

LÉOPOLD BURON

ABOUT

I have been practising digital investigation since I was 16, and professionally for over 4 years. Initially self-taught and trained on military cases during the onset of the Ukraine conflict, then within the crypto ecosystem, I have acquired strong expertise in analysing APT groups and their large-scale attacks. Passionate, rigorous and focused on technical aspects, I am now seeking to join a team on a permanent contract to dedicate myself fully to technical work.

PROFESSIONAL EXPERIENCE

Founder & Principal Analyst

Apr. 2022 – Present

MITAME (digital investigation consultancy)

Remote

- Conducting technical investigations for diverse clients (B2B and B2C).
- Forensic analysis, **OSINT**, modelling and cybercriminal identity research.
- Authored reports contributing to **3 confirmed arrests** (US/Thailand).
- In-depth knowledge of major APT TTPs such as **Lazarus APT38**.

Human Vulnerability Researcher (OPSEC/SE)

Feb. 2023 – Present

Binance (independent contractor)

Remote

- Identification of **social engineering** vectors and **OPSEC vulnerabilities**.
- Detailed reports on attack tactics to improve security posture.

Node Deployment and Security Technician

Feb. 2024 – Nov. 2024

Starknet Foundation (StarkWare)

Remote

- Infrastructure auditing and supplier selection via technical **benchmarks**.
- Secure node deployment using **Ansible**.

Cybersecurity Analyst

Jan. 2024 – Feb. 2024

ComptaCom (placement)

Laval, France

- Sensitive information research via **OSINT**.
- Vulnerability identification and remediation.
- Development of a **detection and reporting** tool for vulnerabilities.

EDUCATION

BTS SIO – SISR Option

2022 – 2024

Esup Rennes

- **Top of class**, specialising in secure infrastructure and systems.

Integrated Preparatory Class – Industrial Engineering and Management

Sept. 2021 – Feb. 2022

ICAM Vannes

- Ranked **top 15/55** before withdrawal (health reasons, fully resolved).

SKILLS

Threat intelligence monitoring: Infostealers (Lumma, Radamantys), Clippers, SEO spoofing.

Security & investigation: Threat Intelligence, **OSINT**, TA analysis, frameworks (MITRE ATT&CK, CAPEC, NIST, TheHive, MISP).

Cloud & infrastructure: AWS (EC2, S3, IAM), Kubernetes (**K3s**), Docker, Proxmox, **Ansible**, GitLab CI/CD.

Development & scripting: Python, Bash, TypeScript (Next.js), Git.

CERTIFICATIONS AND LANGUAGES

Certifications: AWS Cloud Practitioner (preparing SAA & SCS-C02), TOEIC (**890/990**).

Languages: Bilingual English-French.

Interests: Cybersecurity, finance/blockchains, music (piano/guitar), sailing.

SIDE PROJECTS

Homelab: in production since 2021 — stack: Proxmox, Ansible, GitLab CI/CD, Traefik, Wazuh.

Bug Bounty: reports on CursorAI (8/10), OVH (4/10), X/Twitter (1/10) — targets: web misconfigurations.