

CHERIF JEBALI

Cybersecurity Engineer · SOC · Forensic · Blue Team | M2 Work-Study Program

Paris 15e · +33 6 09 53 70 93 · cherifjebali@proton.me · [LinkedIn](#) · [GitHub](#) · [Site Web](#)

M1 Cyber Defense student (3 weeks in company / 1 week at school), specializing in incident detection and critical infrastructure security. Proficient in MITRE ATT&CK frameworks, SIEM/EDR tools, Forensics and Penetration Testing. Seeking a work-study position to strengthen the resilience of your information systems against advanced threats.

PROFESSIONAL EXPERIENCE

Cybersecurity Intern — STMicroelectronics — 2024

- **Secure embedded system:** development of a CO₂ measurement device using STM32 microcontrollers, sensor integration, secure hardware architecture.
- **Data analysis & visualization:** time series processing, Python predictive algorithms, supervision dashboards.
- **Technical documentation & ISS compliance:** writing detailed reports, project traceability and compliance.

Cybersecurity Coordinator — IT LAB Dauphine — 2023 – 2025

- **Organisation of 4 CTFs & hackathons:** creation of steganography, OSINT and cryptanalysis challenges — Red Team application.
- **Project management:** objective setting, progress tracking, coordination of remediation action plans.
- **Communication & Training:** leading GitHub workshops, technical outreach for diverse audiences.

Python BootCamp Trainer — Paris Dauphine University — 2023

- Introduction of students to Python development, simplification of algorithmic and mathematical concepts.

TECHNICAL PROJECTS

- **Defensive Home Lab (Blue Team):** deployment of firewall, personal DNS, IDS/IPS (Fail2ban, Iptables), honeypots and SIEM log analysis.
- **Python automation scripts:** Nmap network scans, CVSS vulnerability analysis, automated incident report generation.
- **CTF & Threat Hunting:** SOC, Forensic, Active Directory challenges on TryHackMe / Hack The Box / Root-Me — MITRE ATT&CK and Kill Chain frameworks.
- **Data & AI Hackathons:** co-organisation and participation in recommendation systems and predictive analytics challenges.

TECHNICAL SKILLS

SOC & Detection: SIEM (Splunk), EDR, Incident Response, Threat Intelligence, Blue Team / Red Team

Pentest & Audit: Pentest, OWASP, Nmap, Honeypots, Iptables, ISO 27001/27xxx, EBIOS RM, SMSI, MITRE ATT&CK, Kill Chain, CVSS/CVE

Networks & Infrastructure: Wireshark, IDS/IPS, network segmentation, secure architecture, Docker, Linux/Unix, Windows

Development: Python, Bash, C, Java, JavaScript, HTML

Data & Visualization: SQL, R, PowerBI, statistical analysis, time series (basics)

EDUCATION

M1 Cyber Defense — École Hexagone — 2025/2026

ISMS · ISO 2700X · EBIOS RM · SOC · Forensic · DevSecOps · Cloud Security · Threat Intelligence · Cryptology · Legal environment · Industrial systems (ICS/SCADA) · Secure architecture

BSc Applied Mathematics & Computer Science — Paris Dauphine — 2022/2025

Algorithms · Java · Databases · Operating Systems · AI · Applied Mathematics

CERTIFICATIONS

- **Cisco Networking Academy:** Introduction to Cybersecurity · Network Defense · Endpoint Security · Networking Devices and Initial Configuration · Networking Basics — [view all badges on Credly](#)
- **Microsoft & LinkedIn Learning:** Preparing for a career in cybersecurity.
- **Practice platforms:** TryHackMe (SOC, Forensic, AD), Hack The Box, Root-Me — numerous rooms and challenges completed.

LANGUAGES · INTERESTS

Languages: French (native) · Arabic (native) · English (professional)

Hobbies: Cyber watch & Pentesting (CTF) · Hardware & electronics · Guitar & singing · Reading