AHMED RAMADAN ABDELMORDI SALEM

SOC Analyst | CyberSecurity Enthusiast

Cairo,Egypt ☎ +20 12 835 378 89 ✉ ahmedramadanmain@gmail.com ✉ linkedin.com/ahmedramadan

✉ Ahmedramadan/portfolio

CAREER SUMMARY

Motivated and detail-oriented SOC Analyst with hands-on experience in SIEM (QRadar, Splunk), firewall management, and incident response gained through practical lab work and an intensive internship at IT Gate Academy in collaboration with Ain Shams University. Skilled in network monitoring, threat detection, and digital forensics, with a solid foundation in networking (CCNA) and system administration (MCSA, Linux). Demonstrates strong analytical and troubleshooting abilities, supported by scripting skills in Python and Bash. Committed to continuous learning and contributing to secure, resilient IT infrastructures.

EXPERIENCE / PROJECTS

SOC Analyst Internship Trainee - *IT Gate Academy (in collaboration with Ain Shams University)* *July 2024 - Aug 2025*

- **Gained hands-on experience in SIEM (IBM QRadar), firewall administration (FortiGate, Sophos), digital forensics, and incident response (ECIR).**
- **Conducted simulated attacks, threat detection, and vulnerability assessments.**
- **Managed network monitoring, log correlation, and alert triage in simulated SOC environments.**
- **Supported the analysis of security events and assisted in incident response playbooks.**

Cybersecurity Lab Projects (Self-Guided & Academic) *2024 – Present*

- **Built and maintained a virtual cybersecurity lab using Kali Linux, Windows Server, and Linux administration tools.**
- **Practiced Active Directory, DNS, DHCP, VPN, and security policy configurations.**
- **Conducted packet analysis using Wireshark and automated tasks using Bash scripting.**

Intrusion Detection System (IDS) Implementation and Analysis - (Graduation Project) OCT 2025

- **Deployed and configured Snort and Suricata for real-time network monitoring and attack detection.**
- **Integrated IDS alerts with QRadar SIEM and performed packet analysis using Wireshark.**
- **Simulated brute force and port scan attacks to validate detection rules and fine-tune alert accuracy.**
- **Documented findings and developed a mini SOC workflow for incident triage and response.**

SKILLS

- **SOC Tools: QRadar, Splunk**
- **Security Operations: Threat Detection, Incident Response, Log Analysis**
- **Network Security: Firewalls, IDS/IPS, Vulnerability Management**
- **Forensics & Analysis: Wireshark, Digital Forensics Tools**
- **Scripting: Python, Bash**
- **Systems: Windows Server, Linux, Active Directory**

LANGUAGES

- **Arabic (Native)**
- **English (Intermediate)**

SOFT SKILLS

- **Analytical & Problem-Solving Mindset**
- **Strong Communication & Team Collaboration**
- **Continuous Learning & Adaptability**

CERTIFICATIONS

- **Cybersecurity SOC Analyst** – IT GATE Academy
- **Cybersecurity SOC Analyst** – Ain Shams University
- **Introduction to Network Security** – Mahara-Tech
- **Introduction to Cybersecurity** – Cisco
- **Red Hat Administrator I (RHCSA Part 1)** – Mahara-Tech

Education

Bachelor's Degree in Computer Engineering and Telecommunication

Higher Institute of Engineering and Technology, Tanta

2021 – present