Ahmed Emad Eldeen Abdelmoneam

SOC Analyst | SOC Engineer & GRC Specialist

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

PROFESSIONAL SUMMARY

- Dedicated **SOC Engineer and Tier 1 SOC Analyst** with practical experience in **threat detection, incident response, and log analysis** using tools such as **Wazuh, ELK Stack (Elasticsearch, Logstash, Kibana), and Suricata**.
- Skilled in **SIEM management, alert triage, and threat hunting**, leveraging the **MITRE ATTACK framework** to improve detection accuracy and response time.
- Knowledgeable in **GRC frameworks**, including **ISO 27001, NIST CSF, and CIS Controls**, with experience conducting **risk assessments and policy alignment**.
- Proven ability to **reduce Mean Time to Respond (MTTR)**, enhance SOC efficiency, and strengthen the overall security posture through proactive monitoring and automation.

PROFESSIONAL EXPERIENCE

Cybersecuirty Team Leader *Jun 2025 – Present*
Terra Tech Company, Tanta
- Directed SOC, Red, and Cloud Security teams, ensuring unified defense and incident handling processes.
- Developed and deployed **6+ incident response playbooks**, improving escalation speed by **20%**.
- Supported risk assessments and internal audits, aligning SOC procedures with ISO 27001 and NIST CSF controls.

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

Information Security Analyst – Intern *Apr 2025 – Present*
Global Knowledge, Cairo

Cybersecurity Instructor *Sep 2024 – Present*
GDG Banha

PROJECTS

- **Mini SOC Environment**
- **Insider Threat Detection & Deception Project**
- **Policy & Compliance Alignment Project**
- **Cryptography Tool**
- **Malware Analysis & Threat Intelligence Program**
- **Personal Website**

CORE SKILLS

- **Security Operations & IR:** 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 & Level 2) – TryHackMe
- SANS SEC450 (Blue Team Fundamentals) | SANS SEC504 (Hacker Tools, Techniques, Exploits, and Incident Handling)
- CCNA – Cisco Certified Network Associate
- Junior Cybersecurity Analyst – 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 Cybersecurity Program
- *In Progress:* ISO 27001 Lead Implementer | ITIL v4 Foundation

---

EDUCATION

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

LANGUAGES

- Arabic: Native
- English: C1 (Advanced)