

# Ahmed Emad Eldeen Abdel Moneim

SOC Analyst Incident Response Analyst  
Email: [ahmedemadelddeen77@gmail.com](mailto:ahmedemadelddeen77@gmail.com) Phone: +20 101 397 2690 Location: Cairo, Egypt Postal Code: 13511  
LinkedIn: [linkedin.com/in/0x3omda](https://www.linkedin.com/in/0x3omda) GitHub: [github.com/Eng-Ahmed-Emad](https://github.com/Eng-Ahmed-Emad) Portfolio: [eng-ahmed-emad.github.io](https://eng-ahmed-emad.github.io)

## SUMMARY

Aspiring **SOC Analyst** and **Incident Response Analyst** with hands-on experience in **security monitoring, alert triage, incident investigation, digital forensics, and malware analysis**. Proficient in **SIEM operations, log correlation, rule tuning, IDS/IPS management, firewall hardening, and EDR monitoring**, achieving a **30% reduction in false positives** and **20% faster incident detection**. Experienced in applying the **MITRE ATT&CK framework**, SOC playbooks, and Completed practical cybersecurity projects.

## 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  
• Investigated and responded to security incidents using SIEM tools, reducing **MTTD by 20%**.  
**Information Security Analyst** Jun 2025 – Dec 2025  
Global Knowledge (DEPI – Digital Egypt Pioneers Initiative), Cairo  
• Monitored security events and analyzed logs across enterprise environments, handling **50+ alerts per day**.

## PROJECTS

- [SOC Environment](#)
- [Insider Threat Detection and Deception](#)
- [Cryptography Tool](#)
- [Steganography Framework](#)
- [Malware and Threat Intelligence Program](#)

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

## VOLUNTEER EXPERIENCE

**Cybersecurity Instructor** — Google Developers Group (GDG), Benha Oct 2024 – Oct 2025  
**Technical Cybersecurity Volunteer** — Science In Code (SIC), Benha Jul 2025 – Aug 2025

## EDUCATION

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

## LANGUAGES

- Arabic — Native
- English — C1