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

Aspiring **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, Alert Triage, Incident Response, Security Monitoring, Log Analysis, IOC Analysis, Threat Hunting, Threat Intelligence, Vulnerability Assessment, Firewall Management.
Soft Skills: Problem-Solving, Attention to Detail, Work Under Pressure, Team Leadership, Incident Prioritization, Decision-Making, Communication Skills, Time Management, Collaboration.

PROFESSIONAL EXPERIENCE

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 **Mean Time to Detect (MTTD) by 20%**.
- Enhanced and executed **automated correlation rules**, improving detection efficiency by **25%**.
- Documented and reported on 100+ incidents, improving 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%**.

PROJECTS

Wazuh SOC Environment
- Built and enhanced a mini **SOC lab** using **Wazuh (SIEM & EDR)**, integrated with **Suricata, Sysmon, and YARA**, and tested with **15+ Atomic Red Team simulations**. Logs were visualized in **Wazuh Dashboard** and **OpenSearch**, enriched with **VirusTotal**, increasing SOC readiness by **30%**.

ELK SOC Environment
- Improved an insider threat detection environment using **ELK Stack** and **honeypots** to monitor user activity, detect anomalies, and generate alerts, preventing **5 simulated insider attacks** and improving internal security visibility by **25%**.

CERTIFICATIONS

- SOC Analyst Path (Level 1 & 2) TryHackMe
- Cisco Junior Cybersecurity Analyst Cisco Networking Academy
- Network Security (Intermediate) Cisco Networking Academy
- CCNA Cisco Certified Network Associate
- eJPT v2 eLearnSecurity Junior Penetration Tester
- Huawei ICT Certifications Datacom, Routing & Switching, HCCD

TRAININGS

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

VOLUNTEERING

Cybersecurity Instructor *Oct 2024 Oct 2025*
Google Developers Group (GDG), Benha, Qalyubia, Egypt
- Planned and delivered **hands-on cybersecurity sessions** to **50+ students**, boosting practical security skills by **40%** and enabling **20% of participants** to pursue cybersecurity certifications.

Technical Cybersecurity Volunteer *Jul 2025 Aug 2025*
Science In Code (SIC), Benha, Qalyubia, Egypt
- Conducted **practical workshops** on **cybersecurity fundamentals** for **20+ students**, increasing **cybersecurity awareness by 30%** and refining lab completion accuracy by **25%**.

EDUCATION

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

LANGUAGES

- Arabic Native
- English C1