أحمد عماد الدين عبد المنعم

Analyst Response Incident Junior | 1 Tier Analyst SOC

Email: ahmedemadeldeen77@gmail.com **Phone:** +20 101 816 6445 **Location:** Cairo, Egypt, 13511
LinkedIn: https://www.linkedin.com/in/0x3omda **Portfolio:** https://eng-ahmed-emad.github.io/AhmedEmad-Dev

الملخص

محلل 1 Tier SOC ومحلل Junior Response Incident يمتلك خبرة عملية في SOC 1 Tier Operations، التدريبات العملية، المشاريع، Alert Triage، والتحقيق في الحوادث الأمنية. يمتلك خبرة قوية في SIEM، EDR، IDS/IPS، Log Analysis، ويطبّق MITRE ATT&CK Framework وPlaybooks SOC لتقليل MTTD بنسبة 12% وتقليل False Positives بنسبة 14%، مع الالتزام بـ SLA وتحقيق Containment وRecovery فعّالين.

الخبرة العملية

محلل الاستجابة للحوادث – متدرب ***Dec 2025 – Present***
Amit Learning (Hybrid) – Nasr City, Cairo, Egypt

- التحقيق في الحوادث الأمنية باستخدام Wazuh، SIEM مما أدى إلى تقليل MTTD بنسبة 12% وتحسين دقة التنبيهات بنسبة 18% ضمن SLA.
- قيادة جلسات مراجعة Playbooks أسبوعية مع فريق SOC مكوّن من 5 أعضاء، مما ساهم في تسريع Containment Incident بنسبة 10%.

محلل أمن معلومات & محقق أدلة رقمية – متدرب ***Jun 2025 – Dec 2025***
Global Knowledge (Hybrid) – Heliopolis, Cairo, Egypt

- إضافة 12 Technique ATT&CK MITRE جديدة إلى Suricata Rules، مما رفع Coverage Detection من 68% إلى 86%.
- تقليل False Positives بنسبة 14%، مما وفر حوالي 120 ساعة عمل شهريًا (9,600$ تكلفة تشغيلية).

المهارات

المهارات التقنية: Incident Response SIEM Operations EDR Investigation Log and IOC Analysis Vulnerability Assessment IDS/IPS
المهارات الشخصية: Analytical Thinking Problem Solving Team Collaboration Communication Attention to Detail Critical Thinking

المشاريع

Enterprise SOC Lab with Wazuh ***Nov 2025 – Dec 2025***
Project Link

- نشر Wazuh 3.4 مع Suricata وأتمتة تحديثات YARA، مما قلل Alerts False بنسبة 13% وخفّض زمن Triage بمقدار 5.2 ساعة.

ELK-Based SOC ***Aug 2025 – Sep 2025***
Project Link

- تحسين Accuracy Correlation Log من 71% إلى 88% عبر 12 مصدر Logs، وتقليل زمن التحقيق بنسبة 13%.

Malware Analysis & Threat Intelligence Tool ***Jun 2025 – Jul 2025***
Project Link

- بناء أداة Analysis Malware Static مدمجة مع VirusTotal وAnalysis Hybrid لإثراء IOCs وتسريع Triage Incident.

التعليم

بكالوريوس علوم الحاسب ***Oct 2022 – Jul 2026***
Benha University – Faculty of Computers and Artificial Intelligence
Major: Information Security and Digital Forensics – **GPA:** 3.7/4.0
الأنشطة: Member of GDG Cybersecurity Club, SIC Cybersecurity Club, CTF Competitions (National & University Level)

الشهادات

Digital Egypt Pioneers Program (DEPI) – Information Security Analyst & Forensics Investigator (MCIT)	*Jan 2026*
SOC Analyst Path Level 1 & Level 2 – TryHackMe	*Aug 2025*
ECIR Preparation Course – Netriders	*May 2025*
Cisco Certified Junior Cybersecurity Analyst – Cisco	*Mar 2025*
Cisco Network Security Essentials – Cisco Networking Academy	*Jan 2025*
CompTIA Security+ (SY0-701) – Netriders	*Nov 2024*
Cisco Certified Network Associate (CCNA 200-301)	*Jul 2024*

العمل التطوعي

مدرب أمن سيبراني ومتطوع تقني (Hybrid) ***Oct 2024 – Oct 2025***
Google Developers Group (GDG) & Science In Code (SIC) – Benha, Egypt

- تقديم تدريبات Cybersecurity لأكثر من 120 متدربًا، مع تحسين المستوى العملي بنسبة 40% وتقييم رضا 5.4/5.

التدريبات

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*

اللغات

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