# Ahmed Emad Nasr

SOC Analyst | Incident Response Analyst

ahmed.em.nasr@gmail.com | +20 101 397 2690 | Benha, Qalyubia, Egypt 13511

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 a 6-month DEPI training program, solving TryHackMe labs simulating the full Incident Response (IR) lifecycle.
- Implementing a DEPI graduation project using ELK SIEM, Wazuh EDR, and Suricata, reducing false positive alerts by 9%.

**Information Security Analyst Intern** *Jun 2025 – Dec 2025*

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

- Completed a 6-month DEPI training program, solving TryHackMe labs simulating the full SOC lifecycle, and alert triage.
- Developed a DEPI capstone project using Wazuh, Suricata, VirusTotal, and YARA rules, increasing detection capabilities by 12%.

## 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*

**Cisco Certified Junior Cybersecurity Analyst** – Cisco *Mar 2025*

**HCIA-Cloud Computing V5.0** – Huawei ICT Academy *Aug 2024*

**HCIA-Datacom V1.0** – Huawei ICT Academy *Aug 2023*

**Cisco Certified Network Associate (CCNA 200-301)** *Jul 2023*

## TECHNICAL SKILLS

**Tools & Platforms:** SIEM, EDR, Wazuh, ELK Stack, Suricata, pfSense, VirusTotal, YARA

**Security Operations:** Incident Response, Alert Triage, Log Analysis, IOC Identification, Phishing Analysis, Vulnerability Assessment

**Networking:** Network Traffic Analysis (NTA), IDS/IPS, TCP/IP, Routing & Switching

**Soft Skills:** Communication, Collaboration, Problem Solving, Critical Thinking, Attention to Detail, Adaptability, Time Management

## VOLUNTEER EXPERIENCE

**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 a 40% improvement in practical skills and an average rating of 4.9/5.

## 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***

**HCIA-Cloud Computing V5.0** – Huawei ICT Academy ***Aug 2024 – Sep 2024***

**Huawei Routing & Switching Summer Training** – Huawei ***Aug 2023 – Sep 2023***

## AWARDS & ACHIEVEMENTS

- Scored **95%** in eJPT v2 (eLearnSecurity Junior Penetration Tester).
- Received the Best Cybersecurity Technical Award from GDG Cybersecurity Club — ranked 1st among 200 participants.
- Ranked **44th out of 400 participants** in a joint CTF competition between ITI and Cybertalents.
- Ranked **Top 5** in a National University CTF Competition, Egypt.
- Scored **98%** in Cisco Certified Network Associate (CCNA 200-301).

## LANGUAGES

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