

AHMED RAMADAN ABD ELMORDI SALEM

Junior SOC Analyst | CyberSecurity Enthusiast

 Cairo, Egypt

 +20 12 835 378 89

 ahmedramadan@gmail.com

 www.linkedin.com/in/ahmed-ramadan-soc  <https://ahmedramadanmain.github.io/Portfolio/Ramadan>

CAREER SUMMARY

Junior SOC Analyst with hands-on experience in security monitoring, incident response, and log analysis using SIEM platforms such as IBM QRadar. Trained in network security, firewall administration, and digital forensics through academic labs and real-world simulations. Strong foundation in threat detection, incident handling, and SOC operations, seeking an entry-level SOC Analyst role to contribute to security operations and continuous improvement.

TECHNICAL 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

SOFT SKILLS

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

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.

Cyber Security Incident Response Analyst – Infrastructure & Security Track

Digital Egypt Pioneers Initiative (DEPI) – Ministry of Communications & Information Technology *DEC 2025 - Present*

- Studied cybersecurity foundations including threats, vulnerabilities, and incident handling.
- Assessed and prioritized security threats and analyzed vulnerabilities.
- Applied remediation techniques for identified security issues.
- Practiced SOC operations and the full incident response lifecycle (Detection, Containment, Eradication, Recovery).
- Handled simulated phishing, malware, network, email, and IDS/AV alerts.
- Performed log analysis, evidence collection, and secure handling procedures.
- Prepared incident reports and security briefs.
- Completed hands-on projects including a cybersecurity incident navigation project and a capstone project.

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

- Designed and implemented a custom Intrusion Detection System (IDS) for real-time network traffic monitoring and analysis.
- Captured and parsed network packets using SharpPcap and PacketDotNet to extract protocol, port, and payload features.
- Developed logic for detecting common attacks such as port scanning and brute-force attempts.
- Logged security events with detailed metadata to support SOC incident triage and investigation.
- Documented detection workflows and created a mini SOC-style incident response process.
- Implemented signature-based detection using Snort and Suricata rules stored and managed in a structured database.

CERTIFICATIONS & TRAINING

- Cybersecurity (SOC Analyst) Engineering Diploma
IT Gate Academy – In collaboration with Ain Shams University
- Cyber Security Incident Response Analyst
Digital Egypt Pioneers Initiative (DEPI) – MCIT (Ongoing)
- Cisco CCNA v7 – Coursework (Semester 1, 2, 3)
- Cybersecurity & Networking Courses – MaharaTech (Online)

LANGUAGES

- Arabic (Native)
- English (Intermediate)