Kilian Jeny Alternant Analyste SOC | Pentest & Gouvernance (GRC)

kilian.jeny.pro@gmail.com 06 95 18 54 00 Paris https://github.com/hueco03
https://www.linkedin.com/in/kilian-jeny-59a913261/ https://tryhackme.com/p/HuecoMundo

Profil

Apprenti technicien support informatique en BTS SIO SISR, orienté cybersécurité. Expérience en administration Windows/Linux, réseau, Active Directory, virtualisation et diagnostic avancé. **Titulaire de la certification eJPT (Junior Penetration Tester)**, je maîtrise les méthodologies d'audit offensif pour mieux anticiper les menaces en environnement SOC. **TOP 6%** sur **tryhackme.com**

Expérience Professionnelle

Apprenti Technicien Support Informatique, Institut Curie | Sept. 2025 – Août 2026
Support utilisateur N1/N2. Gestion AD, réinitialisation mots de passe GPO. Résolution d'incidents réseau, logiciels métiers. Windows MAJ systèmes, tickets GLPI

Stage Développeur Web, Natureland | Novembre 2024 - Décembre 2024
HTML, CSS, PHP, OVHcloud

Formation Académique

BTS Services Informatiques aux Organisations – Option SISR, IRIS | Septembre 2023 - Mai 2026

Compétences

Analyse SOC & Défense (Blue Team)
- **Surveillance & Détection :** Analyse de journaux d'événements et détection d'anomalies via **SIEM (Splunk)**.
- **Réponse aux incidents :** Investigations via le cadre **NIST CSF**, analyse de fichiers suspects (**VirusTotal**) et corrélation de logs.
- **Sécurité Réseau :** Déploiement et administration de pare-feu **pfSense** (filtrage, NAT), **IDS/IPS Snort** et **VPN (OpenVPN, IPsec)**.
- **Analyse de trafic :** Capture et analyse de trames avec **Wireshark** et **Suricata** pour identifier des flux malveillants.

Pentesteur (ejpt)
- **Reconnaissance & Énumération :** Balayage réseau avancé avec **Nmap**, énumération de services (SMB, HTTP, SQL) et recherche de vecteurs d'entrée.
- **Exploitation de vulnérabilités :** Utilisation du **Metasploit Framework**, exploitation de failles Windows/Linux et exécution de charges utiles.
- **Sécurité Web :** Test d'intrusion sur les vulnérabilités du **OWASP Top 10** (SQLi, XSS) via **Burp Suite**.
- **Post-Exploitation :** Techniques de **Pivoting** (routage IP), transfert de fichiers et cassage de hashs (**John the Ripper/Hashcat**)
- **CTF TryHackMe**

Réseau/Système
VLAN, VLSM, DHCP, DNS, NAT, ACL, Cisco IOS, pfSense, VPN, IPv4
Windows 10/11, Windows Server, Linux (Debian/Ubuntu), VMware, Virtualisation, Pfsense

Soft skills
Rigueur, curiosité, autonomie, travail en équipe, pédagogie

Projets cybersécurité

SIEM (Security Information & Event Management)
- Développement d'un SIEM opérationnel from scratch pour la collecte, l'analyse et la corrélation d'événements de sécurité en temps réel.

Pare-feu pfSense
- Déploiement d'infrastructure de sécurité : pare-feu multi-zones, IDS/IPS Snort (détection/blocage automatique), authentification LDAPS/ portail captif, VPN OpenVPN SSL avec PKI interne, sécurisation SSH/HTTPS

Script Python – Gestion automatique d'adresses IP autorisées
- Script Python d'automatisation d'une liste d'IP autorisées : lecture d'un fichier d'allow-list.

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.

VPN Sécurisation inter-sites
- Mise en place VPN site-to-site pour sécuriser les liaisons multi-sites (stade/billetterie/magasin), administration à distance SSH sécurisée, gestion PKI et surveillance des accès en temps réel

Certifications

Google Cybersecurity Professional Certificate • TryHackMe – Pre-Security • TryHackMe – Cyber Security 101 •
eLearnSecurity Junior Penetration Tester (eJPT) • TryHackMe - Web Fundamentals • Tryhackme - JR Penetration tester

Langues

Français	Anglais
C2	B2