Omar Mahmoud Fattouh

+20 103 282 1212 | omarfattouh.work@gmail.com | linkedin.com/in/omar-fattouh | github.com/0xTT-byte | Portfolio

Professional Summary

Cybersecurity Engineer specializing in Detection Engineering, SOC operations, and Malware Analysis. Experienced in building end-to-end security pipelines (SIEM, ELK, Wazuh), developing detection logic mapped to MITRE ATT&CK, and analyzing malware using reverse engineering techniques. Strong focus on automation, threat detection scalability, and security engineering in production environments.

Education

Misr Higher Institute for Engineering and Technology — Mansoura, Egypt
B.Sc. Information Systems (Network Security Track) — *Expected June 2027*

- Focus: Network Security, Operating Systems, Data Structures, Database Systems, Systems Analysis

Achievements & Security Impact

- Top 5% on TryHackMe globally with 80+ hands-on labs in RE, SOC, and Web Security
- Published 5+ security research writeups covering malware analysis, YARA engineering, and detection workflows
- Active CTF competitor specializing in reverse engineering and forensic analysis

Technical Skills

Detection Engineering	Sigma Rules, YARA, MITRE ATT&CK, Detection pipelines, Log correlation, Alert tuning
SOC & SIEM	ELK Stack, Wazuh, Splunk, Microsoft Sentinel, Threat hunting, Incident response
Malware Analysis & RE	IDA Pro, x64dbg, dnSpy, x86 Assembly, Volatility, Procmon, Wireshark, Static/Dynamic analysis
Security Testing	Nmap, Nessus, OpenVAS, Burp Suite, Vulnerability assessment, CVSS scoring
DevSecOps	Docker, CI/CD pipelines, Flask, MySQL, API security, Automation workflows (n8n)
Programming	Python, Bash, PowerShell, C++
Systems	Linux (Arch/Fedora/Kali), Windows Server, Active Directory, Git

Professional Experience

Freelance DevSecOps Engineer — Jan 2026 – Present
Limatrix — *Remote*

- Engineered secure CI/CD pipelines for 3+ production clients, integrating automated security scanning and container hardening
- Designed Docker-based infrastructure reducing deployment time by 40% and enabling zero-downtime releases
- Built Flask/MySQL security dashboards tracking 15+ metrics, reducing incident detection time by 30%
- Integrated AI-driven APIs into production systems with 99.9% uptime across 10K+ daily requests

SOC Analyst Intern — Aug 2025 – Sep 2025
EncryptEdge Labs — *Remote (UK)*

- Built and maintained Wazuh + ELK SIEM pipeline processing 10K+ daily logs across 5+ systems
- Developed 10+ Sigma rules aligned with MITRE ATT&CK (T1003, T1021), improving detection coverage
- Automated log triage using Python, saving 5+ hours/week in SOC operations
- Identified 15+ critical vulnerabilities via Nessus, reducing MTTR by 30% through remediation workflows

Security Research & Projects

Aviation Email Classification System (Production)
Nesma Airlines

itemize
Built LLM-based email classification system processing 500+ emails/day across 17 departments
Fully automated pipeline using Docker, n8n, Gemini API, Flask, and MySQL with zero manual triage
Deployed live dashboard with operational reporting via Telegram for real-time monitoring

Detection Engineering Lab (ELK + Wazuh)
GitHub

itemize
Built full SIEM lab simulating real-world adversary behavior mapped to MITRE ATT&CK

Implemented Sigma-to-Lucene translation pipeline for credential access detection (T1003)

Secrets Scanner (CI/CD Security Tool)

GitHub

itemize

Developed Python-based secret detection engine using entropy + regex analysis

Prevented 50+ credential leaks through CI/CD pre-commit security enforcement

Malware Analysis Research

GitHub

itemize

Reverse engineered AgentTesla and RedLine malware families using static and dynamic analysis

Developed YARA signatures based on behavioral and structural IOC patterns

Soft Skills

- Strong analytical thinking in adversary simulation and detection engineering
- Incident response decision-making under time-critical conditions
- Technical writing (security reports, detection rules, research writeups)
- Collaboration with DevOps and engineering teams in production environments
- Self-directed learning in CTFs, reverse engineering, and threat research
- High attention to detail in log analysis and anomaly detection
- Effective time management across freelance, research, and competitive cybersecurity work

Certifications

CompTIA Security+ eJPTv1 (Junior Penetration Tester)
eCIR (Incident Response) CCNA (Cisco Certified Network Associate)