Ahmed Emad Eldeen Abdelmoneam

SOC Analyst
Incident Response Analyst

ahmedemadeldeen77@gmail.com +20 101 397 2690 **LinkedIn:** linkedin.com/in/0x3omda
Portfolio: eng-ahmed-emad.github.io/AhmedEmad-Dev

PROFESSIONAL SUMMARY

- Results-driven **SOC Analyst** and **Incident Response Analyst** with hands-on experience in **threat detection, incident investigation, log analysis, and security monitoring** across multiple environments.
- Skilled in **SIEM operations, alert triage, log correlation, threat hunting, and dashboard creation** using tools such as **Wazuh, ELK Stack, Splunk, Suricata, Security Onion, and pfSense**.
- Experienced in conducting **incident response**, evidence collection, malware analysis, and applying the **MITRE ATT&CK Framework** to improve detection capability and reduce response time.
- Strong ability to enhance **SOC workflows**, create playbooks, automate repetitive tasks, and support investigations to reduce **MTTR** and improve overall security posture.

PROFESSIONAL EXPERIENCE

Incident Response Analyst *Intern (Dec 2025 – Present)*
Digital Egypt Pioneers Initiative (Amit-Learning), Egypt
- Designed and deployed over **six incident response playbooks**, improving escalation speed by **20%**.

Information Security Engineer *Training (Jun 2025 – Nov 2025)*
Global Knowledge, Cairo

ITI Summer Security Program *(Jul 2025 – Jan 2026)*
Information Technology Institute (ITI)

Cybersecurity Instructor
GDG Banha

CTF Challenge Creator - Contract (Remote)
Cyber Cohesion

PROJECTS

- **Mini SOC Environment**
- **Insider Threat Detection and Deception Project**
- **Cryptography Tool**
- **Steganography Framework**
- **Malware Analysis and Threat Intelligence Program**
- **Personal Website**

CORE SKILLS

- **Security Operations & Incident Response:** SIEM tuning (Wazuh, ELK, Splunk), alert triage, log correlation, dashboard creation, threat hunting, incident investigation, malware analysis, vulnerability assessment, IDS/IPS management (Suricata), firewall hardening (pfSense), EDR monitoring, playbook development, SOC workflow optimization.
- **Networking & Systems:** TCP/IP, DNS, DHCP, Active Directory, Group Policy, Windows Server, Linux fundamentals, CCNA-level networking, network traffic analysis, VPN and remote access security.
- **Threat Intelligence & Monitoring:** Threat feed integration, IOC hunting, MITRE ATT&CK mapping, log enrichment, automated alerting, threat reporting.
- **Soft Skills:** Leadership, communication, problem-solving, adaptability, teamwork, reporting, training, documentation.

CERTIFICATIONS

- **EC-Council Incident Response (ECIR)**
- **Certified SOC Analyst (Level 1 and 2)** — TryHackMe
- **CCNA** — Cisco Certified Network Associate
- **Junior Cybersecurity Analyst** — Cisco Networking Academy
- **eJPT v1** — eLearnSecurity Junior Penetration Tester
- **CompTIA Security+ (SY0-601)**
- **Huawei ICT Certifications:** Datacom, ICT Associate (Routing and Switching), HCCD (Huawei Certified ICT Expert — Datacom)
- **ITI Summer Cybersecurity Programs** — Benha Branch (2024 and 2025)
- **Certified Penetration Tester Bootcamp** — CyberTalents and ITI (Oct 2025)

EDUCATION

Bachelor of Computer Science *Oct 2022 – Present*
Benha University (BFCAI) — GPA: 3.7/4.0
Specialization: Information Security and Digital Forensics

LANGUAGES

- Arabic — Native
- English — C1 (Advanced)