Ahmed Emad Eldeen

SOC Analyst | Tier 1 SOC Analyst | Security Operations Center
Email: ahmedemadeldeen77@gmail.com **Phone:** +20 101 397 2690 **Location:** Cairo, Egypt
LinkedIn: linkedin.com/in/0x3omda **Portfolio:** eng-ahmed-emad.github.io/AhmedEmad-Dev

SUMMARY

Junior SOC Analyst & Incident Response (IR) with hands-on experience in Tier 1 SOC operations, alert triage, incident investigation, and escalation handling. Achieved up to 12% reduction in MTTD and 14% decrease in false positives. Proficient in SIEM, EDR, IDS/IPS, log analysis, alert correlation, and threat intelligence, with practical application of the MITRE ATT&CK framework and SOC playbooks to ensure SLA-driven detection, rapid incident containment, continuous security monitoring, and overall SOC resilience.

SKILLS

Technical: SIEM, EDR, IDS/IPS, Alert Triage, Incident Response, Log Analysis, IOC Analysis, MITRE ATT&CK, Threat Intelligence
Security & Networking: Network Security, Vulnerability Assessment, Packet Analysis
Scripting: Python, Bash, PowerShell
Tools: Splunk, Wazuh, ELK Stack, MISP, Suricata, Snort, Sysmon, YARA, Wireshark
Soft Skills: Analytical Thinking, Problem Solving, Attention to Detail, Incident Documentation, Team Collaboration, Communication

EXPERIENCE

Incident Response Analyst Trainee — ***Dec 2025 – Present***
Amit Learning (Hybrid) – Digital Egypt Pioneers Initiative, Nasr City, Cairo, Egypt

- Investigated security incidents using Splunk SIEM and Wazuh EDR, reducing MTTD by 20% and improving alert accuracy by 35% within defined SLAs.

Information Security Analyst Trainee — ***Jun 2025 – Dec 2025***
Global Knowledge (Hybrid) – Digital Egypt Pioneers Initiative, Heliopolis, Cairo, Egypt

- Collaborated with a 5-member SOC team to enhance correlation rules, increasing detection efficiency by 25%.
- Reduced false positives by 30%, saving an estimated 120 analyst-hours per month.

CERTIFICATIONS

SOC Analyst Path Level 1 and Level 2 – TryHackMe	***Aug 2025***
ECIR Preparation Course – Netriders	***May 2025***
Cisco Certified Junior Cybersecurity Analyst – Cisco	***Mar 2025***
Cisco Network Security Essentials – Cisco Networking Academy	***Jan 2025***
CompTIA Security+ 701 – Netriders	***Nov 2024***
Cisco Certified Network Associate (CCNA 200-301)	***Jul 2024***

PROJECTS

Enterprise SOC Lab with Wazuh – github.com/Eng-Ahmed-Emad/SOC-Enviroment — ***Oct 2025 – Dec 2025***

- Built an enterprise-grade SOC lab integrating Wazuh 4.3, Suricata 6.0, Sysmon 13, and YARA 4.2, simulating 15+ attack scenarios and reducing false positives by 30%, Demo video: youtube.com/watch?v=xdgfJFCGFsE

ELK-Based SOC – github.com/Eng-Ahmed-Emad/insider-threat-detection-deception — ***Jun 2025 – Sep 2025***

- Developed an ELK-based SOC with honeypots, improving investigation time by 25%, reducing undetected threats by 20%, and increasing log correlation accuracy by 35%, Demo video: youtube.com/watch?v=xdgfJFCGFsE

EDUCATION

Bachelor of Computer Science
Benha University, Faculty of Computers and Artificial Intelligence, Benha, Qalyubia, Egypt — ***Oct 2022 – Jul 2026***
Major: Information Security and Digital Forensics | GPA: 3.7/4.0

VOLUNTEERING

Volunteer Cybersecurity Instructor and Technical Trainer (Hybrid) — ***Oct 2024 – Oct 2025***
Google Developers Group (GDG) and Science In Code (SIC) – Benha, Qalyubia, Egypt

- Delivered hands-on cybersecurity training to 120+ learners, improving practical skills by 40% and achieving an average learner rating of 4.8/5.

TRAININGS

Cybertalents Universities Penetration Testing Bootcamp – Cybertalents (Remote)	***Nov 2025 – Dec 2025***
ITI Summer Cybersecurity Program – Information Technology Institute (Hybrid)	***Sep 2025 – Nov 2025***
Introduction to Cybersecurity Bootcamp – Cybertalents (Remote)	***Nov 2024 – Jan 2025***

LANGUAGES

Arabic: Native | **English:** Professional Working Proficiency (C1)