Farouq Hassan Junior SOC Analyst / Defensive Security Analyst

✉ 12farouq12@gmail.com ☎ +962 791757726 📍 Amman Jordan in LinkedIn Github

PROFESSIONAL SUMMARY

Defensive Security Analyst & DFIR-focused Cybersecurity student with hands-on experience in SOC investigations, SIEM threat hunting, Active Directory abuse detection, and digital forensics. Trained through national-level programs (NCSCJO) and real-world defensive validation within government environments. Strong in incident response, detection engineering fundamentals, and security reporting.

PROFESSIONAL EXPERIENCE

Security Assurance & Defensive Validation Apprentice
Special Communications Commission – Jordan Armed Forces (SCC-JAF) | Oct 2025 – Present

- Supported SOC-style alert analysis and defensive validation across 10+ enterprise systems (network, application, infrastructure).
- Reviewed Windows Event Logs, Sysmon telemetry, and network configurations to identify suspicious activity and control gaps.
- Validated detection and remediation effectiveness for credential abuse, misconfigurations, and exposure risks.
- Built and maintained Docker-based lab environments to test security controls and detection coverage.
- Assisted in incident response readiness assessments, focusing on detection, escalation, and reporting workflows.
- Performed alert triage, false-positive analysis, and escalation following SOC playbooks and severity models.

National Cyber Security Center – Jordan (NCSCJO) | Oct 2025 – Dec 2025

- Completed 200+ hours of structured defensive security and SOC training across 24+ hands-on labs.
- Performed incident triage, memory, disk, and network forensics to investigate malware, persistence mechanisms, and credential abuse.
- Conducted SIEM-based investigations and log analysis to reconstruct attack timelines and validate detections.
- Applied NIST-aligned incident response workflows and produced SOC-style findings and remediation recommendations.

SIGNIFICANT PROJECTS

Enterprise SOC & DFIR Investigations
(Hands-on simulations & enterprise-style environments, including HTB CDSA)

- Conducted SIEM-driven investigations (Splunk, ELK) covering phishing, malware execution, credential abuse, and lateral movement, reconstructing attack timelines from Windows logs, Sysmon, network traffic, and memory artifacts.

Active Directory Attack Detection & Defense

- Investigated AD abuse including Kerberoasting, Pass-the-Ticket, LSASS dumping, DCSync, and DCShadow, mapping activity to MITRE ATT&CK and recommending SOC-aligned detection and containment actions.

Malware, Memory & Network Forensics

- Performed disk and memory forensics (Volatility, FTK Imager) and PCAP analysis (Wireshark) to identify fileless persistence, credential theft artifacts, C2 traffic, and actionable IOCs.

Threat Hunting & Detection Engineering Fundamentals

- Executed hypothesis-driven threat hunts and applied Sigma and YARA rules to improve detection coverage and reduce false positives across SIEM telemetry.

End-to-End Breach Analysis (Malware → Identity → Cloud)

- Analyzed multi-stage intrusions from initial malware access to identity compromise and cloud exposure, documenting findings with ATT&CK mapping and prioritized remediation.

EDUCATION

Bachelor's Degree in Cybersecurity, HTU | Al Hussein Technical University | Expected Graduation: June. 2026 | Oct. 2021 – Present

CERTIFICATES

- Certified Defensive Security Analyst (CDSA) – Hack The Box | 2025
- Certified Web Security Expert (CWSE) – Hackviser | 2025
- Certified Associate Penetration Tester (CAPT) – Hackviser | 2025
- Nutanix Certified Associate (NCA) v6 – Nutanix | 2025
- CompTIA Security+ (SY0-701) | Expected 2026
- Cisco CCNA (200-301) | Expected 2026

SKILLS

SIEM & Log Analysis: Splunk, Elastic Stack (ELK), Windows Event Logs, Sysmon
Threat Detection & Response: Alert triage, false-positive analysis, IOC extraction, MITRE ATT&CK
Network Analysis: Wireshark, Zeek, TCP/IP, DNS, HTTP/S, TLS
DFIR: Memory & disk forensics (Volatility, FTK Imager), endpoint artifact analysis
Detection Engineering: Sigma rules, YARA rules (usage & analysis)
IDS / IPS: Snort & Suricata concepts and rule-based detection
Systems: Windows & Linux, Active Directory (Kerberoasting, Pass-the-Ticket, DCSync)
Reporting: Incident timelines, executive & technical SOC reports
Core Competencies: Technical Reporting, Cross-Team Communication, Incident Triage & Escalation, Log Correlation, Root Cause Analysis

ACHIEVEMENTS & LEADERSHIP

HTU Admission & Registration Volunteer: Guided 400+ students, resolving ~90% of inquiries | Jan 2024 – Present
Team Leader – SPARK Project: Led a 6-person team; validated $1.65M market potential | Oct 2024 – Feb 2025
Top 10 / 300 – NCSCJO Cybersecurity Bootcamp | 2024
1st Place (Temporary Leaderboard) – HTU Cybersecurity CTF | 2024