Ahmed Emad Nasr

SOC Analyst | Incident Response Analyst

ahmed.em.nasr@gmail.com | +20 101 816 6445 | Cairo, Egypt, 11765

GitHub: github.com/Ahmed-Emad-Nasr | LinkedIn: linkedin.com/in/ahmed-emad-nasr | Portfolio: ahmed-emad-nasr.github.io/Portfolio

SUMMARY

SOC Analyst with hands-on experience across 10+ SOC training programs and 200+ simulated alerts and cases (DEPI, ITI, home labs, projects). Skilled in monitoring, detection, SIEM/EDR investigations, alert triage, IOC analysis, and log analysis across the incident response lifecycle. Focused on improving detection accuracy, accelerating incident response, and strengthening blue team resilience.

EDUCATION

Bachelor of Computer Science – Information Security and Digital Forensics *Oct 2022 – Jul 2026*

Benha University, Benha, Qalyubia, Egypt – GPA: 3.7/4.0

EXPERIENCE

Incident Response Analyst Intern *Jan 2026 – Present*

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

- Investigated and triaged security alerts, performing the full Incident Response lifecycle in SOC environments.
- Tuned SIEM (ELK, Wazuh, Suricata), which improved alert quality and cut false positives by 50%.

CyberTalents & ITI Cybersecurity Training Program *May 2025 – Jan 2026*

CyberTalents – Hybrid, Benha, Qalyubia, Egypt

- Identified and validated 15+ vulnerabilities across various labs and CTF competitions, demonstrating practical penetration testing capabilities.
- Applied comprehensive security methodologies, including information gathering, network scanning, and vulnerability assessment.
- Conducted web application security testing using exploitation and post-exploitation techniques in INE lab environments.

Information Security Analyst Intern *Jun 2025 – Dec 2025*

Digital Egypt Pioneers Initiative (DEPI) – Remote

- Analyzed and triaged simulated SOC alerts using structured workflows, improving consistency and response time.
- Developed a detection lab using Wazuh, Suricata, VirusTotal, and YARA rules, which increased detection coverage by 12%.

Volunteer Cybersecurity Instructor & Technical Trainer *Oct 2024 – Oct 2025*

Google Developer Groups (GDG) – Hybrid, Benha, Qalyubia, Egypt

- Delivered 35+ structured cybersecurity sessions to 120+ learners, which achieved a 4.9/5 rating and raised lab scores by 40%.

PROJECTS

Insider Threat Detection & Deception GitHub Repository *Jan 2026 – Present*

- Designed an insider threat deception environment with honeytokens and Wazuh SIEM.
- Integrated pfSense and Suricata for real-time monitoring, reducing false positives by 12 alerts per week.

Malware Analysis and Prevention Strategy (Wazuh SIEM) GitHub Repository *Feb 2026 – Present*

- Developed and deployed an isolated malware lab using YARA rules and threat intelligence feeds for IOC extraction and analysis.
- Performed static and dynamic malware analysis, analyzing 5+ ransomware samples, enhancing detection logic.

SOC Environment GitHub Repository *Nov 2025 – Dec 2025*

- Deployed a SOC stack using Wazuh, Suricata, and pfSense, which enabled centralized logging and detection.
- Simulated 50+ attacks to validate detection rules, improving incident response readiness through detection tuning.

Threat Intelligence Tool (Python, VirusTotal & Hybrid Analysis) GitHub Repository *Aug 2025 – Oct 2025*

- Enhanced a threat intelligence tool integrating VirusTotal and Hybrid Analysis APIs, accelerating email analysis by 12%
- Automated data collection and analysis, reducing manual investigation effort and accelerating threat analysis.

SKILLS

SIEM & Security Monitoring: Wazuh, ELK Stack, Splunk, Suricata, Zeek, pfSense, Sysmon, Nessus, Volatility, Security Onion, Wireshark, YARA

Incident Response & Threat Detection: Monitoring, Detection, Alert Triage, IOC Analysis, Log Analysis, Threat Hunting, Malware Analysis

Programming & Automation: Python, Bash, PowerShell, Regex, C++, HTML, CSS, JavaScript, TypeScript

Networking & Security: TCP/IP, VPN, Packet Analysis, IDS/IPS

Soft Skills: Analytical Thinking, Problem Solving, Team Collaboration, Communication, Adaptability, Attention to Detail

CERTIFICATIONS

- **eCIR Preparation (eLearnSecurity Certified Incident Responder)**
- **Information Security Analyst & Forensics Investigator** – DEPI
- **HCCDA-Tech Essentials Course** – Huawei ICT Academy
- **HCIA-Datacom V1.0 Course** – Huawei Talent Online
- **eJPT v2 (eLearnSecurity Junior Penetration Tester)** – INE
- **SOC Analyst Path Level 1 & Level 2** – TryHackMe
- **HCIA-Cloud Computing V5.0 Course** – Huawei ICT Academy
- **Cisco Certified Network Associate (CCNA 200-301)**

LANGUAGES

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