Ahmed Emad Nasr

SOC Analyst Tier 1 | Junior Incident Response Analyst

ahmedemadeldeen77@gmail.com | +20 101 816 6445 | Benha, Qalyubia, Egypt, 13511 (Open to Remote, On-site, Relocation)

LinkedIn Portfolio GitHub

SUMMARY

SOC Analyst Tier 1 and Junior Incident Response Analyst with hands-on experience through DEPI and ITI programs, SOC lab environments, SOC projects, and CTF competitions. Skilled in SIEM and EDR investigations, alert triage, log and IOC analysis, and incident handling aligned with the Incident Response Lifecycle. Actively pursuing continuous learning and open to relocation to support enterprise-scale security operations.

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, TryHackMe, and Hack The Box, focusing on alert triage, incident handling and IR lifecycle.
- Implementing a DEPI graduation project simulating end-to-end SOC monitoring 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 investigation and 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 ELK SIEM with honey tokens, pfSense firewall, Suricata, Yara rules, and threat emulation scenarios, reducing insider threats by 7%.

Malware Analysis and Prevention Strategy (Wazuh SIEM) [Project Link] ***Feb 2026 – present***

- Conducted static and dynamic malware analysis using Wazuh, VirusTotal and sandboxing techniques to identify malicious behavior and IOCs.

SOC Environment [Project Link] ***Nov 2025 – Dec 2025***

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

Malware Analysis & Threat Intelligence Tool [Project Link] ***Jun 2025 – Jul 2025***

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

SKILLS

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

CERTIFICATIONS

Ejpt v2 (eLearnSecurity Junior Penetration Tester) – INE [Verification] ***Feb 2026***

Information Security Analyst & Forensics Investigator – DEPI [Verification] ***Jan 2026***

HCCDA-Tech Essentials – Huawei ICT Academy [Verification] ***Sep 2025***

SOC Analyst Path Level 1 & Level 2 – TryHackMe [Verification] ***Aug 2025***

HCIA-Cloud Computing V5.0 – Huawei ICT Academy [Verification] ***Jul 2025***

ECIR Preparation Course – Netriders [Verification] ***May 2025***

Cisco Certified Junior Cybersecurity Analyst – Cisco [Verification] ***Mar 2025***

HCIA-Datacom V1.0 – Huawei Talent Online [Verification] ***Aug 2024***

Cisco Certified Network Associate (CCNA 200-301) [Verification] ***Jul 2024***