AMR ATALLA

DETAILS

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

LINKS

LinkedIn
https://www.amratalla.com

LANGUAGES

English: Proficient (C2)

Arabic: Native

PROFILE

Cybersecurity graduate (BSc, RIT 2025) and a SOC Analyst at IT Butler E-Services. Currently, I specialize in alert triaging, log analysis, and incident response.

I don't just watch alerts; I investigate them. Utilizing SIEM tools like *Elastic* and *Qradar*. *Darktrace* as an NDR, and *MS Defender as an EDR*. I dig deep into network traffic and computer registries to find what others might miss.

Additionally, I'm levelling up with CCNA and AS-200. I am actively learning, trying to leverage automation tools to increase efficiency and productivity and attempting to integrate AI into digital secuirty.

EMPLOYMENT HISTORY

SOC Analyst at It Butler E Services FZ LLC, Dubai

October 2025 —Present

Role: Active member of an MSSP 24/7 Security Operations Center (SOC) team, responsible for continuous threat monitoring, advanced investigation, and incident response, ensuring the integrity and security of client network environments.

- Threat Detection & Analysis: Analysed and triaged an average of 40+ security alerts weekly from the SIEM platform (QRadar/Elastic), effectively distinguishing between false positives and high-priority incidents to maintain optimal alert fidelity.
- Advanced Network Investigation: Leveraged Network Traffic Analysis (NTA) tools, specifically Darktrace, to conduct deep-dive investigations into complex network-level alerts, significantly improving the accuracy of true positive identification and enhancing response procedures.
- Incident Documentation & Reporting: Managed and documented over 30 investigation summaries per week within the GLPI ticketing system, ensuring meticulous tracking, clear communication of findings, and adherence to established compliance and reporting standards.

SOC Analyst Intern at DELL Technologies, Dubai

June 2025 —September 2025

- Triaged 20+ 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

SOC Analyst Intern at VaporVM, Dubai

February 2025 —April 2025

- Shadowed SOC analysts using Microsoft sentinel.
- 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

May 2024 — August 2024

- 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+
- ISC2 CC

PROJECTS

Home Lab SOC Simulation

- Set up a Wazuh home lab with 4 agents, including, windows server, ubuntu, Mac OS, and a windows machine.
- Used Suricata and snort for intrusion detection and real-time log review.
- Integrated Sysmon for more detailed end point system monitoring for windows end points.
- Conducted live packet capture, log correlation, and threat remediation on virtual endpoints.
- Simulated common attack types and analyzed the indicators via Wazuh to differentiate between the baseline and an IOC.

Healthcare Risk Assessment Project

- 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, coordinated frontend with secure sandbox VMs, and used a proxy server to communicate with the backend.

Incident Response & Disaster Recovery Plan

- 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:

Elastic/ELK, Wazuh, Splunk, Qradar

Detection:

Snort, Sysmon, Windows Event Viewer, Zeek, Darktrace

Tools & Platforms

TCPDump, Wireshark, Netcat, Nmap, Osquery

Operating Systems

Linux, Windows 10/11, macOS

Programming Languages

Python, C, Java

Database

MySQL

Virtualization

VMware, VirtualBox