Ahmed Emad Eldeen Abdelmoneam

Cairo & Banha, Egypt
Email: ahmedemadeldeen77@gmail.com
Phone: +20 101 397 2690
LinkedIn: https://www.linkedin.com/in/ahmed-emad-eldeen-a77420284
GitHub: https://github.com/Eng-Ahmed-Emad
TryHackMe: https://tryhackme.com/p/0x3omdaa

Professional Summary

Results-driven SOC Analyst with hands-on experience in threat detection, incident response, and cybersecurity operations. Skilled in log analysis, malware analysis, and vulnerability assessment, with a solid foundation in networking, programming, and digital forensics. Demonstrated ability to compete in CTF competitions, deliver technical training, and actively contribute to cybersecurity communities.

Skills

Security Operations: Threat Detection & Response, Log Analysis & Correlation, SIEM (Rule Tuning & Alerting), Endpoint Detection & Response (EDR), IDS/IPS, Firewall Management, Malware Analysis, Vulnerability Scanning
Networking & Infrastructure: Cisco CCNA, CCNA Security, CCNP Security, Group Policy, Windows Server, Active Directory, MCSA
Programming & Scripting: Python, C++, Bash, PHP, MySQL, HTML, CSS, JavaScript
Soft Skills: Teamwork, Communication, Problem Solving, Analytical Thinking, Attention to Detail, Time Management, Leadership, Critical Thinking, Integrity, Adaptability

Certifications

- CompTIA Security+ (SY0-601)
- Cisco Certified Network Associate (CCNA)
- Huawei Certified ICT Associate (Routing and Switching)
- Huawei Datacom Certification
- EC-Council Certified Incident Handler (ECIH)
- Certified Ethical Hacker (CEH) – EC-Council
- ITI Cybersecurity Summer Program

Projects

CTF Challenge Developer – Cyber Cohesions

- Designed and managed over 15 Capture the Flag (CTF) challenges simulating real-world attack scenarios, used in bootcamps and competitions by 200+ participants.

Professional Experience

SOC Analyst (Tier 1) & Cloud Security Engineer — *Terra Tech Company, Cairo, Egypt*

Aug 2025 – Present

- Monitored and analyzed 200+ daily security events using SIEM/EDR tools, improving threat detection accuracy by 30%.
- Conducted 10+ cloud infrastructure security assessments monthly, helping reduce cloud misconfigurations by 25%.
- Collaborated on 15+ incident investigations, contributing to a 40% reduction in mean time to detect (MTTD) and respond (MTTR).
- Tuned 50+ SIEM detection rules and enriched threat feeds, reducing false positives by 35%.

Information Security Analyst (Tier 1/2) – Internship *Global Knowledge, Cairo, Egypt*
Jul 2025 – Mar 2026

- Monitored 500+ security alerts weekly using SIEM tools, cutting average incident response time from 4 to 3.2 hours (20% improvement).
- Analyzed 100+ security incidents and performed triage/log reviews, improving threat containment efficiency by 25%.
- Supported vulnerability scans across 200+ assets, identifying and escalating 40+ critical issues.
- Contributed to implementation of endpoint protection policies, reducing malware infections by 15%.

Technical Cybersecurity Engineer *GDG On Campus, Banha, Egypt*
Mar 2023 – Present

- Delivered 6+ technical sessions to 50+ attendees, increasing engagement and knowledge retention by 40% (post-session surveys).
- Organized 15+ CTF challenges with realistic attack scenarios, attracting 200+ participants across Egypt.
- Participated in 10+ competitions, achieving top 10 ranking in 3 national-level events.

Education

Bachelor of Computer Science (GPA: 3.7)
Faculty of Computers and Artificial Intelligence, Banha University, Egypt
Oct 2022 – Present
Specialization: Information Security and Digital Forensics
Active Member, Student Union Council

Languages

- Arabic — Native
- English — C1 (Advanced)