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 لينكدإن: linkedin.com/in/0x3omda
الموقع الشخصي: eng-ahmed-emad.github.io GitHub: github.com/Eng-Ahmed-Emad

---

الملخص المهني

- محلل مركز عمليات أمنية (SOC) واستجابة للحوادث بخبرة عملية في مراقبة الأمن، فرز التنبيهات، التحقيق في الحوادث، تحليل السجلات، وتحسين أداء SOC.
- متمكن من SIEM، correlation، IDS/IPS، firewall، EDR، Playbooks وأتمتة العمليات باستخدام أدوات مثل ELK، Wazuh، Splunk، Security Suricata، Onion pfSense.
- خبرة في تطبيق MITRE ATT&CK، تطوير Playbooks، وتحليل البرمجيات الخبيثة لتقليل MTTR وتسريع الاستجابة للحوادث.

الخبرة المهنية

محلل الاستجابة للحوادث ديسمبر 2025 – حتى الآن
مبادرة مصر الرقمية – Amit Learning، مصر

- تصميم ونشر 6+ Playbooks للاستجابة للحوادث، مما أدى إلى تقليل زمن الاستجابة بنسبة 20%.

مهندس أمن المعلومات يونيو 2025 – ديسمبر 2025
جلوبال نولدج، القاهرة

- مراقبة الأحداث الأمنية وتحليل السجلات، والتعامل مع 50+ تنبيه يوميًا.

الدورات والتدريب

- Bootcamp Pentesting Universities Cybertalents — نوفمبر 2025 – ديسمبر 2025
- برنامج الأمن السيبراني — ITI — سبتمبر 2025 – نوفمبر 2025
- Huawei — Training Summer Cybersecurity — سبتمبر 2024 – نوفمبر 2024

المشاريع

- بيئة مركز عمليات أمنية مصغّرة (Mini SOC Project)
- كشف التهديدات الداخلية والخداع الأمني
- أداة التشفير (Cryptography Tool)
- إطار إخفاء البيانات (Steganography Framework)
- برنامج تحليل البرمجيات الخبيثة واستخبارات التهديدات

المهارات

- **الأمن السيبراني واستجابة للحوادث:** SIEM، فرز التنبيهات، correlation، التحقيق في الحوادث، IDS/IPS، firewall، EDR، تطوير Playbooks، تحسين SOC.
- **الشبكات والأنظمة:** TCP/IP، DNS، DHCP، Active Directory، Windows Server، Linux، VPN، تحليل الشبكات.
- **استخبارات التهديدات:** IOC، MITRE Hunting، ATT&CK، إثراء السجلات، تحسين الإنذارات المؤتمتة.
- **المهارات الشخصية:** التواصل، التفكير التحليلي، حل المشكلات تحت الضغط، التوثيق الفني، العمل الجماعي، إدارة الوقت.

الشهادات

- TryHackMe — (Level Analyst SOC Certfiied (1 & 2
- Cisco — CCNA
- Academy Networking Cisco — Analyst Cybersecurity Junior Cisco
- eLearnSecurity — v2 eJPT
- HCCD Switching, & Routing Datacom, — Certfications ICT Huawei

---

الخبرات التطوعية

- **مدرب أمن سيبراني** — Group Developers Google، (GDG) بنها أكتوبر 2024 – أكتوبر 2025
  تقديم جلسات تدريبية لـ 50+ طالب حول SIEM واستجابة الحوادث.
- **متطوع تقني** — Code In Science، (SIC) بنها يوليو 2025 – أغسطس 2025
  تنظيم ورش عمل عملية لـ 30+ مشارك.

التعليم

بكالوريوس علوم الحاسب — أمن المعلومات والتحليل الجنائي الرقمي — جامعة بنها (BFCAI) أكتوبر 2022 - حتى الآن

اللغات

- العربية — اللغة الأم
- الإنجليزية — مستوى C1