

Ahmed Emad Nasr

SOC Analyst

ahmedemadeldeen77@gmail.com | +20 101 397 2690 | Benha, Qalyubia, Egypt

[LinkedIn](#) [Portfolio](#) [GitHub](#)

SUMMARY

SOC Analyst Tier 1 and Junior Incident Response Analyst with hands-on experience through DEPI, ITI, SOC projects, and home labs. Skilled in SIEM/EDR investigations, alert triage, log and IOC analysis, and incident handling. Open to remote, on-site, and relocation.

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

- Member of GDG Cybersecurity Club; awarded the *Best Technical Award*; participated in national and university CTF competitions.

EXPERIENCE

Incident Response Analyst Intern

Jan 2026 – Present

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

- Completing hands-on labs on LetsDefend and TryHackMe, focusing on alert triage, incident handling, and the IR lifecycle.
- Implementing a DEPI graduation project using ELK SIEM, Wazuh EDR, Suricata, and Sigma rules.

Information Security Analyst Intern

Jun 2025 – Dec 2025

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

- Solved hands-on cybersecurity labs focusing on malware analysis, SIEM investigations, and the Security Operations Center lifecycle.
- Developed a DEPI capstone project involving initial triage and SOC engineering using Wazuh, Zeek, and YARA rules.

PROJECTS

Insider Threat Detection & Deception [\[Project Link\]](#)

Jan 2026 – Present

- Deployed Wazuh SIEM with honey tokens, pfSense firewall, Suricata, and YARA rules, reducing false positive alerts by 7%.

Malware Analysis and Prevention Strategy (Wazuh SIEM) [\[Project Link\]](#)

Feb 2026 – Present

- Built a malware analysis lab using Wazuh, VirusTotal, and sandboxing techniques to identify malicious behavior and IOCs.

SOC Environment [\[Project Link\]](#)

Nov 2025 – Dec 2025

- Deployed Wazuh with pfSense firewall, Suricata, and automated YARA rule updates, reducing false positive alerts by 9%.

Malware Analysis & Threat Intelligence Tool [\[Project Link\]](#)

Jun 2025 – Jul 2025

- Built a static malware analysis tool integrating VirusTotal and Hybrid Analysis, reducing phishing alert false positives by 10%.

CERTIFICATIONS

eJPT v2 (eLearnSecurity Junior Penetration Tester) – INE

Feb 2026

Information Security Analyst & Forensics Investigator – DEPI

Jan 2026

SOC Analyst Path Level 1 & Level 2 – TryHackMe

Aug 2025

HCIA-Cloud Computing V5.0 – Huawei ICT Academy

Jul 2025

ECIR Preparation Course – Netriders

May 2025

Cisco Certified Junior Cybersecurity Analyst – Cisco

Mar 2025

HCIA-Datcom V1.0 – Huawei Talent Online

Aug 2024

Cisco Certified Network Associate (CCNA 200-301)

Jul 2024

SKILLS

SIEM (Wazuh, ELK) | EDR (Wazuh) | Incident Response | Alert Triage | Log and IOC Analysis | IDS/IPS (Suricata) | Network Traffic Analysis (Wireshark, Zeek) | Vulnerability Assessment (Nessus) | Active Directory | Malware Analysis (Basic) | Phishing Analysis