أحمد عماد الدين عبد المنعم

محلل مركز العمليات الأمنية (SOC) Analyst | محلل الاستجابة للحوادث Analyst) Response (Incident
الرمز البريدي: 13511 **الموقع:** Cairo, Egypt **الهاتف:** +201013972690 **البريد الإلكتروني:** ahmedemadeldeen77@gmail.com
LinkedIn: www.linkedin.com/in/0x3omda/ **Portfolio:** eng-ahmed-emad.github.io/AhmedEmad-Dev/

الملخص

محلل SOC ومحلل Response Incident يعمل على Security، Alert Monitoring، Triage والتحقيق في الحوادث داخل Center Operations Security (SOC). يمتلك خبرة في SIEM وIDS/IPS وEDR وتطبيق MITRE ATT&CK وPlaybooks SOC لتحسين Detection Accuracy وكفاءة الاستجابة بنسبة 30%.

الكفاءات الأساسية

SOC Monitoring | Incident Handling | Threat Detection | Log Correlation | Blue Team Operations | Vulnerability Assessment

المهارات

المهارات التقنية: SIEM EDR IDS/IPS Security Monitoring Alert Triage Incident Response Log Analysis IOC Analysis Threat Intelligence Vulnerability Assessment Network Security Malware Analysis Digital Forensics Packet Analysis

أنظمة التشغيل: Windows Linux (Ubuntu Kali CentOS)

البرمجة والسكربتنج: Python Bash PowerShell

أطر العمل الأمنية: MITRE ATT&CK NIST CSF Cyber Kill Chain

الأدوات: Splunk Wazuh ELK Kibana Suricata Sysmon YARA pfSense Wireshark Metasploit Burp Suite Nmap

المهارات الشخصية: Analytical Thinking Problem Solving Communication Teamwork Time Management Adaptability Leadership

الخبرة العملية

محلل الاستجابة للحوادث (متدرب) ***Dec 2025 – Current***
Amit Learning (Hybrid) – DEPI, Cairo, Egypt

- التحقيق في الحوادث باستخدام SIEM مما أدى إلى تقليل MTTD بنسبة 20%.
- تحسين Rules Correlation وتقليل False Positives بنسبة 30%.

محلل أمن معلومات (متدرب) ***Jun 2025 – Dec 2025***
Global Knowledge (Hybrid) – DEPI, Cairo, Egypt

- مراقبة أكثر من 50 تنبيه يوميًا وتحسين Analysis Log بنسبة 30%.
- تنفيذ Vulnerability Assessments وتقليل Exposure Risk بنسبة 20%.

مدرب أمن سيبراني ومتطوع تقني ***Oct 2024 – Oct 2025***
Google Developers Group (GDG) & Science In Code (SIC) – Benha, Qalyubia, Egypt

- تقديم تدريب عملي في Cybersecurity وFundamentals SOC لأكثر من 70 متدربًا، مما أدى إلى تحسين المستوى العملي بنسبة 40%.
- إدارة Labs تقنية وHands-on Exercises لرفع جاهزية الشهادات وتحسين Analysis Threat بنسبة 35%.

المشاريع

Wazuh SOC Environment ***Nov 2025 – Dec 2025***

- بناء Lab SOC ومحاكاة أكثر من 15 هجومًا وتحسين Triage Alert بنسبة 40%.

ELK SOC Environment ***Jun 2025 – Jul 2025***

- تحسين وقت التحقيق بنسبة 25% وزيادة دقة Correlation Log بنسبة 35%.

الشهادات

- Cisco Network Security *Mar 2025*
- Cisco Junior Cybersecurity Analyst *Jan 2025*
- SOC Analyst Path L1 & L2 *Aug 2024*
- CCNA *Jul 2024*

التعليم

بكالوريوس علوم الحاسب — Benha University ***Oct 2022 – Jul 2026***
Major: Information Security & Digital Forensics | **GPA:** 3.7/4.0

اللغات

العربية: Native | **الإنجليزية:** C1