أحمد عماد الدين عبد المنعم

محلل مركز العمليات الأمنية (SOC Analyst) | مهندس أمن سيبراني وحوكمة ومطابقة (GRC Specialist)

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

الملخص المهني

- مهندس أمن معلومات دقيق الملاحظة يتمتع بخبرة عملية في **اكتشاف التهديدات، والاستجابة للحوادث، وتحليل السجلات** باستخدام أدوات مثل **Wazuh وStack ELK وSuricata**.
- متمكن في إدارة أنظمة **SIEM**، وفرز التنبيهات، وعمليات **Hunting Threat**، مع تطبيق إطار عمل **MITRE ATT&CK** لتعزيز دقة الاكتشاف وتقليل زمن الاستجابة.
- يمتلك خبرة في أطر **الحوكمة والمخاطر والامتثال (GRC)** بما في ذلك **ISO 27001 وNIST CSF وCIS Controls**، مع دعم عمليات تقييم المخاطر ومواءمة السياسات.
- سجل قوي في تحسين **عمليات مركز العمليات الأمنية (SOC)** وأتمتة المهام لتقليل متوسط زمن الاستجابة (MTTR) وتحسين الكفاءة الأمنية الشاملة.

الخبرة المهنية

مهندس أمن سيبراني - عقد حر — مايو 2025 -- نوفمبر 2025
شركة تيرا تك، طنطا
- قاد فرق الأمن الزرقاء والحمراء والسحابية، لضمان تكامل الدفاعات وفعالية الاستجابة للحوادث.
- صمم ونفّذ أكثر من ستة **أدلة استجابة للحوادث (Playbooks)** مما أدى إلى تحسين سرعة التصعيد بنسبة **20%**.

محلل أمن معلومات - تدريب — أبريل 2025 -- حتى الآن
شركة جلوبال نولدج، القاهرة

مدرب في الأمن السيبراني — سبتمبر 2024 -- حتى الآن
مجموعة مطوري جوجل بنها (GDG Banha)

برنامج الأمن السيبراني الصيفي بمعهد تكنولوجيا المعلومات (ITI) — يوليو 2025 -- يناير 2026
معهد تكنولوجيا المعلومات، بنها

المشاريع

- **بيئة مركز عمليات أمنية مصغّرة (Mini SOC)** — بناء بيئة افتراضية لمركز عمليات أمنية متكامل مع نظام SIEM.
- **مشروع كشف التهديدات الداخلية والخداع الأمني** — تطوير نظام خداعي لاكتشاف التهديدات الداخلية.
- **مشروع مواءمة السياسات والامتثال** — ربط سياسات المؤسسة بعناصر معيار ISO 27001.
- **أداة التشفير** — تطوير وظائف التشفير وفك التشفير.
- **أداة تحليل البرمجيات الخبيثة واستخبارات التهديدات** — أتمتة تحليل البيانات وإعداد التقارير.
- **الموقع الشخصي** — معرض للمشاريع والشهادات المهنية.

المهارات الأساسية

- **عمليات الأمن والاستجابة للحوادث:** ضبط وتحسين SIEM، الصيد عن التهديدات، أنظمة EDR وIDS/IPS، تقوية الجدران النارية، تحليل البرمجيات الخبيثة.
- **الحوكمة والمخاطر والامتثال (GRC):** تقييم المخاطر، تطوير السياسات، ISO 27001، NIST CSF، تدقيقات الامتثال، GDPR، ضوابط CIS.
- **التحليل الجنائي الرقمي:** تحليل الأقراص والذاكرة، تحليل الحزم، إعادة بناء الخط الزمني، تحليل الذاكرة المتطايرة.
- **الشبكات والأنظمة:** TCP/IP، نظام أسماء النطاقات (DNS)، Active Directory، سياسات المجموعات، خوادم Windows، مستوى CCNA في الشبكات.
- **المهارات الشخصية:** القيادة، التواصل، حل المشكلات، التكيّف، العمل الجماعي، العمل الحر.

الشهادات

- **ECIR** — استجابة الحوادث من EC-Council
- **Analyst SOC Certfiied (المستوى 1 و2)** — TryHackMe
- **SEC450 SANS (أساسيات الفريق الأزرق) | SEC504 SANS (أدوات وتقنيات واستغلالات واكتشاف الحوادث)**
- **CCNA** — شهادة سيسكو للشبكات
- **Analyst Cybersecurity Junior** — أكاديمية سيسكو للشبكات
- **eJPT v1** — محلل اختراق مبتدئ من eLearnSecurity | **CEH** — الهاكر الأخلاقي المعتمد
- **CompTIA Security+ (SY0-601)**
- **شهادات هواوي:** Datacom، مساعد معتمد في الشبكات، وخبير شبكات معتمد (HCCD)
- **برامج الأمن السيبراني الصيفية بمعهد تكنولوجيا المعلومات** — فرع بنها (2024 و2025)

- **معسكر مختبر اختبار الاختراق المعتمد** — *CyberTalents* و*ITI* (أكتوبر 2025)
- قيد الإنجاز: **مدقق رئيسي لنظام ISO 27001 | أساسيات ITIL v4**

التعليم

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

اللغات

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