

Mevorah Abergel

Cybersécurité & infrastructure

Ingénieur cybersécurité et administration en alternance chez Recygo · cycle ingénieur à l'École 2600

abergelmevo@gmail.com

abergelmevo.github.io

linkedin.com/in/mevorah-abergel-a33325298

github.com/Abergelmevo

Trois ans d'alternance sur l'infrastructure d'une PME : faire tourner le réseau, l'annuaire et les sauvegardes, puis les auditer, les mesurer et les défendre. J'audite avant d'agir, je mesure avant et après, et je teste mes défenses en les attaquant en laboratoire. Chaque projet est documenté sur mon portfolio, avec ses incidents et ses résultats.

EXPÉRIENCE

Ingénieur cybersécurité et administration (alternance) · Recygo, filiale de La Poste et de Suez
Depuis septembre 2026

Au sein de la direction SI et Data : feuille de route cybersécurité du SI et des applications SaaS à partir des tests d'intrusion, sensibilisation et tests des collaborateurs, PCA, PRA et PSSI, identités et postes (IAM, UEM), automatisation métier avec n8n.

Alternance en administration systèmes, réseaux et sécurité · PME de distribution (une vingtaine de personnes)
2023 – 2026 · BTS SIO, puis licence professionnelle

- **Audit et durcissement Active Directory** en production : score PingCastle « Anomalies » de 100 à 74, SMBv1 retiré, krbtgt renouvelé après 11 ans, 169 objets obsolètes supprimés, sans coupure imprévue.
- **Détection** : SIEM Wazuh, IDS Suricata (50 682 règles) et leurre qui alerte en moins de 30 s ; IA locale (n8n, Ollama) qui explique les alertes critiques sans qu'aucune donnée ne quitte le serveur.
- **Réseau** : cœur de réseau audité puis migré en 10 Gigabit (8,25 Gb/s mesurés), supervision Zabbix et Grafana avec alertes.
- **Exposition et accès** : portail B2B publié en DMZ, TLS noté A sur SSL Labs ; VPN WireGuard dédié, bascule des utilisateurs sans coupure.
- **Socle** : second contrôleur de domaine, sauvegardes Veeam, supervision Netdata, mise en service des postes.

PROJETS DE LABORATOIRE ET D'ÉCOLE

- **Noyau Linux** (École 2600) : noyau recompilé, appels système, rootkit par hook ftrace, puis miniEDR en BPF-LSM qui journalise et emprisonne des processus (17 tests sur 17).
- **Attaque d'un Active Directory** (homelab) : d'un simple compte au Golden Ticket, chaque étape reliée à sa trace et à sa parade.
- **Cyber range** (homelab) : mesurer ce qu'un SIEM voit réellement d'une intrusion derrière un pare-feu FortiGate.
- **Audit AWS** (laboratoire) : Prowler, échecs critiques de 5 à 3 et hauts de 20 à 14, sauvegardes immuables avec Object Lock.

COMPÉTENCES

Systèmes

Active Directory, GPO, Kerberos, Windows Server, Linux, Hyper-V, PowerShell

Défense

Wazuh, Suricata, PingCastle, durcissement AD et TLS, MITRE ATT&CK

Réseau

Cisco IOS, pfSense, VLAN, OSPF, WireGuard, Zabbix, Grafana

Offensif (laboratoire)

Nmap, BloodHound, Impacket, Hashcat, Metasploit

Automatisation et cloud

n8n, Python, IA locale (Ollama), AWS, Microsoft 365 ; Ansible en apprentissage

FORMATION

Cycle ingénieur cybersécurité

École 2600 · depuis 2026

Licence pro ASS&R, mention bien

Administration et sécurité des systèmes et des réseaux · UPEC · 2025 – 2026

Bachelor Technology & Business

PST&B · 2025 – 2026

BTS SIO option SISR

PST&B · 2023 – 2025

CERTIFICATIONS

- **CCNA** · Cisco, juillet 2026
- **eJPT v2** · INE Security, en cours, examen en décembre 2026
- **HTB CDSA** · Hack The Box, en cours
- **MOOC RGPD, modules 1 et 2** · CNIL, juin 2024