny.pro@gmail.com     0695185400     Paris     <https://github.com/hueco03>  
 <https://www.linkedin.com/in/kilian-jeny-59a913261/>



## Profil

Apprenti technicien support informatique en BTS SIO SISR, orienté cybersécurité. Expérience en administration Windows/Linux, réseau, Active Directory, virtualisation et diagnostic avancé. Réalisation de projets cybersécurité concrets (NIST, Splunk, vulnérabilités, SOC, TryHackMe). Recherche une alternance en cybersécurité (SOC, blue team, pentest junior ou administration sécurité).

## Compétences

### Cybersécurité

- Analyse de vulnérabilités selon **NIST SP 800-30** (serveur MySQL exposé).
- Audits de sécurité basés sur le **NIST CSF, PCI DSS, GDPR et SOC 2**
- Gestion d'incidents de sécurité selon le cadre NIST
- Investigation de logs et corrélation d'événements avec **Splunk**.
- Analyse de trafic réseau avec **Wireshark** et **Suricata**
- Analyse de fichiers suspects via VirusTotal et CrowdStrike.
- Exploitation de vulnérabilité
- Utilisation de **SQL** pour l'analyse de logs de sécurité
- Automatisation de tâches de sécurité avec **Python**

### Réseau

VLAN, VLSM, DHCP, DNS, NAT, ACL, Cisco IOS, pfSense, VPN, IPv4

### Systèmes

Windows 10/11/12, Windows Server, Linux (Debian/Ubuntu), VMware, Virtualisation, Pfsense

### Support

Support utilisateur N1/N2, diagnostic matériel/logiciel, gestion d'incidents (GLPI), Active Directory, GPO, préparation et déploiement de postes.

### Outils

Wireshark, Suricata, Splunk, Burp Suite, Nessus, VirusTotal, OWASP ZAP, PowerShell, CMD, Metasploit, Nmap, SQL, Git, Python, GLPI, Azure

### Soft skills

Rigueur, curiosité, autonomie, travail en équipe, pédagogie

### Développement Web

WordPress, HTML, CSS, JavaScript, OVH

## Formation Académique

### BTS Services Informatiques aux Organisations – Option SISR

IRIS  
09/2023 – 07/2026 | Paris

## Expérience Professionnelle

### Apprenti Technicien Support Informatique

Institut Curie  
09/2025 – 08/2026 | Saint-Cloud (en cour)

- Support utilisateur N1/N2
- Gestion AD, réinitialisation mots de passe, GPO
- Résolution d'incidents réseau, logiciels métiers, Windows
- Préparation, installation et configuration de postes
- Diagnostic matériel / support sur site
- MAJ systèmes, tickets GLPI
- Application de bonnes pratiques de sécurité (AD, GPO, durcissement).
- Contrôle des accès utilisateurs & MFA.

### Stage Développeur Web

Natureland  
11/2024 – 12/2024 | Bar-Sur-Aube  
Développement du site web en HTML, CSS, PHP et JavaScript.  
Hébergement du site via OVHcloud

### Stage en Développement Web

Espace Lilas  
06/2024 – 07/2024 | Paris  
Développement du site et hébergement via WordPress.

## Projets cybersécurité

### Évaluation de vulnérabilité serveur – NIST SP 800-30

- Analyse d'un serveur MySQL exposé : identification des risques (exfiltration, DoS), matrice probabilité × impact et recommandations

### Script Python – Gestion automatique d'adresses IP autorisées

- Mettre à jour dynamiquement une liste d'IP autorisées
- Gérer une liste de suppression
- Automatiser la gestion d'accès réseau dans un environnement sensible (santé)

### Audit de sécurité – Botium Toys (NIST CSF)

- Évaluation des contrôles : accès, sauvegardes, chiffrement, politique mots de passe ; analyse conformité PCI/GDPR/SOC et plan d'amélioration prioritaire.

### Journal d'enquêtes sur incidents – Cadre NIST

4 incidents analysés : scan de ports, malware Emotet, faux positif réseau, tentatives brute force ; investigations via Splunk, Wireshark, Nmap, VirusTotal et mesures correctives.

### Mitigation d'attaque DDoS – ICMP Flood

- Rapport complet sur une attaque DDoS ICMP : analyse de l'impact, durcissement du pare-feu, segmentation réseau, IDS Suricata et actions de mitigation.

### Analyse SQL pour investigation sécurité

- Requêtes SQL avancées (AND/OR/NOT/LIKE) pour identifier connexions suspectes, anomalies horaires/géographiques et employés à cibler pour actions de sécurité.

### TryHackMe – Challenge "Takeover" (Subdomain Takeover)

Identification d'un sous-domaine vulnérable et prise de contrôle via un DNS non réclamé.

## Certifications

Google Cybersecurity Professional Certificate

TryHackMe – Pre-Security

TryHackMe – Cyber Security 101

## Langues

**Français** C2    **Anglais** B2