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** with hands-on experience in SOC projects within a **Security Operations Center (SOC)**, including security monitoring, alert triage, incident investigation, and vulnerability assessments. Proficient in SIEM, IDS/IPS, EDR, log analysis, and threat intelligence, leveraging the MITRE ATT&CK framework and SOC playbooks, enhancing detection and response efficiency by 30% across multiple SOC deployments. Solid understanding of network protocols and vulnerability management, improving 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
Tools: Splunk, Wazuh, ELK, Kibana, Suricata, Sysmon, YARA, pfSense
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+ security incidents weekly using SIEM, reducing MTTD by 20% and improving SOC alert accuracy by 35%.
- Enhanced automated correlation rules, boosting detection efficiency by 25% and cutting false positives by 30%.
- Documented 100+ incidents, increasing SOC knowledge base coverage by 40% and accelerating incident tracking by 20%.

Information Security Analyst Intern ***Jun 2025 – Dec 2025***
Global Knowledge (Hybrid) – DEPI, Heliopolis, Cairo, Egypt

- Monitored 50+ alerts daily, improving log analysis efficiency by 30% and threat detection by 25%.
- Conducted vulnerability assessments, identifying 10+ critical issues and reducing potential risks by 20%.
- Implemented mitigation strategies, enhancing system security posture by 35% and compliance adherence 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+ students, improving practical cybersecurity skills by 40% and lab completion accuracy by 25%.
- Led labs and exercises, boosting certification readiness by 30% and learners' 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

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

TRAININGS

Cybertalents Universities Penetration Testing Bootcamp ***Nov 2025 – Dec 2025***
cybertalents (Remote)
ITI Summer Cybersecurity Program ***Sep 2025 – Nov 2025***
Information Technology Institute (Hybrid), Benha, Qalyubia, Egypt
Introduction to Cybersecurity Bootcamp ***Dec 2024 – Jan 2025***
cybertalents (Remote)
Networking and Cloud Summer Training ***Sep 2023 – Nov 2023***
Huawei (Hybrid), Cairo, Egypt

EDUCATION

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

LANGUAGES

Arabic: Native | English: C1