

# أحمد عماد نصر

## SOC Analyst Tier 1 | Junior Incident Response Analyst

Email: ahmedemadeldeen77@gmail.com | Phone: +20 101 816 6445 | Benha, Qalyubia, Egypt

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

### الملخص

محلل SOC Tier 1 ومحلل استجابة للحوادث (Junior) يمتلك خبرة عملية من خلال برامج DEPI وITI، ومشاريع SOC، ومنافسات CTF. لديه خبرة في SIEM وEDR والتحقيق في الحوادث الأمنية وفق Response Incident Lfecycle. ملتزم بالتعلم المستمر ومتاح للانتقال للمساهمة في عمليات الأمن المؤسسية.

### الخبرة العملية

محلل استجابة للحوادث - متدرب *Jan 2026 – Present*

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

- تنفيذ معامل عملية على LetsDefend وTryHackMe وBox The Hack مع التركيز على Triage Alert وHandling Incident وResponse Incident وLfecycle.
- تنفيذ مشروع تخرج DEPI لمحاكاة Monitoring SOC متكامل باستخدام SIEM ELK وEDR Wazuh وSuricata وSigma وRules.

محلل أمن معلومات - متدرب *Jun 2025 – Dec 2025*

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

- حل معامل عملية في الأمن السيبراني مع التركيز على Analysis Malware وتحقيقات SIEM وSOC وLfecycle.
- تنفيذ مشروع Capstone يشمل Triage Initial وEngineering SOC باستخدام Wazuh وZeek وYARA وRules.

### المهارات

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

### المشاريع

SOC Environment with Wazuh [Project Link](#) *Nov 2025 – Dec 2025*

- نشر SIEM Wazuh وEDR مع Firewall pfSense وأتمتة تحديثات YARA وSuricata.

ELK-Based SOC [Project Link](#) *Aug 2025 – Sep 2025*

- نشر SIEM ELK مع Honeypots وFirewall pfSense وZeek وRules Sigma وسيناريوهات Threat Emulation.

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

- بناء أداة Analysis Malware Static باستخدام Python مع دمج VirusTotal وHybrid وAnalysis.

### التعليم

بكالوريوس علوم الحاسب

Benha University, Faculty of Computers and Artificial Intelligence *Oct 2022 – Jul 2026*

**Major:** Information Security and Digital Forensics – **GPA:** 3.7/4.0

- عضو Club Cybersecurity GDG وحاصل على Award Technical Best والمشاركة في مسابقات CTF.

### الشهادات

Digital Egypt Pioneers Program (DEPI) – Information Security Analyst & Forensics Investigator (MCIT) [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*

Cisco Network Security Essentials – Cisco [Verification](#) *Jan 2025*

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

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

التدريبات

Cybertalents Universities Penetration Testing Bootcamp – Cybertalents	Nov 2025 – Dec 2025
ITI Summer Cybersecurity Program – Information Technology Institute	Sep 2025 – Nov 2025
Introduction to Cybersecurity Bootcamp – Cybertalents	Nov 2024 – Jan 2025

الجوائز والإنجازات

- الحصول على Award Technical Cybersecurity Best في Cybersecurity GDG Club.
- المركز 44 من أصل 400 مشارك في مسابقة CTF بين ITI وCybertalents.
- المركز الخامس في Competition CTF University National في Egypt.
- تدريب أكثر من 120 متدرباً في مجال الأمن السيبراني.

اللغات

العربية: Native – الإنجليزية: Professional Working Proficiency (C1)