أحمد عماد نصر

SOC Analyst

Email: ahmed.em.nasr@gmail.com | Phone: +20 101 397 2690 | Cairo, Egypt

LinkedIn Portfolio

الملخص المهني

محلل مركز عمليات الأمن (SOC) يمتلك خبرة عملية من خلال برامج DEPI وITI ومشاريع SOC وبيئات Lab، Home لديه خبرة في تحقيقات SIEM وEDR، وفرز التنبيهات (Alert)، (Triage وتحليل السجلات وIOC، وأنشطة التعامل مع الحوادث. شغوف بتحسين دقة الاكتشاف وتقليل Fatigue Alert من خلال التحسين المستمر والتحليل المبني على التهديدات.

الخبرة العملية

متدرب محلل استجابة للحوادث *Jan 2026 – Present*

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

- إتمام برنامج تدريبي لمدة 6 أشهر يتضمن حل معامل TryHackMe التي تحاكي دورة حياة الاستجابة للحوادث بالكامل.
- تنفيذ مشروع تخرج باستخدام SIEM ELK وEDR Wazuh وSuricata مما ساهم في تقليل التنبيهات الخاطئة بنسبة 9%.

متدرب محلل أمن معلومات *Jun 2025 – Dec 2025*

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

- تحليل وفرز التنبيهات الأمنية داخل بيئات TryHackMe وتطبيق منهجيات SOC الأساسية.
- تطوير مشروع نهائي باستخدام Wazuh وSuricata وVirusTotal وYARA مما زاد قدرات الاكتشاف بنسبة 12%.

مدرب ومتطوع في الأمن السيبراني *Oct 2024 – Oct 2025*

Google Developers Group (GDG) and Science In Code (SIC) – Hybrid, Benha, Egypt

- تقديم تدريبات أمن سيبراني لأكثر من 120 متعلم مما أدى إلى تحسن المهارات العملية بنسبة 40% وتقييم 4.5/5.

المشاريع

Insider Threat Detection & Deception *Jan 2026 – Present*

Project Link

- نشر SIEM Wazuh مع Tokens Honey وpfSense وSuricata وقواعد YARA مما قلل False Positives بنسبة 7%.

Malware Analysis and Prevention Strategy *Feb 2026 – Present*

Project Link

- تصميم بيئة معزولة لتحليل البرمجيات الخبيثة تتيح التحليل السلوكي واستخراج IOC والتحقق من الاكتشاف.

SOC Environment *Nov 2025 – Dec 2025*

Project Link

- نشر Wazuh مع pfSense وSuricata وتحديثات YARA تلقائياً مما قلل التنبيهات الخاطئة بنسبة 9%.

التعليم

بكالوريوس علوم الحاسب

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

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

الشهادات

eJPT v2 – 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 & Datacom V1.0 – Huawei	Sep 2024
Cisco Certified Network Associate (CCNA 200-301)	Jul 2023

المهارات التقنية

Tools: Wazuh, ELK Stack, Splunk, Sysmon, Suricata, pfSense, VirusTotal, YARA, Wireshark

Security Operations: Incident Response, Threat Hunting, Alert Triage, Detection Engineering, IOC Analysis

Frameworks: MITRE ATT&CK, Incident Response Lifecycle

Networking: TCP/IP, Network Traffic Analysis, IDS/IPS

اللغات

العربية: اللغة الأم – English: C1

الجوائز والإنجازات

- تحقيق نسبة 95% في شهادة eJPT v2.
- الحصول على Award Technical Cybersecurity Best من GDG (المركز الأول من بين 200 مشارك).
- المركز 44 من أصل 400 مشارك في مسابقة CTF مشتركة بين ITI وCybertalents.
- ضمن أفضل 5 فرق في مسابقة CTF جامعية على مستوى مصر.
- تحقيق نسبة 98% في شهادة CCNA.