Oussama Ghali

+216 29 840 281 | oussama.ghali@eniso.u-sousse.tn | oussamaghali.me | oussama-ghali | oussama-ghali

Profile

- Cybersecurity-focused engineering student with hands-on SOC experience, having designed and operated a SIEM + IDS homelab simulating real-world attacks.
- Skilled in log analysis, alert triage, and threat detection using Wazuh and Suricata, with experience in building detection use-cases and tuning rules.
- Combines defensive monitoring, offensive testing, and AI-driven automation to enhance security analysis and incident response efficiency.

Education

- **National Engineering School of Sousse (ENISO)** **Expected 2027**
  Applied Computer Science Engineering *Tunisia*
- **Preparatory Institute for Engineering Studies - El Manar** **2023 – 2025**
  Physics & Technology Track (Ranked 172) *Tunisia*

Cybersecurity Experience

- **Personal SOC Lab (SIEM + IDS + ML)** **2025 – Present**
  Security Analyst & Lab Engineer (Self-Directed)
  - Designed and deployed a SOC homelab integrating Wazuh SIEM, Suricata IDS, and multiple monitored endpoints (Linux & Windows VMs)
  - Configured network-based intrusion detection to monitor traffic and generate alerts on suspicious behavior
  - Simulated real-world attacks (brute-force, reverse shell, privilege escalation, persistence) generating 100+ correlated alerts
  - Centralized and correlated endpoint and network logs to reconstruct full attack chains
  - Developed a lightweight ML-based anomaly detection module to identify abnormal system behavior
  - Tuned detection rules and decoders to reduce false positives and improve alert quality
  - Implemented SOC detection use-cases (unauthorized access, suspicious processes, abnormal login patterns)
- **CTF Platforms (TryHackMe, PicoCTF)** **2024 – Present**
  Offensive Security Practice
  - Completed 50+ hands-on challenges covering web exploitation, privilege escalation, and network enumeration
  - Applied real-world attack techniques (reconnaissance, exploitation, post-exploitation) in controlled environments
  - Improved analytical speed and debugging skills through time-constrained scenarios
- **Cyberguards Cybersecurity Club – ENISO** **2025 – Present**
  General Secretary
  - Organized cybersecurity workshops and events impacting 50+ students
  - Coordinated internal operations and contributed to hands-on training sessions

Projects

- **Offensive Security & Defense Toolkit** | Python, Web Security
  - Developed multiple security tools including a port scanner, password checker, and lab-use keylogger
  - Built a vulnerable web application environment to simulate common attack vectors (injection, authentication flaws)
  - Integrated attack simulations with SOC lab to validate detection capabilities and improve monitoring coverage
- **AI-Driven Security Automation** | Python, OpenClaw, Local LLMs
  - Automated log analysis and alert summarization using local LLMs
  - Reduced manual SOC workload by assisting investigation and alert interpretation

Technical Skills

- **SIEM & Monitoring:** Wazuh, Log Analysis, Alert Triage, Threat Detection
- **IDS & Networking:** Suricata, TCP/IP, Network Monitoring
- **Systems:** Linux, Windows, Virtualization
- **Offensive Security:** Web Exploitation, Privilege Escalation, Enumeration
- **Programming:** Python, C, Java, SQL, .NET
- **Other:** Machine Learning Basics, AI Automation (Local LLMs)