

CHERIF JEBALI

Analyste Cybersécurité · SOC · Forensic · Blue Team | Alternance M2 Cyberdéfense

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

Étudiant en M1 Cyberdéfense (3 sem. entreprise / 1 sem. école), spécialisé dans la détection d'incidents et la sécurisation des infrastructures critiques. Maîtrise des frameworks MITRE ATT&CK, outils SIEM/EDR, Forensic et Pentest. Je recherche une alternance pour renforcer la résilience de vos systèmes d'information face aux menaces avancées.

EXPÉRIENCE PROFESSIONNELLE

Stagiaire Cybersécurité — STMicroelectronics — 2024

- **Système embarqué sécurisé** : développement d'un dispositif CO₂ via microcontrôleurs STM32, intégration de capteurs, architecture matérielle sécurisée.
- **Analyse & visualisation de données** : traitement de séries temporelles, algorithmes prédictifs Python, tableaux de bord de supervision.
- **Documentation technique & conformité SSI** : rédaction de rapports détaillés, traçabilité et conformité projet.

Coordinateur Cybersécurité — IT LAB Dauphine — 2023 – 2025

- **Organisation de 4 CTF & hackathons** : création de challenges en stéganographie, OSINT et cryptanalyse — application Red Team.
- **Pilotage de projets techniques** : définition d'objectifs, suivi d'avancement, coordination des plans d'action de remédiation.
- **Communication & Formation** : animation d'ateliers GitHub, vulgarisation technique pour publics variés.

Formateur BootCamp Python — Université Paris Dauphine — 2023

- Initiation d'étudiants au développement Python, vulgarisation des concepts algorithmiques et mathématiques.

PROJETS TECHNIQUES

- **Home Lab Défensif (Blue Team)** : déploiement de pare-feu, DNS personnel, IDS/IPS (Fail2ban, Iptables), honeypots et analyse de logs SIEM
- **Scripts Python d'automatisation** : scans réseau Nmap, analyse de vulnérabilités CVSS, génération automatisée de rapports d'incidents.
- **CTF & Threat Hunting** : challenges SOC, Forensic, Active Directory sur TryHackMe / Hack The Box / Root-Me — application des frameworks MITRE ATT&CK et Kill Chain.
- **Hackathons Data & IA** : co-organisation et participation à des challenges de systèmes de recommandation et d'analyse prédictive.

COMPÉTENCES TECHNIQUES

SOC & Détection : 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

Réseaux & Infra : Wireshark, IDS/IPS, segmentation réseau, architecture sécurisée, Docker, Linux/Unix, Windows

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

Data & Visualisation : SQL, R, PowerBI, analyse statistique, séries temporelles (notions)

FORMATION

M1 Cyberdéfense — École Hexagone — 2025/2026

SMSI · ISO 2700X · EBIOS RM · SOC · Forensic · DevSecOps · Sécurité Cloud · Threat Intelligence · Cryptologie · Environnement juridique · Systèmes industriels (ICS/SCADA) · Architecture sécurisée

Licence Mathématiques Appliquées & Informatique — Paris Dauphine — 2022/2025

Algorithmique · Java · Bases de données · Systèmes d'exploitation · IA · Mathématiques appliquées

CERTIFICATIONS

- **Cisco Networking Academy** : Introduction to Cybersecurity · Network Defense · Endpoint Security · Networking Devices and Initial Configuration · Networking Basics — [voir les badges sur Credly](#)
- **Microsoft & LinkedIn Learning** : Préparer votre carrière dans la cybersécurité.
- **Plateformes pratiques** : TryHackMe (SOC, Forensic, AD), Hack The Box, Root-Me — nombreuses rooms et challenges complétés.

LANGUES · CENTRES D'INTÉRÊT

Langues : Français (bilingue) · Arabe (bilingue) · Anglais courant (technique)

Hobbies : Veille cyber & Pentesting (CTF) · Hardware & électronique · Guitare & chant · Lecture