

# Ahmed Emad Eldeen Abdelmoneam

## SOC Analyst | SOC Engineer & GRC Specialist

Email: [ahmedemadeldeen77@gmail.com](mailto:ahmedemadeldeen77@gmail.com) Phone: +20 101 397 2690 Location: Qalyubia, Banha, Egypt LinkedIn: [linkedin.com/in/0x3omda](https://linkedin.com/in/0x3omda)  
Portfolio: [eng-ahmed-emad.github.io/AhmedEmad-Dev/](https://eng-ahmed-emad.github.io/AhmedEmad-Dev/)

### PROFESSIONAL SUMMARY

- Detail-oriented **Security Operations Engineer** with hands-on experience in **threat detection, incident response, and log analysis** using tools such as **Wazuh, ELK Stack, and Suricata**.
- Proficient in **SIEM management, alert triage, and threat hunting**, applying the **MITRE ATT&CK framework** to enhance detection accuracy and reduce response time.
- Experienced with **Governance, Risk, and Compliance (GRC)** frameworks including **ISO 27001, NIST CSF, and CIS Controls**, supporting risk assessments and policy alignment.
- Strong record in optimizing **SOC workflows** and automating tasks to decrease Mean Time to Respond (MTTR) and improve overall security efficiency.

### PROFESSIONAL EXPERIENCE

#### Incident Response Analyst – Intern

Digital Egypt Pioneers Initiative (DEPI), Egypt

Dec 2025 – Present

#### ITI Summer Security Program

Information Technology Institute (ITI)

Jul 2025 – Jan 2026

#### Information Security Engineer – Intern

Global Knowledge, Cairo

- Designed and deployed over **six incident response playbooks**, improving escalation speed by **20%**.

#### Cybersecurity Instructor

GDG Banha

Sep 2024 – Present

#### CTF Challenge Creator Contract – Remote Cyber Cohesion

### PROJECTS

- Mini SOC Environment** — Built a simulated SOC with SIEM integration.
- Insider Threat Detection & Deception Project** — Developed deception-based insider threat defenses.
- Policy & Compliance Alignment Project** — Mapped organizational policies to ISO 27001 controls.
- Cryptography Tool** — Implemented encryption and decryption functionalities.
- Malware Analysis & Threat Intelligence Program** — Automated malware data enrichment and reporting.
- Personal Website** — Portfolio showcasing projects and certifications.

### CORE SKILLS

- Security Operations & Incident Response:** SIEM tuning, threat hunting, EDR, IDS/IPS, firewall hardening, malware analysis
- Governance, Risk & Compliance (GRC):** Risk assessment, policy development, ISO 27001, NIST CSF, compliance audits, GDPR, CIS Controls
- Digital Forensics:** Disk & memory forensics, packet analysis, timeline reconstruction, volatile memory analysis
- Networking & Systems:** TCP/IP, DNS, Active Directory, Group Policy, Windows Server, CCNA-level networking
- Soft Skills:** Leadership, communication, problem-solving, adaptability, teamwork, freelancing

### CERTIFICATIONS

- ECIR** — EC-Council Incident Response
- Certified SOC Analyst (Level 1 & 2)** — TryHackMe
- SANS SEC450 (Blue Team Fundamentals) | SANS SEC504 (Hacker Tools, Techniques, Exploits, and Incident Handling)**
- CCNA** — Cisco Certified Network Associate
- Junior Cybersecurity Analyst** — Cisco Networking Academy
- eJPT v1** — eLearnSecurity Junior Penetration Tester | **CEH** — Certified Ethical Hacker
- CompTIA Security+ (SY0-601)**
- Huawei ICT Certifications:** Datacom, ICT Associate (Routing & Switching), HCCD (Huawei Certified ICT Expert — Datacom)
- ITI Summer Cybersecurity Programs** — Benha Branch (2024 & 2025)
- Certified Penetration Tester Bootcamp** — *CyberTalents & ITI* (Oct 2025)
- In Progress:* **ISO 27001 Lead Implementer | ITIL v4 Foundation**

### EDUCATION

#### Bachelor of Computer Science

Banha University (BFCU) — GPA: 3.7/4.0

Specialization: Information Security and Digital Forensics

Oct 2022 – Present

### LANGUAGES

- Arabic — Native
- English — C1 (Advanced)