Ahmed Emad Eldeen

SOC Analyst
Incident Response Analyst

Email: ahmedemadeldeen77@gmail.com **Phone:** +20 101 397 2690 **Location:** Cairo, Egypt **Postal Code:** 13511
LinkedIn: https://www.linkedin.com/in/0x3omda/ **Portfolio:** https://eng-ahmed-emad.github.io/AhmedEmad-Dev/

SUMMARY

SOC Analyst and **Incident Response Analyst** driving security monitoring, alert triage, incident investigation, and vulnerability assessments within a **Security Operations Center (SOC)**. Leveraging SIEM, IDS/IPS, EDR, log analysis, and threat intelligence alongside the MITRE ATT&CK framework and SOC playbooks to enhance detection and response efficiency by 30% across multiple SOC deployments. Applying strong knowledge of network protocols and vulnerability management to improve incident resolution metrics by 25%.

SKILLS

Technical Skills: SIEM, EDR, IDS/IPS, Security Monitoring, Alert Triage, Incident Response, Log Analysis, IOC Analysis, Threat Intelligence, Vulnerability Assessment, Network Security, Malware Analysis, Digital Forensics, Packet Analysis
Operating Systems: Windows (Server/Desktop), Linux (Ubuntu, Kali, CentOS)
Scripting & Programming: Python, Bash, PowerShell
Security Frameworks: MITRE ATT&CK, NIST CSF, Cyber Kill Chain
Tools: Splunk, Wazuh, ELK, Kibana, Suricata, Sysmon, YARA, pfSense, Wireshark, Metasploit, Burp Suite, Nmap
Soft Skills: Analytical Thinking, Problem Solving, Communication, Teamwork, Time Management, Adaptability, Team Leading

EXPERIENCE

Incident Response Analyst Intern ***Dec 2025 – Present***
Amit Learning (Hybrid) – DEPI, Nasr City, Cairo, Egypt

- Investigated 30+ weekly 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%.
- Documented 100+ incidents, expanding SOC knowledge base coverage by 40% and speeding incident tracking by 20%.

Information Security Analyst Intern ***Jun 2025 – Dec 2025***
Global Knowledge (Hybrid) – DEPI, 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%.
- Implemented mitigation actions, strengthening security posture by 35% and compliance by 15%.

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

- Delivered hands-on training to 70+ learners, improving practical skills by 40% and lab accuracy by 25%.
- Led technical labs, increasing certification readiness by 30% and threat analysis capability by 35%.

PROJECTS

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

CERTIFICATIONS

- Cisco Network Security, Cisco Networking Academy *Mar 2025*
- Cisco Junior Cybersecurity Analyst (JCA) *Jan 2025*
- SOC Analyst Path Level 1 and Level 2, TryHackMe *Aug 2024*
- Cisco Certified Network Associate (CCNA), Cisco *Jul 2024*
- eLearnSecurity Junior Penetration Tester (eJPT v2) *Apr 2026 (Expected)*

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) ***Dec 2024 – Jan 2025***
Networking and Cloud Summer Training – Huawei (Hybrid), Cairo, Egypt ***Sep 2023 – Nov 2023***

EDUCATION

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

LANGUAGES

Arabic: Native | English: C1