Ahmed Emad Eldeen

SOC Analyst | Tier 1 SOC Operations | Incident Response Analyst
Email: ahmedemadeldeen77@gmail.com **Phone:** +201013972690 **Location:** Cairo, Egypt
LinkedIn: linkedin.com/in/0x3omda/ **Portfolio:** eng-ahmed-emad.github.io/AhmedEmad-Dev/

SUMMARY

Junior SOC Analyst with hands-on experience in Tier 1 SOC operations, alert triage, incident investigation, and escalation handling, achieving 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 SOC resilience.

EDUCATION

Bachelor of Computer Science – Benha University (BFCAI), Benha, Qalyubia, Egypt *Oct 2022 – Jul 2026*
Major: Information Security and Digital Forensics | GPA: 3.7/4.0

SKILLS

Technical Skills: SIEM, EDR, IDS/IPS, Security Monitoring, Alert Triage, Incident Response, Log Analysis, IOC Analysis
Network and Security: Network Security, Vulnerability Assessment, Packet Analysis
Scripting and Tools: Python, Bash, PowerShell
Tools: Splunk, Wazuh, Elastic Stack (Elasticsearch, Logstash, Kibana), MISP, Suricata, Snort, Sysmon, YARA, Wireshark

EXPERIENCE

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

- Investigated security incidents using SIEM, reducing MTTD by 20% and improving alert accuracy by 35% within SLAs.
- Enhanced correlation rules, increasing detection efficiency by 25% and reducing false positives by 30%.

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

- Monitored 50+ daily alerts, improving log analysis efficiency by 30% and threat detection by 25%.
- Conducted vulnerability assessments, identifying 10+ critical issues and reducing risk exposure by 20%.

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) – Cisco	***Jul 2024***

PROJECTS

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

- Built enterprise-grade SOC lab integrating Wazuh, SIEM, EDR, Suricata, Sysmon, and YARA, simulating 15+ attacks, reducing false positives by 30%, and increasing alert triage efficiency by 40%.

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

- Developed ELK-based SOC with honeypots, improving investigation time by 25%, reducing undetected threats by 20%, and increasing log correlation accuracy by 35%.

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 training to 120+ learners, improving practical skills by 40% and lab accuracy by 25%.

TRAININGS

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

LANGUAGES

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