

أحمد عماد نصر

SOC Analyst Tier 1 | Junior Incident Response Analyst

Email: ahmeddemadeldeen77@gmail.com | Phone: +20 101 816 6445 | Benha, Qalyubia, Egypt

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

المؤهلات

محلل SOC Tier 1 و محلل استجابة للحوادث (Junior) يمتلك خبرة عملية من خلال برامج DEPI و ITI، ومشاريع، SOC و منافسات CTF. لديه خبرة في SIEM و EDR والتحقيق في الحوادث الأمنية وفق LifeCycle. ملتزم بالتعلم المستمر و متاح للانتقال للمساهمة في عمليات الأمان المؤسسية.

الخبرة العملية

محلل استجابة للحوادث - متدرب	Jan 2026 – Present
Digital Egypt Pioneers Initiative (DEPI) – Hybrid, Cairo, Egypt	
<ul style="list-style-type: none">LifeCycle, Response Incident Handling Incident Triage Alert مع التركيز على Box The Hack, TryHackMe, LetsDefendRules, Sigma, Suricata و EDR Wazuh و SIEM ELK Monitoring SOC متكامل باستخدام DEPI لحاسة	تنفيذ معامل عملية على التركيز على
	تنفيذ مشروع تخرج
محلل أمن معلومات - متدرب	Jun 2025 – Dec 2025
Digital Egypt Pioneers Initiative (DEPI) – Remote, Cairo, Egypt	
<ul style="list-style-type: none">LifeCycle, SOC و SIEM Analysis Malware و تحليلاتRules, YARA, Zeek, Wazuh Engineering SOC, Triage Initial Capstone يشمل Wireshark Network Traffic Analysis (Wireshark) Malware Analysis (Basic) Phishing Analysis	حل معامل عملية في الأمن السييري مع التركيز على
	تنفيذ مشروع يشتمل

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
<ul style="list-style-type: none">YARA, Suricata و Firewall pfSense مع EDR و SIEM Wazuh نشر	أقامة تحديات
ELK-Based SOC Project Link	Aug 2025 – Sep 2025
<ul style="list-style-type: none">Emulation, Threat Rules Sigma و Firewall pfSense, Honeypots مع SIEM ELK نشر	و سيناريوهات
Malware Analysis & Threat Intelligence Tool Project Link	Jun 2025 – Jul 2025
<ul style="list-style-type: none">Analysis, Hybrid, VirusTotal و Python باستخدام Analysis Malware Static بناء أدلة	بنج

التعليم

بكالوريوس علوم الحاسوب

Benha University, Faculty of Computers and Artificial Intelligence [Verification](#) Oct 2022 – Jul 2026

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

- CTF، Award Technical Best Club Cybersecurity GDG عضو وحاصل على

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

- Club. Cybersecurity GDG Award Technical Cybersecurity Best الحصول على جائزة أفضل تقنية في أمن المعلومات.
- .CyberTalents من أصل 400 مشارك في مسابقة CTF بين ITI و CyberTalents المركز 44.
- Egypt. – Competition CTF University National المركز الخامس في المسابقة الجامعية لـ CTF.
- تدريب أكثر من 120 متدربياً في مجال الأمن السيبراني.

اللغات

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