DAOUD ABU MADI

CYBER SECURITY ANALYST

+962-781537410 ☎
daoudjamalabumadi@gmail.com ✉
Amman , Jordan
GitHub & LinkedIn

ABOUT ME

Cybersecurity Specialist with practical experience in SOC operations, SIEM analysis, and threat detection. Ranked in the Top 2% on TryHackMe with over +90 labs completed, demonstrating strong technical and analytical skills of defensive security. Skilled in Splunk, Elastic Stack, malware analysis, and network security. Contributed to the development of QARK6 an open-source Android pentesting tool that automates vulnerability detection and PoC generation using Python and JADX, focusing on real-world mobile security flaws.

EDUCATION

Bachelor of Computer Science – Cybersecurity
Tafila Technical University | GPA: 77.55% (Very Good)
Oct 2021 – Jun 2025

Experience & Projects

07/2024 - Present
LetsDefend ,TryHackMe and HackTheBox

Security Operations Analyst (Intern / Training)

- Completed multiple SOC analyst labs with practical exercises in SIEM (Splunk, ELK), EDR, malware analysis, vulnerability management, and alert triage.
- Triaged and investigated 30+ weekly alerts in a simulated SOC environment, achieving 95% classification accuracy from LetsDefend.
- Gained hands-on experience with Splunk and Elastic Stack for log investigation, detection queries, and dashboard use.
- Applied MITRE ATT&CK, Pyramid of Pain, Cyber Kill Chain frameworks for incident analysis.

02/2025 - 06/2025
Mobile Security Developer (Academic Project)

QARK

- Developed QARK6 framework for automated .apk file and source code analysis, integrating decompilation and vulnerability pattern detection.
- Generated comprehensive HTML and CSV reports with detailed vulnerability tutorials explaining root causes and remediation steps.
- Achieved 60% reduction in manual scanning time and improved detection accuracy through multi-tool decompilation integration.

Technical Skills

- Operating Systems: Linux (System Administration – Udemy Certified), Windows, Active Directory.
- Networking: TCP/IP, OSI, Network Security, Cisco Fundamentals (CCNA – Self Study).
- SOC & Incident Response: Incident Handling (Hands-on Labs), Security Monitoring, Threat Detection, Malware Analysis (Static/Dynamic), Log Analysis, Basic Reporting.
- SIEM & Monitoring: Splunk (SPL Queries, Incident Handling), ELK/Elastic Stack (KQL Queries, Threat Hunting, Dashboards).
- Cybersecurity Frameworks: MITRE ATT&CK, Cyber Kill Chain, Unified Kill Chain, Diamond Model, Pyramid of Pain.
- Threat Hunting: Windows Event Logs (Sysmon, ETW), Hunting with Elastic, Splunk Investigations.
- Offensive Security: Junior Web Penetration Testing (91% progress – TryHackMe), Enumeration & Exploitation, Vulnerability Assessment.
- Fast Typing (60 WPM, 97% accuracy).

Soft Skills

- Strong Analytical Thinking.
- Communication.
- Team Collaboration.

Certifications & Training

- CompTIA Security+ (Course Completion – Netriders Academy)
- Networking (TryHackMe , HackTheBox , Youtube)
- Linux System Administrator (Udemy)
- TryHackMe Certificates / Progress :
  - Pre-Security Path (Completed)
  - Intro to Cybersecurity Pathway (Completed)
  - SOC Analyst Path (Completed)
  - Junior Penetration Tester (In Progress)
- SOC Path – LetsDefender (Completed)
- Scenario Training – CyberDefender
- HackTheBox :
  - (SOC Analyst Path (In progress)
- Upcoming / In Preparation:
  - Preparing for HTB Certified Defensive Security Analyst (HTB CDSA) – focused on hands-on security analysis, SOC operations, incident handling, threat detection, and creating actionable security reports.

LANGUAGES

- Arabic: Native
- English**:** Professional Proficiency (Reading: Excelllentt, Writing: Excelllentt, Speaking: VeryGood)