# AHMED EMAD ELDEEN ABDELMONEAM
## SOC Analyst | GRC Engineer
**Email:** ahmedemadeldeen77@gmail.com | **Phone:** +20 101 397 2690
**LinkedIn:** www.linkedin.com/in/0x3omda

---

## PROFESSIONAL SUMMARY

- Cybersecurity professional with experience across SOC operations, governance, and risk management. Skilled in threat detection, incident response, policy development, and compliance alignment with ISO 27001 and NIST CSF.
- Proficient in Blue Team operations (log analysis, SIEM tuning, threat hunting) and governance practices (risk assessments, control mapping, compliance audits).
- Delivered measurable results: reduced MTTR by **25%**, improved detection accuracy by **30%**, and lowered false positives by **20%**.
- Strong background in automation, cross-team collaboration, and building playbooks that enhanced SOC maturity and compliance posture.

---

## PROFESSIONAL EXPERIENCE

**Head of Security Operations**                                              *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.

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

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

**Information Security Analyst Bootcamp**                                    *Dec 2024 – Jan 2025*
Cybertalents, Remote

**Cloud Security Summer Training**                                          *Aug 2025 – Sep 2025*
Huawei, Cairo

**Cybersecurity Summer Training**                                           *Aug 2024 – Oct 2024*
Huawei, Cairo

---

## PROJECTS

- **Malware Hash & URL Scanner Tool** – Python Tkinter GUI integrating VirusTotal & Hybrid Analysis APIs; cut enrichment time per sample by **25–35%**.
- **SOC Automation Lab** – Log parsing & enrichment scripts on Splunk & ELK; accelerated analyst throughput by **25%** and reduced queue times.
- **Policy & Compliance Alignment Project** – Designed templates for security policies mapped to ISO 27001 and NIST CSF, improving audit readiness.
- **Personal Website** – Portfolio available at eng-ahmed-emad.github.io

---

## 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 – TryHackMe
- SANS SEC450 (Blue Team Fundamentals)
- SANS SEC504 (Hacker Tools, Techniques, Exploits, and Incident Handling)
- eJPT v1 – eLearnSecurity Junior Penetration Tester
- CompTIA Security+ (SY0-601)
- Certified Ethical Hacker (CEH)
- Cisco Certified Network Associate (CCNA)
- Huawei ICT Associate (Routing & Switching)
- Huawei Datacom Certification
- Huawei 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