Omar ElShenawy

contactme@omarelshenawy.com ❖ +20 120 839 2099 ❖ Cairo, Egypt
❖ www.omarelshenawy.com ❖ linkedin.com/in/omarelshenawy

EDUCATION

Arab Open University **Sept. 2021 – Jan. 2025 (Graduated)**
Bachelor's Degree in Computer Science Cairo, Egypt

- **Final Year Project/Thesis:**

  Developed a secure, cross-platform mentorship application featuring encrypted messaging, role-based access control, and user authentication.
- Participated in ECPC programming competitions, Cyber Security Club, and Enactus.

Al Retaj Language School **Graduated: 2021**
General Secondary Education Cairo, Egypt

WORK EXPERIENCE/INTERNSHIPS

CyberX **Nov. 2024 – Dec. 2024**
Red Team Trainee Remote

- Conducted penetration testing and vulnerability assessments, identifying critical security flaws and recommending effective mitigation strategies.
- Created detailed reports on simulated attacks, providing actionable insights to strengthen system defenses.

National Telecommunication Institute **Oct. 2024 – Nov. 2024**
Cyber Security Trainee Nasr City, Cairo

- Completed Huawei HCIA Security Certification, gaining foundational knowledge in network security and threat management strategies.
- Implemented secure configurations and firewall management during lab simulations, ensuring adherence to cybersecurity best practices.

SKILLS

- **Incident Response & Monitoring:** SIEM (Splunk, IBM QRadar, Google Chronicle), EDR (CrowdStrike, SentinelOne), IDS/IPS (Snort, Suricata, Zeek), log analysis, alert triage, escalation procedures.
- **Threat Detection & Hunting:** MITRE ATT&CK, YARA, MISP, phishing analysis, malware triage, network traffic analysis, User & Entity Behavior Analytics (UEBA).
- **Digital Forensics & Malware Analysis:** Memory forensics (Volatility), disk imaging & evidence acquisition (FTK Imager), static & dynamic malware analysis, artifact analysis.
- **Vulnerability Management & System Hardening:** Nessus, OpenVAS, patch management, CIS Benchmarks, risk assessment.
- **Security Automation:** SOAR (Splunk SOAR), Python, Bash, SQL, regex, log parsing, automated security workflows.
- **Threat Intelligence & Adversary Tactics:** IOC management, threat actor TTPs, intelligence platforms (MISP, OpenCTI), Open Source Intelligence (OSINT).

CERTIFICATIONS

- **TryHackMe SOC Level 1 / Cyber Security 101 / Pre Security – Remote, 2025**
- **Google Cyber Security Professional Certification – Remote, 2025**
- **Antisyphon Training SOC Core Skills Certificate – Remote, 2025**
- **Kaspersky Cyber Generation Training Certificate – Remote, 2025**
- **CyberX Internship Certificate – CyberX, 2025**
- **Huawei HCIA Security Certification – Huawei & NTI, 2024**

LANGUAGES

- **Arabic** – Native
- **English** – Upper-Intermediate (CEFR B2)
- **German** – Intermediate (CEFR B1)