Mohammad Hassan Al Nemer

SOC Analyst

📍 Beirut, Lebanon · ✉ maa264@usal.edu.lb · 📱 +96178830180

LinkedIn · GitHub · TryHackMe

PROFILE

Entry-level SOC Analyst with a solid foundation in cybersecurity, specializing in security risk assessments, threat detection, and incident response. Proficient in leveraging SIEM tools, intrusion detection systems, and vulnerability management platforms to identify, analyze, and mitigate security threats effectively. Experienced in network analysis, digital forensics, and penetration testing, with the ability to secure systems and reduce cyber-attack risks by implementing industry-standard security controls.

EDUCATION

University of Sciences and Arts in Lebanon

September 2021- July 2024 | GPA: 3.51

Relevant Coursework:

- *Ethical Hacking & Penetration Testing (EC-Council)*
- *Web Application Security (EC-Council)*
- *System and Network Administration*
- *Digital Forensic (EC-Council)*
- *Network Security*
- *Computer Networks (CCNA I, II, III)*
- *Information Security Management*

Certificates:

- TryHackMe SOC L1 learning path
- CCNA 1,2
- DFE EC- council
- EC-Council: Hands-on Vulnerability Management with QualysGuard
- Coursera: Azure Networking Fundamentals

Projects

- Completed SOC scenario “Phishing Unfolding” provided by TryHaskMe, by analyzing and reporting different phases of the breach.
- Configured virtualized services (AD, pfSense, CentOS, and PRTG Monitor) using VMware ESXi, focusing on access control, performance, and security.
- Conducted a vulnerability management program using QualysGuard, including scanning, prioritization, and remediation
- Developed a ransomware Incident Response Plan with a real-life attack scenario and mitigation steps.
- Conducted OWASP-based security testing, identifying and addressing web application vulnerabilities.
- Secured web apps by integrating ModSecurity with Nginx and OWASP Core Rule Set for attack mitigation.
- Implemented SAML-based single sign-on for secure authentication of web applications.

Skills

- Network and traffic analysis: Wireshark, Tcpdump, NetworkMiner.
- Threat detection and response: Snort, IDS/IPS, SIEM, Splunk, Wazuh, ELK stack .
- Vulnerability management: Nessus, Nmap, Qualys VMDR.
- Incident response and forensics: Autopsy, Redline, Volatility, FTK Imager.
- Programming and scripting: Python, Bash.
- Security frameworks and compliance: ISO 27001/27002, NIST, MITRE ATT&CK.
- Cloud Security: Basic knowledge in securing cloud environments like Azure and AWS.

Languages

- Arabic: Native
- English: Professional Working Proficiency