

Yassine Abid

abid.yassine@esprit.tn

+216 99 545 525

Cybersecurity Engineering Student

Tunis, Tunisia

github.com/yassine-abid | linkedin.com/in/yassine-abid-908888325

Final-year cybersecurity engineering student at ESPRIT focused on security operations and automation. Built Waymark for phishing investigations at ODDO BHF Tunis, with projects in SOC automation, network provisioning, and identity management.

Education

ESPRIT, Tunis | Engineering Degree in Cybersecurity | Expected 2027

Professional Experience

ODDO BHF, Tunis | Cybersecurity Intern

Jun – Aug 2026

- Built Waymark, a phishing detection and investigation tool combining FastAPI, React, email analysis, YAML/YARA rules, and seven indicator-enrichment sources.
- Added AI agents to examine evidence and draft TheHive tasks, with analyst approval and verification of case updates.
- Deployed with Docker, Redis, SQLite, and Nginx TLS; added prompt-injection defenses and automated tests.

3S Standard Sharing Software | Network Automation Intern

Jun – Aug 2025

- Automated MPLS L3VPN provisioning with Python, Flask, Ansible, and Netmiko: VRF creation, IPAM allocation, and selectable PE–CE routing.
- Built admin/customer portals with WebSocket monitoring and traffic-engineering options; validated provisioning in EVE-NG.

Projects

ATLAS | Next-generation SOC | ESPRIT

2026

- Built a banking SOC lab connecting ELK/Wazuh monitoring across six zones, five SOAR playbooks, and an AI analyst using Neo4j graph evidence and RAG policy context.

Award: 1st place, Bal des Projets 2026, Network, Infrastructure and Data Security category.

Identity and Access Management | ESPRIT

2026

- Integrated midPoint, AD, and Keycloak for SSO, tested account blocking, and audited AD with PingCastle.

Technical Skills

Security: SIEM/SOAR, incident response, phishing analysis, MITRE ATT&CK, YARA, Suricata, MISP.

SOC and IAM: ELK, Wazuh, TheHive, Cortex, Shuffle, Neo4j, Active Directory, midPoint, Keycloak, OIDC, PingCastle.

Development and AI: Python, FastAPI, Flask, TypeScript, React, pytest, RAG, Amazon Bedrock, GitHub Copilot SDK.

Infrastructure: Linux, Docker, Nginx, Git, Redis, SQLite, Kafka.

Networking: MPLS L3VPN, Ansible, Netmiko, EVE-NG, IPAM, OSPF, BGP, EIGRP.

Training

AWS Academy Cloud Security Foundations training badge (2026). Cisco course completions: CyberOps Associate; Network Security; CCNA Switching, Routing and Wireless Essentials.

Languages: Arabic (native), French (fluent), English (fluent).