# Ahmed Emad Eldeen Nasr

**SOC Analyst | Incident Response Analyst**
**Email:** ahmedemadeldeen77@gmail.com **Phone:** +20 101 397 2690 **Location:** Cairo, Egypt, 13511 (Willing to Relocate)
**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 Tier 1 SOC operations, alert triage, and incident investigation. Proficient in SIEM, EDR, IDS/IPS, and log analysis. Applies MITRE ATT&CK framework and SOC playbooks to reduce MTTD by 12% and false positives by 14%, ensuring rapid detection, SLA-driven response, and effective incident containment and recovery.

## SKILLS

**Technical Skills:** Incident Response, SIEM Operations, EDR Investigation, Log and IOC Analysis, Vulnerability Assessment, IDS/IPS
**Soft Skills:** Analytical Thinking, Problem Solving, Team Collaboration, Communication, Attention to Detail, Critical Thinking

## EXPERIENCE

**Incident Response Analyst Intern** ***Dec 2025 – Present***
Amit Learning (Hybrid) – Nasr City, Cairo, Egypt

- Investigated security incidents using Wazuh SIEM, reducing MTTD by 12% and improving alert accuracy by 18% within SLAs.
- Led weekly playbook review sessions with a 5-member SOC team, accelerating incident containment times by 10%.

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

- Added 12 new MITRE ATT&CK technique mappings to Suricata rules, raising detection coverage from 68% to 86%.
- Reduced false positives by 14%, saving an estimated 120 analyst-hours per month ( $9,600 in labor costs).

## CERTIFICATIONS

Digital Egypt Pioneers Program (DEPI) – Information Security Analyst & Forensics Investigator (MCIT) ***Jan 2026***
SOC Analyst Path Level 1 & Level 2 – TryHackMe ***Aug 2025***
ECIR Preparation Course – Netriders ***May 2025***
Cisco Certified Junior Cybersecurity Analyst – Cisco ***Mar 2025***
Cisco Network Security Essentials – Cisco Networking Academy ***Jan 2025***
CompTIA Security+ (SY0-701) – Netriders ***Nov 2024***
Cisco Certified Network Associate (CCNA 200-301) ***Jul 2024***

## PROJECTS

**Enterprise SOC Lab with Wazuh** ***Nov 2025 – Dec 2025***

- Deployed Wazuh 4.3 with Suricata, and automated YARA updates, reducing false alerts by 13% and cutting triage time by 2.5 hours.

**ELK-Based SOC** ***Aug 2025 – Sep 2025***

- Improved log correlation accuracy from 71% to 88% in 12 sources, reducing the investigation time by 13%.

**Malware Analysis & Threat Intelligence Tool** ***Jun 2025 – Jul 2025***

- Built a static malware analysis tool integrating VirusTotal and Hybrid Analysis to enrich IOCs and support faster incident triage.

## EDUCATION

**Bachelor of Computer Science**
Benha University, Faculty of Computers and Artificial Intelligence, Benha, Qalyubia, Egypt ***Oct 2022 – Jul 2026***
**Major: Information Security and Digital Forensics** – **GPA: 3.7/4.0**

## VOLUNTEERING

**Volunteer Cybersecurity Instructor and Technical Trainer (Hybrid)** ***Oct 2024 – Oct 2025***
Google Developers Group (GDG) and Science In Code (SIC) – Benha, Qalyubia, Egypt

- Delivered cybersecurity training to 120+ learners, improving practical skills by 40% with a 4.8/5 satisfaction rating.

## TRAININGS

**Cybertalents Universities Penetration Testing Bootcamp** – Cybertalents (Remote) ***Nov 2025 – Dec 2025***
**ITI Summer Cybersecurity Program** – Information Technology Institute (Hybrid) ***Sep 2025 – Nov 2025***
**Introduction to Cybersecurity Bootcamp** – Cybertalents (Remote) ***Nov 2024 – Jan 2025***

## LANGUAGES

**Arabic:** Native , **English:** Professional Working Proficiency (C1)