# أحمد عماد الدين عبد المنعم

**محلل مركز العمليات الأمنية (SOC Analyst)**
**محلل الاستجابة للحوادث (Incident Response Analyst)**

البريد: ahmedemadeldeen77@gmail.com الهاتف: +20 101 397 2690 لينكدإن: linkedin.com/in/0x3omda
الموقع الشخصي: eng-ahmed-emad.github.io/AhmedEmad-Dev

## الملخص المهني

- محلل مركز عمليات أمنية (SOC) واستجابة للحوادث بخبرة عملية في اكتشاف التهديدات، التحقيق في الحوادث، تحليل السجلات، والمراقبة الأمنية.
- متمكن من إدارة أنظمة SIEM، فرز التنبيهات، correlation، الصيد عن التهديدات، وإنشاء لوحات المتابعة باستخدام أدوات مثل: ELK Wazuh، Stack، Splunk، Security Suricata، pfSense Onion.
- خبرة في تنفيذ الاستجابة للحوادث، جمع الأدلة، تحليل البرمجيات الخبيثة، واستخدام إطار MITRE ATT&CK لتحسين الاكتشاف وتقليل زمن الاستجابة.
- قدرة قوية على تحسين عمليات الـ SOC، إنشاء الـ Playbooks، أتمتة المهام، ودعم التحقيقات لتقليل MTTR وتعزيز الوضع الأمني.

## الخبرة المهنية

**محلل الاستجابة للحوادث — متدرب** ديسمبر 2025 -- حتى الآن
مبادرة مصر الرقمية – Amit Learning، مصر
- تصميم ونشر أكثر من ستة أدلة استجابة للحوادث (Incident Response Playbooks) مما حسّن سرعة التصعيد بنسبة 20%.

**مهندس أمن المعلومات — تدريب** يونيو 2025 -- نوفمبر 2025
جلوبال نولدج، القاهرة

**برنامج الأمن السيبراني الصيفي** يوليو 2025 -- يناير 2026
معهد تكنولوجيا المعلومات (ITI)

**مدرب أمن سيبراني**
مجموعة مطوري جوجل – بنها (GDG Banha)

**منشئ تحديات CTF — عمل حر (عن بُعد)**
Cohesion Cyber

## المشاريع

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

## المهارات الأساسية

- **عمليات الأمن والاستجابة للحوادث:** ضبط SIEM، فرز التنبيهات، correlation، الصيد عن التهديدات، التحقيق في الحوادث، تحليل البرمجيات الخبيثة، تقييم الثغرات، IDS/IPS، تقوية الجدران النارية، مراقبة EDR، تطوير Playbooks، تحسين الـ SOC.
- **الشبكات والأنظمة:** TCP/IP، DNS، DHCP Active، Directory Group، Policy Windows، Server لينكس، CCNA، تحليل الشبكات، أمن VPN.
- **استخبارات التهديدات:** تغذيات التهديدات، IOC، MITRE Hunting، ATT&CK، إثراء السجلات، الإنذارات المؤتمتة، التقارير.
- **المهارات الشخصية:** القيادة، التواصل، حل المشكلات، التكيّف، العمل الجماعي، التدريب، التوثيق.

## الشهادات

- EC-Council Incident Response (ECIR)
- TryHackMe — SOC Analyst Certfiied (Level 1 & 2)
- CCNA — سيسكو
- Cybersecurity Junior Analyst — Cisco Networking Academy
- eJPT v1 — eLearnSecurity
- CompTIA Security+ (SY0-601)

- **شهادات هواوي :ICT**، HCCD Switching، & Routing Datacom
- **برنامج الأمن السيبراني الصيفي — ITI** (2024 و2025)
- **معسكر Penetration+ Bootcamp Tester** — CyberTalents و ITI (أكتوبر 2025)

---

## التعليم

**بكالوريوس علوم الحاسب** أكتوبر 2022 -- حتى الآن
جامعة بنها — كلية الحاسبات والذكاء الاصطناعي — المعدل: 7.3 من 0.4
التخصص: أمن المعلومات والتحليل الجنائي الرقمي

---

## اللغات

- العربية — اللغة الأم
- الإنجليزية — مستوى C1 (متقدم)