MOHAMED AZIZ AGUIR — ENGLISH

Monastir, Tunisia • +216 93 236 576 • mohamedaziz.aguir@outlook.com

LinkedIn: https://www.linkedin.com/in/mohamedazizaguir

GitHub: https://github.com/Mohamed-Aziz-Aguir

KEY ACHIEVEMENTS

• Bal des Projets 2025 Excellence & Innovation Award

• Designed & deployed Capgemini CTI Platform (production-ready backend, automotive-focused threat analysis)

• Automated incident response workflows reducing triage time (academic SOC project)

CORE EXPERTISE

Blue Team:

• SOC Design & SIEM (Wazuh, ELK, Splunk)

• Incident Response & Threat Hunting

• Log Correlation & Forensics (Velociraptor)

• Alert Enrichment (TheHive, Cortex, Shuffle)

Red Team:

• Vulnerability Assessment

• Network & Web Exploitation

• Post-Exploitation Simulation

Dev :

• Python, FastAPI, REST APIs

CERTIFICATIONS

PROFESSIONAL SUMMARY

Cybersecurity engineering student specializing in SOC architecture, threat intelligence, and AI-driven defensive automation. Experienced in building CTI platforms, integrating open-source SOC tooling, and developing scalable backends with FastAPI, Docker, and Elasticsearch. Recognized at Bal des Projets 2025 for technical excellence. Passionate about blending Red & Blue team methodologies to improve defender readiness.

EXPERIENCE

Cyber Threat Intelligence Platform Developer Capgemini Engineering Tunisia

Jun 2025 – Sep 2025 (Internship) | Tunis, Tunisia (Hybrid)

• Designed and developed a Cyber Threat Intelligence (CTI) Platform for automotive and general cybersecurity.

• Built a FastAPI backend integrated with Elasticsearch (v8.13.4), Redis, and Docker for scalable data analytics.

• Implemented AI-based threat classification and similarity search for automated CVE correlation.

• Deployed on Ubuntu 24.04 in a Dockerized production-ready environment; followed Agile practices.

SOC Architecture & Automation Project ESPRIT (Academic and Bal des Projets 2025 winner)

Nov 2024 – June 2025 | Tunis, Tunisia

• Built a complete open-source SOC using Wazuh, TheHive, Cortex, Shuffle, Velociraptor, and Zabbix.

• Configured pfSense for segmented zones (DMZ, Honeynet, LAN, SOC) and created alert pipelines.

• Automated incident response workflows and integrated analyzers for

• Cisco — CCNA

LANGUAGES

• Arabic — Native

• English — Fluent (90%)

• French — Intermediate (60%)

INTERESTS

Threat Intelligence, SOC Operations, Red Teaming, AI in Security, CTFs, Ethical Hacking

ticket enrichment.

Automated Incident Response Lab ESPRIT (Apprenticeship)

Jan 2025 – Jun 2025 (Apprenticeship)

• Implemented auto-blocking workflows for malicious IPs triggered by Wazuh alerts.

• Integrated Cortex analyzers for enrichment in TheHive, reducing triage time significantly.

KEY PROJECTS

Cyber Threat Intelligence Platform (Capgemini, 2025)

Production-grade backend for threat collection, AI classification, and visualization.

Full SOC Deployment (ESPRIT, 2024–2025)

Open-source SOC with zoning, alert pipelines, and automation.

EDUCATION

ESPRIT – Private Higher School of Engineering and Technologies

Engineering program, Information Technology Engineering Cybersecurity focus, 2023 – 2026. This engineering degree is widely recognized as equivalent to a Master’s degree in many European systems (Bologna framework / MQF Level 7).

Preparatory Institute for Engineering Studies - Monastir (IPEIM)

Preparatory Classes (Mathematics & Physics), 2020 – 2023