# Ahmed Emad Nasr

SOC Analyst | Incident Response Analyst
Email: ahmed.em.nasr@gmail.com | Phone: +20 101 397 2690 | Location: Cairo, Egypt
LinkedIn: linkedin.com/in/Ahmed-Emad-Nasr | Portfolio: Ahmed-Emad-Nasr.github.io/AhmedEmad-Portfolio

## Professional 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 activities. Passionate about improving detection accuracy and reducing alert fatigue through continuous tuning and threat-driven analysis.

## Education

**Bachelor of Computer Science**
Benha University, Faculty of Computer Science and Artificial Intelligence, Benha, Qalyubia, Egypt ***Oct 2022 – Jul 2026***
**Major:** Information Security and Digital Forensics – **GPA:** 3.7/4.0

## Professional Experience

**Incident Response Analyst Intern** ***Jan 2026 – Present***
Digital Egypt Pioneers Initiative (DEPI) – Hybrid, Cairo, Egypt

- Completed a 6-month DEPI training program, solving TryHackMe labs that simulate the full Incident Response (IR) lifecycle.
- Implemented 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

- Analyzed and triaged simulated security alerts within TryHackMe environments, applying core SOC lifecycle methodologies.
- Developed a DEPI capstone project using Wazuh, Suricata, VirusTotal, and YARA rules, increasing detection capabilities by 12%.

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

- Delivered cybersecurity training to 120+ learners, resulting in a 40% improvement in practical skills and rating of 4.9/5.

## 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***

- Designed an isolated malware analysis environment enabling behavioral analysis, IOC extraction, and detection validation.

**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%.

## 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***
**Huawei Certified ICT Associate (HCIA) Cloud Computing V5.0 & Datacom V1.0** – Huawei ICT Academy ***Sep 2024***
**Cisco Certified Network Associate (CCNA 200-301)** ***Jul 2023***

## Technical Skills

**Tools & Platforms:** Wazuh, ELK Stack, Splunk, Sysmon, Suricata, pfSense, VirusTotal, YARA, Wireshark
**Security Operations:** Incident Response, Threat Hunting, Alert Triage, Detection Engineering, IOC Analysis, Playbook Execution
**Frameworks & Methodologies:** MITRE ATT&CK, Incident Response Lifecycle
**Networking:** TCP/IP, Network Traffic Analysis (NTA), IDS/IPS

## Languages

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

## 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).