

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

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

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).

Dec 2025 – Present

Jun 2025 – Dec 2025

CERTIFICATIONS

Digital Egypt Pioneers Program (DEPI) – Information Security Analyst & Forensics Investigator (MCIT)

SOC Analyst Path Level 1 & Level 2 – TryHackMe

ECIR Preparation Course – Netriders

Cisco Certified Junior Cybersecurity Analyst – Cisco

Cisco Network Security Essentials – Cisco Networking Academy

CompTIA Security+ (SY0-701) – Netriders

Cisco Certified Network Associate (CCNA 200-301)

Jan 2026

Aug 2025

May 2025

Mar 2025

Jan 2025

Nov 2024

Jul 2024

PROJECTS

Enterprise SOC Lab with Wazuh

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

- 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

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

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

Malware Analysis & Threat Intelligence Tool

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

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

Nov 2025 – Dec 2025

Aug 2025 – Sep 2025

Jun 2025 – Jul 2025

EDUCATION

Bachelor of Computer Science

Benha University, Faculty of Computers and Artificial Intelligence, Benha, Qalyubia, Egypt

Major: Information Security and Digital Forensics – **GPA: 3.7/4.0**

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

Oct 2022 – Jul 2026

VOLUNTEERING

Volunteer Cybersecurity Instructor and Technical Trainer (Hybrid)

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.

Oct 2024 – Oct 2025

TRAININGS

Cybertalents Universities Penetration Testing Bootcamp – Cybertalents (Remote)

ITI Summer Cybersecurity Program – Information Technology Institute (Hybrid)

Introduction to Cybersecurity Bootcamp – Cybertalents (Remote)

Nov 2025 – Dec 2025

Sep 2025 – Nov 2025

Nov 2024 – Jan 2025

LANGUAGES

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