Farouq Hassan

Junior SOC Analyst - Threat Detection & Incident Response
12farouq12@gmail.com | +962 791 757 726 | Amman, Jordan | LinkedIn | GitHub | farouqhassan.dev

SUMMARY

Junior SOC Analyst with real-world security validation at a government defence organization - 12 documented findings across 10+ live systems (3 critical, CVSS 8.8–9.3). CDSA-certified: produced a 63-page commercial-grade DFIR report across Elastic SIEM and Splunk, covering domain-wide compromise and DCSync/DCShadow detection. Currently teaching cybersecurity to 60+ students full-time. Proven across SIEM triage, C2/DNS-tunnelling detection, memory forensics (Volatility 3), AD threat detection, structured IR planning, and governance.

EXPERIENCE

Cybersecurity Instructor
Mint Education - Online — 2026 – Present

- Teaching cybersecurity to 60+ students across 4 concurrent classes; developing lab exercises covering network security, web exploitation, OSINT, threat detection, and incident response fundamentals.

Security Assurance & Defensive Validation Apprentice
Special Communications Commission – Jordan Armed Forces (SCC-JAF) — Oct 2025 – Jun 2026

- Conducted authorized VAPT across 10+ live government systems (web, mobile, network) - 12 findings: 3 critical (CVSS 8.8–9.3) incl. auth bypass, unauthenticated data exfiltration, APK credential extraction; 3 high (CVSS 7.5–8.5) incl. exposed FortiGate admin interface; 6 medium/low - all delivered with CVSS scores, PoC evidence, and remediation roadmap.
- Performed alert triage, false-positive reduction, and severity classification across 10+ enterprise systems using SOC escalation playbooks; reviewed Windows Event Logs and Sysmon telemetry to validate detection coverage across attack scenarios.
- Administered FortiGate firewall in live government environment - configured security policies, web content category filtering, application control, and VLAN/subnet segmentation; built 5+ isolated Docker labs for detection validation; authored 7-section Android/MDM pentest doctrine for government fleet.

Cybersecurity Analyst Intern (Masar Program)
National Cyber Security Center – Jordan (NCSCJO) — Oct – Dec 2025

- Completed 24+ structured practical sessions producing deliverables across SIEM analysis, memory forensics, network forensics, threat intelligence, IR playbooks, and governance assessments aligned to ISO 27014, PDPL, and PCI DSS.

PROJECTS

CDSA Exam - Dual-Incident DFIR Investigation (Elastic SIEM + Splunk) — Nov 2025

Investigated 2 independent incidents to full domain compromise:

- phishing-to-DC attack chain - traced C2 communication, process injection, privilege escalation, Kerberoasting, lateral movement, and LSASS credential dumping using Elastic SIEM corroborated by Volatility 3 memory forensics;
- DCSync/DCShadow detection - identified unauthorized AD replication abuse, Pass-the-Hash authentication, and forest-wide privilege group manipulation using Splunk. 16 MITRE ATT&CK techniques mapped across both incidents.

Threat Intelligence & Incident Response - APT29, Lumma Stealer & IR Playbooks — Dec 2025

- Profiled 2 threat actors (APT29, Lumma Stealer) across 3 OSINT sources (CISA, Microsoft, Mandiant) - 12 ATT&CK techniques mapped, Navigator layers impact-scored, 3 D3FEND countermeasures identified targeting credential theft. Built 2 structured IR playbooks (clinic malware outbreak + software supply-chain breach): containment matrix across 3 options, ATT&CK→D3FEND mappings, executive and staff comms templates, ransomware decision tree with evidence preservation and recovery prerequisites.

Digital Forensics - BlackEagle Investigation — Feb 2025

- End-to-end forensic investigation: disk acquisition using FTK Imager with hardware write-blocker, hex-level recovery of corrupted NTFS USB volume (HxD), hash-verified evidence chain throughout, steganographic message extraction from PNG file - uncovering covert intelligence. Followed McKemmish 4-step model with full chain of custody documentation.

FAIR Risk Modelling - Phishing Incident (DPSR) — May 2025

- STRIDE/DREAD threat modelling (6 categories) + FAIR-U Monte Carlo simulation - ALE before controls: $1.38M/yr; after: $177K/yr; ~$1.2M/yr risk reduction. Risk register, KRIs, and executive board summary produced. Aligned to Jordan Cybersecurity Law No. 16 (2019) and PDPL No. 24 (2023).

SKILLS

SIEM & Logs: Splunk, Elastic Stack (ELK), Windows Event Logs, Sysmon
DFIR: Volatility 3, FTK Imager, Wireshark, PCAP analysis, C2 detection, DNS tunnelling detection
Threat Detection: MITRE ATT&CK/D3FEND, Sigma, YARA, IOC extraction, threat hunting
Network Security: FortiGate (security policies, web filtering, app control, VLAN segmentation), AD threat detection
IR & Risk: NIST lifecycle, containment planning, ransomware playbooks, BIA/RTO/RPO, FAIR modelling
Governance: ISO 27001, ISO 27014, COBIT 2019, PDPL, PCI DSS, gap analysis, risk registers, KRIs
Other: Docker, Python, Git, Semgrep SAST, GitHub Actions, Linux, Windows

CERTIFICATIONS

- Certified Defensive Security Analyst (CDSA) - HTB | Nov 2025 - 63-page exam report
- Certified Web Security Expert (CWSE) - Hackviser | 2025
- Certified Associate Penetration Tester (CAPT) - Hackviser | 2025
- CompTIA Security+ - In Progress | 2026
- CPTS (HTB) - 70% Complete | 2026

EDUCATION

BSc Cybersecurity Al Hussein Technical University (HTU) — Graduated June 2026

ACHIEVEMENTS

- Top 10/300 - NCSCJO Cybersecurity Bootcamp (Top 3%) | 2024
- 1st Place - HTU Cybersecurity CTF (50+ participants) | 2024
- Team Leader - SPARK: $1.65M market validated | 2024–2025
- HTU Volunteer: guided 400+ students, ~90% resolved | 2024–Present