AMR ATALLA

DETAILS

- +971-052-752-6229
- amrhatalla@gmail.com

LINKS

LinkedIn

LANGUAGES

English: Proficient (C2)

Arabic: First Language

PROFILE

Cybersecurity graduate (BSc, RIT 2025) with hands-on SOC experience in alert triage, log analysis, and incident response using tools like Suricata, Wireshark, and Kibana. Familiar with endpoint monitoring, network traffic analysis, and security hardening. Currently pursuing HackTheBox's CDSA (Certified Defensive Security Analyst), and CompTIA Security+. Seeking a Junior SOC Analyst position to apply and deepen technical defensive skills in a real-world environment.

EMPLOYMENT HISTORY

SOC Analyst Intern at DELL Technologies, Dubai

May 2024 — August 2024

- Triaged 40+ alerts/week using SIEM tools (Suricata, Kibana, Microsoft Sentinel), performing initial investigation and log analysis.
- Correlated events across multiple data sources (Windows Event Logs, firewall, IDS) to identify suspicious patterns
- Used Playbooks to respond to alerts.
- Participated in threat hunting initiatives using MITRE ATT&CK techniques and IOC matching

Penetration Tester Intern at TechZone, Dubai

June 2025 —September 2025

- Conducted internal/external vulnerability scans using Nmap.
- Exploited web app flaws (e.g., XSS, SQLi) and reported the findings with CVSS scoring
- Executed ARP spoofing and DNS starvation attacks in a segmented lab network
- Collaborated with Red Team to document attack paths and simulate social engineering vectors
- Recommended remediation plans and presented post-assessment evaluations to our managers.

EDUCATION

Bachelor of Science in Cybersecurity, Rochester Institute of Technology (RIT),

May 2021 — May 2025

Certifications

- CompTIA Security+
- CSDA (HackTheBox)

University Courses

Programming (Python, C, Java),

Routing and Switching

Network Services

Penetration Testing

Risk management for Information Security

Cyber Security Policy and Law

Introduction to Database and Data Modelling

Network Security & Forensics

Computer System Forensics

Web Application Security

Reverse Engineering

Cryptography

Authentication

Disaster Recovery/Incident Response

★ PROJECTS

Enterprise SOC Simulation

- Built and defended a virtual network simulating an SME environment
- Used Kibana and Suricata for intrusion detection and real-time log review
- Conducted live packet capture, log correlation, and threat remediation on virtual endpoints

Healthcare Risk Assessment

- Created a NIST-compliant risk plan for a hospital, including threat modelling, asset classification, and HIPAA mapping
- Delivered executive reporting and suggested mitigations for top 10 risk scenarios

CTF-Based Web Game (Capstone Project)

- Developed browser-based CTF platform integrating VM-based labs for student learning
- Gamified cybersecurity training using challenge tiers aligned with MITRE ATT&CK techniques
- Managed backend in Python and coordinated frontend with secure sandbox VMs

Incident Response & Disaster Recovery Plan (Capstone)

- Designed full IRP/DRP for a simulated ransomware incident targeting a finance firm
- Mapped recovery workflows to NIST 800-34 and business continuity planning standards

- Included escalation paths, comms templates, BIA, and recovery RTO/RPO metrics

SKILLS

SIEM & Detection:

Suricata, Snort, Splunk (basic), Kibana, Sysmon, Windows Event Logs, Zeek

SOC Tools & Platforms

TCPDump, Wireshark, Netcat, Nmap, Burp Suite

Operating Systems

Linux, Windows 10/11, macOS

Programming Languages

Python, C, Java

Database

MySQL

Virtualization

VMware, VirtualBox

Other

Visual Studio Code, Packet Analysis, Log Correlation, Threat Intelligence Reports