

أحمد عماد الدين عبد المنعم

محلل مركز العمليات الأمنية (SOC Analyst)

محلل الاستجابة للحوادث (Incident Response Analyst)

البريد الإلكتروني: ahmedemadeldeen77@gmail.com الهاتف: +20 101 397 2690 الموقع: القاهرة، مصر الرمز البريدي: 13511
eng-ahmed-emad.github.io Portfolio: github.com/Eng-Ahmed-Emad GitHub: linkedin.com/in/0x3omda LinkedIn:

الملخص

محلل SOC و Incident Response طموح، لديه خبرة عملية في مراقبة الأمن، فرز التنبيهات، التحقيق في الحوادث، التحليل الجنائي الرقمي، وتحليل البرمجيات الخبيثة. متمكن من SIEM، log operations، rule correlation، IDS/IPS tuning، firewall management، hardening، monitoring EDR، و حقق تقليلاً بنسبة 30% في False Positives وتسريع اكتشاف الحوادث بنسبة 20%. لديه خبرة في تطبيق MITRE framework ATT&CK و playbooks SOC، وتنفيذ مشاريع عملية في مجال الأمن السيبراني.

المهارات

المهارات التقنية: SIEM، IDS/IPS، Incident EDR، Threat Response، Hunting، Windows/Linux TCP/IP، MITRE Administration، Analysis، IOC ATT&CK،
المهارات الشخصية: التفكير التحليلي، حل المشكلات، العمل الجماعي، إدارة الوقت، التواصل التقني.

الخبرة العملية

محلل الاستجابة للحوادث
Pioneers Egypt Digital – (DEPI Learning Amit Initiative)، مدينة نصر
• التحقيق في الحوادث الأمنية والاستجابة لها باستخدام أدوات SIEM، مما أدى إلى تقليل MTTD بنسبة 20%.
محلل أمن معلومات
Pioneers Egypt Digital – (DEPI Knowledge Global Initiative)، القاهرة
• مراقبة الأحداث الأمنية وتحليل السجلات في بيئات مؤسسية، والتعامل مع أكثر من 50 تنبيه يومياً.

المشاريع

- Environment SOC
- Deception and Detection Threat Insider
- Tool Cryptography
- Framework Steganography
- Program Intelligence Threat and Malware

الشهادات

- TryHackMe – (Level Path Analyst SOC 2 & 1)
- Associate Network Certified Cisco – CCNA
- Academy Networking Cisco – Analyst Cybersecurity Junior Cisco
- Tester Penetration Junior eLearnSecurity – v2 eJPT
- HCCD Switching, & Routing Datacom, – Certifications ICT Huawei
- Academy Networking Cisco – (Intermediate) Security Network

التدريب

نوفمبر 2025 – ديسمبر 2025 CyberTalents – Bootcamp Testing Penetration Universities CyberTalents
سبتمبر 2025 – نوفمبر 2025 Institute Technology Information – Program Cybersecurity بنها (ITI)
ديسمبر 2024 – يناير 2025 CyberTalents – Bootcamp Cybersecurity to Introduction
سبتمبر 2024 – نوفمبر 2024 Huawei، القاهرة Training Summer Cybersecurity
سبتمبر 2023 – نوفمبر 2023 Huawei – Training Summer Cloud & Networking

الخبرة التطوعية

أكتوبر 2024 – أكتوبر 2025 مدرب أمن سيبراني – Group Developers Google (GDG)، بنها
يوليو 2025 – أغسطس 2025 متطوع تقني في الأمن السيبراني – Code In Science (SIC)، بنها

التعليم

بكالوريوس علوم الحاسب – جامعة بنها (BFCAI)، بنها، القليوبية، مصر
أكتوبر 2022 – حتى الآن

اللغات

- العربية – اللغة الأم
- الإنجليزية – C1