MOHAMED MASSOUS

Monastir, Tunisia | mohamed.massous@proton.me | +216 25 196 416

LinkedIn: linkedin.com/in/massous-med | GitHub: github.com/MedMassous

PROFESSIONAL SUMMARY

Cybersecurity student transitioning from Business Intelligence with proven analytical and system troubleshooting expertise. Hands-on experience developing Python-based security tools for log analysis, malware triage, and threat detection. Built multiple SOC-focused projects including a Mini SIEM, Windows log parser, and PowerShell command detector. Proficient in blue team operations, incident investigation workflows, and security automation. Seeking a cybersecurity internship to apply practical detection engineering and SOC analysis skills in a real-world environment.

EDUCATION

Cybersecurity Engineering (Informatique)

TEK-UP University, Ariana, Tunisia | 2025 – Present

- *Specialized in cybersecurity engineering, focusing on network security, threat analysis, and secure systems*
- *Applying programming and scripting skills to security automation and analysis*

Bachelor of Science – Business Intelligence

Université De Kairouan, Tunisia | Graduated June 2025

- Developed strong analytical and data processing skills applicable to security log analysis and threat detection
- Gained programming expertise in Python, Java, and SQL used in security automation projects

CERTIFICATIONS

- **Advent of Cyber 2025** | SOC operations, malware analysis, incident response
- **Jr Penetration Tester** | Offensive security fundamentals for defensive application
- **Foundations of Cybersecurity** | Security principles, threats, vulnerabilities
- **Python Fundamentals** | Algorithms, debugging, automation
- **Open Source Software Development** | Git, GitHub, version control

TECHNICAL SKILLS

Blue Team & SOC Operations: Log analysis and alert triage, incident investigation workflows, malware static analysis (hash generation, string extraction, PE structure analysis), detection logic development, threat identification and classification

Networking & Traffic Analysis: TCP/IP protocol analysis, DNS and HTTP/S traffic inspection, packet capture and analysis

Tools & Platforms: Wireshark, Nmap, Sysmon, Windows Event Logs, Linux/Windows OS internals, basic SIEM concepts

Programming & Scripting: Python (log parsing, correlation engines, security automation), PowerShell analysis, Regex pattern matching, SQL

CYBERSECURITY PROJECTS

- **Mini SIEM (Python) – Log ingestion, correlation, and alerting for SOC use cases**
- **Malware Analysis Helper – Static file triage: hashes, strings, PE analysis**
- **Windows Log Parser – Windows & Sysmon threat detection**
- **PowerShell Detector – Detection of malicious and obfuscated PowerShell commands**
- **Password Strength Checker – Weak password and entropy analysis**

PROFESSIONAL EXPERIENCE

Founder & Client Support Manager | ProstSMM (Remote) | July 2021 – Present

- Provided technical support to 8,000+ global clients via ticketing systems, resolving platform functionality and access issues
- Troubleshot system errors, user access problems, and technical configuration issues using remote support tools
- Developed strong customer communication and technical problem-solving skills applicable to SOC analyst responsibilities

End-of-Studies Intern | Elyos Digital, Monastir, Tunisia | February 2025 – May 2025

- Collaborated with development team to build mobile application using Flutter framework
- Conducted testing and debugging to ensure application security and functionality

CONTINUOUS LEARNING

Actively expanding cybersecurity knowledge through hands-on labs and self-study:

- SOC operations and blue team workflows (monitoring, triage, escalation procedures)
- SIEM fundamentals (log ingestion, parsing, correlation, detection rule development)
- Windows internals and Event Log analysis for threat hunting
- Network traffic analysis using Wireshark and IDS concepts
- Practical exercises on TryHackMe focusing on real-world security scenarios

ADDITIONAL INFORMATION

- Languages: English , French ,Arabic
- Availability: Open to remote or on-site cybersecurity internships (flexible scheduling)
- Portfolio: All security projects available on GitHub at github.com/MedMassous