Ahmed Emad Eldeen Abdelmoneam

Cairo, Egypt (Willing to Relocate)
Email: ahmedemadeldeen77@gmail.com Phone: +20 101 397 2690
LinkedIn: https://linkedin.com/in/ahmedemadeldeen
GitHub: https://github.com/Eng-Ahmed-Emad

Professional Summary

- SOC Analyst Cloud Security Engineer experienced in threat detection, incident response, and cloud security.
- Optimized detection rules, reducing false positives by 15% and improving threat visibility by 30%.
- Skilled in digital forensics, malware analysis, and automating SOC workflows, boosting team efficiency by 25%.
- Mentored junior analysts and implemented SOAR playbooks to enhance incident response.

Professional Experience

SOC Analyst and Cloud Security Engineer (Tier 1) Terra Tech Company, Tanta
Aug 2025 – Present

- Monitored 1,000+ daily security events, increasing high-confidence detections by 20%.
- Implemented cloud security posture management, reducing misconfigurations by 25% and cloud incidents by 20%.
- Automated incident response workflows, reducing MTTR by 18%.

Information Security Analyst – Intern (Tier 1) Global Knowledge, Cairo
Jul 2025 – Present

- Triaged 500+ weekly SIEM alerts, escalating confirmed incidents aligned with MITRE ATT&CK techniques.
- Automated alert enrichment and ticketing, reducing analyst overhead by 20%.

Cybersecurity Intern – Summer Program Information Technology Institute (ITI), Cairo
Aug 2025 – Sep 2025

- Completed six-week training in SOC operations, incident response, SIEM/EDR analysis, and penetration testing.
- Detected 20+ exploitable misconfigurations during Red Team labs; validated defenses in Purple Team exercises.
- Built and operated a mini SOC ingesting Windows, Linux, firewall, and IDS logs; mapped detections to MITRE ATT&CK, improving simulated MTTD by 25%.

CTF Challenge Creator Cyber Cohesions
2024 – 2025

- Designed 15+ cybersecurity challenges in exploitation, reverse engineering, and forensics, boosting participants' skills by 40%.

Projects

- **Malware Hash URL Scanner Tool**: Python Tkinter GUI integrating VirusTotal Hybrid Analysis APIs for faster malware triage.
- **SOC Automation Lab**: Automated log parsing and enrichment scripts integrating Splunk ELK, increasing SOC efficiency by 25%.
- **Cloud Honeypot Project**: Deployed AWS/Azure honeypots to monitor malicious activity and generate actionable threat intelligence.

Core Skills

Security Operations & Incident Response: Threat hunting, SIEM tuning, EDR, IDS/IPS, firewall hardening, malware analysis, forensic investigations, SOAR playbooks.
Digital Forensics: Disk & memory forensics, packet analysis, timeline reconstruction, volatile memory analysis (Volatility, Autopsy, FTK, EnCase).
Cloud Security: AWS Security Hub, Azure Defender, GCP SCC, CSPM, IAM hardening, CWPP.
Networking & Systems: TCP/IP, DNS, Active Directory, Group Policy, Windows Server, CCNA-level networking.
Programming & Automation: Python (automation & API integration), Bash, PowerShell, SQL.
Soft Skills: Problem-solving, analytical mindset, teamwork, communication, adaptability, time management, leadership.

Certifications

- CompTIA Security+ (SY0-601)
- eJPT v1 – eLearnSecurity Junior Penetration Tester
- Certified Ethical Hacker (CEH)
- SANS SEC450: Blue Team Fundamentals, SANS SEC504: Hacker Tools, Techniques, Exploits, and Incident Handling
- Cisco Certified Network Associate (CCNA)
- Huawei ICT Associate (Routing & Switching), Huawei Datacom Certification
- ITI Cybersecurity Summer Program

Education

Bachelor's in Computer Science (GPA: 3.7/4.0)
Faculty of Computers and Artificial Intelligence, Banha University (BFCAI) Oct 2022 – Present
Specialization: Information Security and Digital Forensics.

Languages

- Arabic: Native
- English: C1 (Advanced)