

أحمد عماد الدين عبد المنعم

محلل أمن سيبراني | استجابة للحوادث | Specialist GRC

بريد: ahmedemadeldeen77@gmail.com هاتف: +20 101 397 2690
لينكدإن: [linkedin.com/in/0x3omda](https://www.linkedin.com/in/0x3omda) بورتفوليو: Portfolio

الملخص المهني

- محلل أمن سيبراني بخبرة في عمليات SOC، الاستجابة للحوادث، كشف التهديدات، والحوكمة والمخاطر والامتثال (GRC).
- متمكن من أنظمة (Wazuh, SIEM, ELK) وأدوات EDR، مع تطبيق إطار ATT&CK MITRE في التحليل والصيد.
- خبرة في التحليل الجنائي الرقمي، تحليل البرمجيات الخبيثة، ومراقبة الشبكات باستخدام منهجية Team Purple.
- معرفة قوية بـ ISO 27001, NIST CSF, CIS Controls, GDPR وتنفيذ التقييمات الأمنية والتدقيقات والسياسات.
- إنجازات: خفض MTTR بنسبة 25%، رفع دقة الكشف 30%، أتمتة مهام SOC بنسبة 20%.

الخبرة العملية

يونيو 2025 -- الآن

قائد فريق الأمن السيبراني
شركة Tech Terra - طنطا

- إدارة فرق SOC و Team Red وأمن السحابة.
- تطوير +6 Playbooks حسنت سرعة التصعيد 20%.
- دعم التقييمات والتدقيقات وفق ISO 27001 و NIST CSF.

يوليو 2025 -- يناير 2026

برنامج الأمن الصيفي -- ITI

معهد تكنولوجيا المعلومات - بنها

أبريل 2025 -- الآن

متدرب محلل أمن معلومات

شركة Knowledge Global - القاهرة

أغسطس 2025 -- سبتمبر 2025

تدريب أمن سحابة

شركة Huawei - القاهرة

أغسطس 2024 -- أكتوبر 2024

تدريب صيفي بالأمن السيبراني

شركة Huawei - القاهرة

المشروعات

- Project SOC Mini
- Deception & Detection Threat Insider
- Alignment Compliance & Policy
- Tool Cryptography
- Intelligence Threat & Analysis Malware

المهارات

- الأمن والاستجابة: Analysis Malware IDS/IPS, EDR, Hunting, Threat SIEM,
- GRC: Controls CIS Audits, Compliance GDPR, CSF, NIST, 27001 ISO Assessment, Risk
- التحليل الجنائي: Reconstruction Timeline Analysis, Packet & Disk Forensics, Memory
- الشبكات والأنظمة: CCNA-Level Server, Windows GPO, AD, DNS, TCP/IP,
- المهارات الشخصية: القيادة، التواصل، حل المشكلات، العمل الجماعي، التكيف

الشهادات

- Response Incident EC-Council - ECIR
- TryHackMe - L1 Analyst SOC Certified
- SEC504 SEC450, SANS
- CCNA | Security+ | CEH | v1 eJPT
- Expert HCCD Associate, ICT Datacom, Huawei:
- Program Cybersecurity ITI
- جاري الحصول: v4 ITIL LI, 27001 ISO

التعليم

2022 -- الآن

بكالوريوس علوم الحاسب
جامعة بنها - كلية الحاسبات والذكاء الاصطناعي
تخصص: أمن المعلومات والتحقيقات الرقمية
المعدل: 0.4 / 7.3

اللغات

- العربية: اللغة الأم
- الإنجليزية: C1 (متقدم)