

Mevorah Abergel

Cybersecurity & infrastructure

Cybersecurity and administration engineer (work-study) at Recygo · engineering degree at École 2600

abergelmevo@gmail.com

abergelmevo.github.io/en

linkedin.com/in/mevorah-abergel-a33325298

github.com/Abergelmevo

Three years of work-study on a small business's infrastructure: keeping the network, the directory and the backups running, then auditing, measuring and defending them. I audit before acting, measure before and after, and test my defences by attacking them in a lab. Every project is documented on my portfolio, with its incidents and its results.

EXPERIENCE

Cybersecurity and administration engineer (work-study) · Recygo, a La Poste and Suez company
Since September 2026

Within the IT and Data department: cybersecurity roadmap for the information system and SaaS applications, driven by penetration test results; staff awareness and testing; business continuity, disaster recovery and security policy; identity and endpoint management (IAM, UEM); business process automation with n8n.

Work-study in systems, network and security administration · distribution company (about twenty people)
2023 – 2026 · BTS SIO, then professional bachelor's degree

- **Active Directory audit and hardening** in production: PingCastle "Anomalies" score from 100 to 74, SMBv1 removed, krbtgt rotated after 11 years, 169 stale objects deleted, with no unplanned outage.
- **Detection:** Wazuh SIEM, Suricata IDS (50,682 rules) and a honeypot that alerts in under 30 s; local AI (n8n, Ollama) that explains critical alerts without any data leaving the server.
- **Network:** core network audited, then migrated to 10 Gigabit (8.25 Gb/s measured); Zabbix and Grafana monitoring with alerts.
- **Exposure and access:** B2B portal published in a DMZ, TLS graded A on SSL Labs; dedicated WireGuard VPN, users switched over with no downtime.
- **Foundations:** second domain controller, Veeam backups, workstation deployment procedure.

LAB AND SCHOOL PROJECTS

- **Linux kernel** (École 2600): recompiled kernel, system calls, an ftrace-hook rootkit, then a BPF-LSM miniEDR that logs and jails processes (17 tests out of 17).
- **Attacking Active Directory** (homelab): from a plain user account to a Golden Ticket, each step tied to its trace and its countermeasure.
- **Cyber range** (homelab): measuring what a SIEM really sees of an intrusion behind a FortiGate firewall.
- **AWS audit** (lab): Prowler, critical findings from 5 to 3 and high from 20 to 14, immutable backups with Object Lock.

SKILLS

Systems

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

Defence

Wazuh, Suricata, PingCastle, AD and TLS hardening, MITRE ATT&CK

Network

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

Offensive (lab)

Nmap, BloodHound, Impacket, Hashcat, Metasploit

Automation and cloud

n8n, Python, local AI (Ollama), AWS, Microsoft 365; learning Ansible

EDUCATION

Engineering degree in cybersecurity
École 2600 · since 2026

Professional bachelor's degree, with honours

Systems and network administration and security · UPEC · 2025 – 2026

Bachelor Technology & Business
PST&B · 2025 – 2026

BTS SIO, SISR option

Two-year national IT diploma · PST&B · 2023 – 2025

CERTIFICATIONS

- **CCNA** · Cisco, July 2026
- **eJPT v2** · INE Security, in progress, exam in December 2026
- **HTB CDSA** · Hack The Box, in progress
- **CNIL GDPR MOOC, modules 1 and 2** · CNIL, June 2024