

Ahmed Emad Nasr

SOC Analyst Tier 1 | Junior Incident Response Analyst

✉ **Email:** ahmedemadeldeen77@gmail.com 📞 **Phone:** +20 101 816 6445 📍 **Location:** Cairo, Egypt, 13511
🌐 **LinkedIn:** [linkedin.com/in/AhmedEmad-Nasr](https://www.linkedin.com/in/AhmedEmad-Nasr) 🌐 **Portfolio:** eng-ahmed-emad.github.io/AhmedEmad-Dev

SUMMARY

SOC Analyst Tier 1 and Junior Incident Response Analyst with hands-on experience in Tier 1 SOC operations, training programs, projects, alert triage, and incident investigation. Proficient in SIEM, EDR, IDS/IPS, and log analysis. Applies MITRE ATT&CK framework, SOC playbooks and Incident Response Lifecycle to ensure rapid detection, SLA-driven response, and incident containment, eradication, and recovery.

EXPERIENCE

Incident Response Analyst Trainee

Dec 2025 – Present

Digital Egypt Pioneers Initiative (DEPI) – Hybrid, Cairo, Egypt

- Completed hands-on labs on LetsDefend, TryHackMe, and Hack The Box, practicing alert triage and Incident Response Lifecycle.
- Implemented a DEPI graduation project simulating end-to-end SOC monitoring using ELK SIEM, Wazuh EDR, Suricata, and Sigma rules.

Information Security Analyst & Forensics Trainee

Jun 2025 – Dec 2025

Digital Egypt Pioneers Initiative (DEPI) – Hybrid, Cairo, Egypt

- Solved hands-on cybersecurity labs on LetsDefend, TryHackMe, and Hack The Box, focusing on malware analysis and SIEM investigation.
- Developed a DEPI capstone project involving initial triage and SOC engineering using Wazuh SIEM, Zeek, and YARA rules.

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

PROJECTS

SOC Environment with Wazuh

Nov 2025 – Dec 2025

Project Link: github.com/Eng-Ahmed-Emad/SOC-Enviroment

- Deployed Wazuh SIEM and EDR with PfSense firewall, Suricata, automated YARA updates, reducing false alerts by 9%.

ELK-Based SOC

Aug 2025 – Sep 2025

Project Link: github.com/Eng-Ahmed-Emad/insider-threat-detection-deception

- Deployed ELK SIEM with honeypots, PfSense firewall, Zeek, Sigma rules, and Manual Threat Emulation, reducing false alerts by 7%.

Malware Analysis & Threat Intelligence Tool

Jun 2025 – Jul 2025

Project Link: github.com/Eng-Ahmed-Emad/Malware-Analysis-Threat-Intelligence-Tool

- Built a static malware analysis tool using Python, integrating VirusTotal and Hybrid Analysis to enrich IOCs.

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

Activities: Member of GDG Cybersecurity Club and SIC Cybersecurity Club; participated in national and university CTF competitions.

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

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, resulting in 40% practical skill improvement and a 4.9/5 average 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)