Ahmed Emad Eldeen

SOC Analyst
Incident Response Analyst

Email: ahmedemadeldeen77@gmail.com Phone: +20 101 397 2690 Location: Cairo, Egypt Postal Code: 13511
LinkedIn: linkedin.com/in/0x3omda GitHub: github.com/Eng-Ahmed-Emad Portfolio: eng-ahmed-emad.github.io

PROFESSIONAL SUMMARY

SOC Analyst and Incident Response Analyst with hands-on experience in SOC projects, security monitoring, alert triage, incident investigation, and vulnerability assessments. Proficient in SIEM, IDS/IPS, EDR, log analysis, threat hunting, and threat intelligence, leveraging the MITRE ATT&CK framework and SOC playbooks to enhance detection and response efficiency. Solid understanding of network protocols, vulnerability management, and business continuity.

SKILLS

Technical Skills: SIEM, EDR, IDS/IPS, Security Monitoring, Alert Triage, Incident Response, Log Analysis, IOC Analysis, Threat Hunting, Threat Intelligence, Vulnerability Assessment.
Soft Skills: Analytical Thinking, Problem Solving, Attention to Detail, Incident Prioritization, Communication Skills.

PROFESSIONAL EXPERIENCE & VOLUNTEERING

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

- Investigated and responded to 30+ security incidents weekly using SIEM tools, performing alert triage, root cause analysis, and escalation, reducing MTTD by 20%.
- Enhanced and executed automated correlation rules, improving detection efficiency by 25%.
- Documented and reported on 100+ incidents, improving the SOC knowledge base and incident tracking by 15%.

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

- Monitored enterprise security environments and analyzed logs, handling 50+ alerts daily while adhering to SOC playbooks.
- Conducted vulnerability assessments, identifying and reporting 10+ critical vulnerabilities.
- Assisted in implementing mitigation strategies, reducing potential risks by 20%.

Volunteer Cybersecurity Instructor & Technical Trainer *Oct 2024 Oct 2025*
Google Developers Group & Science In Code, Benha, Qalyubia, Egypt

- Designed and delivered hands-on cybersecurity training sessions and workshops for 70+ students, improving practical security skills by 40% and increasing cybersecurity awareness by 30%.
- Led practical labs on cybersecurity fundamentals, improving lab completion accuracy by 25% and enabling 20% of participants to pursue cybersecurity certifications.

PROJECTS

Wazuh SOC Environment Built a SOC lab integrating Wazuh, SIEM, EDR, Suricata, Sysmon, and YARA, simulating 15+ attacks and reducing false positives by 30%.
ELK SOC Environment Developed ELK-based SOC with honeypots for insider threat detection, creating dashboards that improved investigation time by 25%.

CERTIFICATIONS

- SOC Analyst Path (Level 1 and Level 2) TryHackMe
- Cisco Junior Cybersecurity Analyst (JCA) Cisco Networking Academy
- Cisco Network Security (Intermediate) Cisco Networking Academy
- Cisco Certified Network Associate (CCNA, 2024) Cisco
- eLearnSecurity Junior Penetration Tester (eJPT v2) eLearnSecurity

TRAININGS

Cyber Talents Universities Penetration Testing Bootcamp Cyber Talents (Remote) *Nov 2025 Dec 2025*
Cybersecurity Program Information Technology Institute, Benha *Sep 2025 Nov 2025*
Introduction to Cybersecurity Bootcamp Cyber Talents (Remote) *Dec 2024 Jan 2025*
Cybersecurity Summer Training Huawei, Cairo *Sep 2024 Nov 2024*
Networking and Cloud Summer Training Huawei, Cairo *Sep 2023 Nov 2023*

EDUCATION

Bachelor of Computer Science Benha University (BFCAI), Benha, Qalyubia, Egypt *Oct 2022 Present*

LANGUAGES

Arabic: Native | English: C1 (Fluent)