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

SUMMARY

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

SKILLS

Technical Skills: SIEM, IDS/IPS, EDR, incident response, threat hunting, TCP/IP, Windows/Linux admin, MITRE ATT&CK, IOC analysis.
Soft Skills: Analytical thinking, problem-solving, teamwork, time management, technical communication.

EXPERIENCE

Incident Response Analyst *Dec 2025 – Present*
Amit Learning – DEPI (Digital Egypt Pioneers Initiative), Nasr City, Cairo, Egypt
- Investigated and responded to security incidents using SIEM tools, reducing **Mean Time to Detect (MTTD) by 20%**.

Information Security Analyst *Jun 2025 – Dec 2025*
Global Knowledge – DEPI (Digital Egypt Pioneers Initiative), Heliopolis, Cairo, Egypt
- Monitored security events and analyzed logs across enterprise environments, managing **over 50 alerts daily**.

PROJECTS

SOC Environment

- Built a mini **SOC lab** using **Wazuh (SIEM & EDR)**, integrated with **Suricata, Sysmon, and YARA**, and tested with **Atomic Red Team simulations**. Logs were visualized in **Wazuh Dashboard** and **OpenSearch**, enriched with **VirusTotal**.

Insider Threat Detection and Deception

- Developed an **insider threat detection environment** using **ELK Stack** and **honeypots** to monitor user activity, detect anomalies, and generate alerts for investigation.

CERTIFICATIONS

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

TRAINING

CyberTalents Universities Penetration Testing Bootcamp *Nov 2025 – Dec 2025*
CyberTalents, Remote

Cybersecurity Program *Sep 2025 – Nov 2025*
Information Technology Institute (ITI), Benha

Introduction to Cybersecurity Bootcamp *Dec 2024 – Jan 2025*
CyberTalents, Remote

Cybersecurity Summer Training *Sep 2024 – Nov 2024*
Huawei, Cairo

Networking & Cloud Summer Training *Sep 2023 – Nov 2023* Huawei, Cairo

VOLUNTEERING

Cybersecurity Instructor *Oct 2024 – Oct 2025*
Google Developers Group (GDG), Benha, Qalyubia, Egypt
- Planned and delivered **hands-on cybersecurity sessions** on **basics, networking, Linux, and ethical hacking** to **50+ students**.

Technical Cybersecurity Volunteer *Jul 2025 – Aug 2025*
Science In Code (SIC), Benha, Qalyubia, Egypt
- Conducted **practical workshops** covering **cybersecurity fundamentals, networking, Linux, and ethical hacking** for **20+ students**.

EDUCATION

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

LANGUAGES

Arabic — Native | English — Fluent