Ahmed Emad Eldeen Abdel Moneim

SOC Analyst Incident Response Analyst
Email: ahmedemadeldeen77@gmail.com Phone: +20 101 397 2690 Location: Cairo, Egypt
LinkedIn: linkedin.com/in/0x3omda GitHub: github.com/Eng-Ahmed-Emad Portfolio: eng-ahmed-emad.github.io

SUMMARY

Results-driven **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 automation using **Python and Bash** to improve operational efficiency.

SKILLS

Hard Skills

- **Security Operations & Incident Response:** SIEM monitoring, alert triage, log analysis and correlation, incident investigation and response, threat hunting, IDS/IPS monitoring, firewall security, EDR monitoring, SOAR fundamentals, playbooks and SOPs.
- **Networking & Systems:** TCP/IP, DNS, HTTP/S, Active Directory fundamentals, Windows and Linux administration, PCAP analysis, VPN security.
- **Threat Intelligence:** IOC analysis and hunting, MITRE ATT&CK mapping, TTP analysis, log enrichment, correlation tuning, false positive reduction.

Soft Skills

- Incident communication, analytical thinking, problem-solving under pressure, technical documentation, teamwork, time management.

EXPERIENCE

Incident Response Analyst *Dec 2025 – Present*
Amit Learning (DEPI), 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), 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 (Information Security & Digital Forensics) — Benha University (BFCAI) *Oct 2022 – Present*

LANGUAGES

- Arabic — Native
- English — C1