# Ahmed Emad Eldeen

**SOC Analyst | Tier 1 SOC Operations | Incident Response Analyst**
**Email:** ahmedemadeldeen77@gmail.com **Phone:** +201013972690 **Location:** Cairo, Egypt
**LinkedIn:** linkedin.com/in/0x3omda/ **Portfolio:** eng-ahmed-emad.github.io/AhmedEmad-Dev/

## SUMMARY

SOC Analyst and Incident Response Analyst with hands-on experience in Tier 1 SOC operations, driving security monitoring, alert triage, and security incidents investigation within a Security Operations Center (SOC). Leveraging SIEM, IDS/IPS, and EDR technologies with log analysis and threat intelligence alongside the MITRE ATT&CK framework and SOC playbooks.

## CORE COMPETENCIES

SOC Monitoring | Incident Handling | Threat Detection | Log Correlation | Blue Team Operations | Vulnerability Assessment

## SKILLS

**Technical Skills**: SIEM, EDR, IDS/IPS, Security Monitoring, Alert Triage, Incident Response, Log Analysis, IOC Analysis, Threat Intelligence, Vulnerability Assessment, Network Security, Malware Analysis, Digital Forensics, Packet Analysis

**Operating Systems**: Windows (Server/Desktop), Linux (Ubuntu, Kali, CentOS)

**Scripting & Programming**: Python, Bash, PowerShell

**Security Frameworks**: MITRE ATT&CK, NIST CSF, Cyber Kill Chain

**Tools**: Splunk, Wazuh, ELK, Kibana, Suricata, Sysmon, YARA, pfSense, Wireshark, Metasploit, Burp Suite, Nmap

**Soft Skills**: Analytical Thinking, Problem Solving, Communication, Teamwork, Time Management, Adaptability, Leadership

## EXPERIENCE

**Incident Response Analyst Intern** ***Dec 2025 – Current***
Amit Learning (Hybrid) – Digital Egypt Pioneers Initiative, Nasr City, Cairo, Egypt

- Investigated security incidents using SIEM, reducing MTTD by 20% and improving alert accuracy by 35% within SLAs.
- Enhanced correlation rules, increasing detection efficiency by 25% and reducing false positives by 30%.

**Information Security Analyst Intern** ***Jun 2025 – Dec 2025***
Global Knowledge (Hybrid) – Digital Egypt Pioneers Initiative, Heliopolis, Cairo, Egypt

- Monitored 50+ daily alerts, improving log analysis efficiency by 30% and threat detection by 25%.
- Conducted vulnerability assessments, identifying 10+ critical issues and reducing risk exposure by 20%.

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

- Delivered hands-on training to 70+ learners, improving practical skills by 40% and lab accuracy by 25%.
- Led technical labs, increasing certification readiness by 30% and threat analysis capability by 35%.

## PROJECTS

**Wazuh SOC Environment** – **GitHub:** github.com/Eng-Ahmed-Emad/SOC-Enviroment ***Nov 2025 – Dec 2025***

- Built a SOC lab integrating Wazuh, SIEM, EDR, Suricata, Sysmon, and YARA, simulating 15+ attacks, reducing false positives by 30%, and increasing alert triage efficiency by 40%.

**ELK SOC Environment** – **GitHub:** github.com/Eng-Ahmed-Emad/insider-threat-detection-deception ***Jun 2025 – Jul 2025***

- Developed ELK-based SOC with honeypots, improving investigation time by 25%, reducing undetected threats by 20%, and increasing log correlation accuracy by 35%.

## CERTIFICATIONS

- SOC Analyst Path Level 1 and Level 2, TryHackMe ***Aug 2025***
- Cisco Junior Cybersecurity Analyst ***Mar 2025***
- Cisco Network Security, Cisco Networking Academy ***Jan 2025***
- Cisco Certified Network Associate – CCNA, Cisco ***Jul 2024***

## TRAININGS

- **Cybertalents Universities Penetration Testing Bootcamp** – Cybertalents (Remote) ***Nov 2025 – Dec 2025***
- **ITI Summer Cybersecurity Program** – Information Technology Institute (Hybrid), Benha, Qalyubia, Egypt ***Sep 2025 – Nov 2025***
- **Introduction to Cybersecurity Bootcamp** – Cybertalents (Remote) ***Dec 2024 – Jan 2025***
- **Networking and Cloud Summer Training** – Huawei (Hybrid), Cairo, Egypt ***Sep 2023 – Nov 2023***

## EDUCATION

**Bachelor of Computer Science** – Benha University (BFCAI), Benha, Qalyubia, Egypt ***Oct 2022 – Jul 2026***
**Major: Information Security & Digital Forensics | GPA: 3.7/4.0**

## LANGUAGES

**Arabic: Native | English: C1**