

Mohammad Issam Musa Arabieh

Amman, Jordan

+962-780969260 | mohammadissam410@gmail.com | LinkedIn | GitHub

Professional Summary

Telecom and cybersecurity professional with 6+ years across network operations and security monitoring. Hands-on experience installing, maintaining, and troubleshooting 2G/3G/4G/5G radio access and microwave infrastructure on Huawei and Ericsson equipment, alongside SOC work in alert triage, SIEM monitoring, and detection engineering using Elastic SIEM, Wazuh, and ArcSight. CCNA and BTL1 certified. Comfortable in shift-based, KPI-driven operations, and experienced coordinating field teams, engineers, and operational stakeholders.

Skills

Telecom & Radio Networks: 2G/3G/4G LTE/5G installation and configuration, Huawei, Ericsson, microwave links, tower infrastructure, site integration, network deployment

Network Operations: Network monitoring, connectivity troubleshooting, fault isolation, root cause analysis, incident escalation, service availability, technical documentation

Networking Fundamentals: TCP/IP, routing and switching, NAT, DNS, VPN, Fortinet FortiGate, OPNsense, pfSense, IDS/IPS

Security Operations: SOC monitoring, SIEM, alert triage, incident investigation, incident response, log analysis, detection engineering, MITRE ATT&CK, threat hunting

Security Tools: Elastic SIEM, Wazuh SIEM/XDR, ArcSight, Splunk, Wireshark, Nmap, Burp Suite, YARA

Digital Forensics: Volatility, Autopsy, FTK Imager, Magnet AXIOM

Cloud: Google Cloud Platform, IAM, Cloud Logging, VPC networking

Programming and Automation: Python, Bash, Java, C++, n8n SOAR, security workflow automation

Systems: Linux administration and hardening, Windows Server

Certifications

- CCNA (Cisco Certified Network Associate) - Completed
- Blue Team Level 1 (BTL1), Security Blue Team - 2026
- Elastic Security for SIEM - Certification
- CEH (Certified Ethical Hacker) - Training completed

Training & Courses

- CompTIA Security+ - Training completed
- Google Cloud Fundamentals: Core Infrastructure
- Architecting with Google Compute Engine
- GCP Security & Networking

Education

Bachelor's Degree in Cyber Security - GPA: 74.4% Al-Zaytoonah University of Jordan | Amman, Jordan | Mar 2022 - Jan 2026

Professional Experience

Team Lead / Site Coordinator, Telecom & Network Operations

ICCCC Company | Jordan | 2020 - 2024

- Monitored network performance and connectivity across live cellular sites, identifying faults and service degradations through continuous surveillance.
- Installed, configured, and maintained 2G/3G/4G/5G radio access network equipment on Huawei and Ericsson platforms, including microwave links and tower-mounted infrastructure.
- Investigated connectivity and infrastructure incidents, performed root-cause analysis, and coordinated corrective actions with engineering teams.
- Escalated and tracked faults through resolution, maintaining accurate technical documentation of site changes, equipment status, and operational activity.
- Coordinated field activities, installation tasks, and maintenance work across technicians, engineers, and operational stakeholders.

Telecom Technician / Site Coordinator

NDT Company | Jordan | 2018 - 2020

- Supported telecom and microwave site installations, including tower rigging and wireless equipment deployment.
- Performed routine maintenance and fault troubleshooting on radio access network sites.
- Coordinated field tasks with technicians and engineers, and maintained technical documentation for site activity and equipment changes.

Co-founder & SOC / Cybersecurity Engineer

AMAN Security Startup (Part-time) | Amman, Jordan | 2024 - 2026

- Built and maintained cybersecurity and network-security tools for monitoring, threat detection, and infrastructure protection.
- Configured and monitored OPNsense firewall environments, network traffic, firewall policies, NAT, and connectivity between internal and external network segments.
- Integrated firewall and Google Cloud logs into Wazuh for centralized monitoring and security analysis.
- Developed and validated MITRE ATT&CK-mapped detection rules to improve monitoring visibility and reduce false positives.
- Co-developed and maintain an AI-powered email threat detection browser extension for Gmail and Outlook, achieving 98% detection accuracy in internal testing.
- Automated security and operational workflows using Python, Bash, and n8n SOAR.
- Documented technical configurations, security controls, monitoring requirements, and operational procedures.

Cyber Security Intern

Jordan Islamic Bank | Amman, Jordan | Sept 2025 - Oct 2025

- Monitored and analyzed security alerts using Elastic SIEM and ArcSight.
- Supported alert triage, incident investigation, escalation, and technical documentation procedures.
- Analyzed security logs and events to help identify suspicious activity and potential security incidents.
- Gained practical experience working with security operations and technology infrastructure in a financial-sector environment.

Cybersecurity Masar Trainee

National Cyber Security Center (NCSC) | Amman, Jordan | 2025

- Completed a 200-hour cybersecurity training program covering network security, SOC operations, threat detection, incident handling, penetration testing, and security fundamentals.
- Performed authorized network analysis, security testing, and CTF challenges in controlled training environments.
- Practiced identifying attack techniques, analyzing technical findings, and documenting observations.

Customer Service Advisor

Concentrix | Amman, Jordan | May 2026 - Sep 2026

- Support customers in a fast-paced enterprise environment while maintaining accuracy, professionalism, and attention to detail.
- Investigate issues, identify root causes, document findings, and communicate practical solutions to non-technical users.
- Work within shift-based operations, KPI-driven workflows, service-level expectations, and established procedures.

Projects

Advanced SOC Simulation - Hybrid XDR & Automation

- Built a hybrid on-premises and cloud-based network and security-monitoring environment using limited hardware resources.
- Deployed Wazuh SIEM/XDR for centralized log collection, monitoring, and event analysis.
- Integrated OPNsense firewall logs and Google Cloud firewall logs into the SIEM platform.
- Configured firewall rules, NAT, traffic controls, and connectivity between internal and external network segments.
- Developed and validated 15+ custom MITRE ATT&CK-mapped detection rules.
- Automated incident-response workflows using n8n SOAR.
- Tested connectivity, firewall controls, and detection logic against simulated brute-force, lateral-movement, and phishing scenarios in an authorized lab environment.

Aman Security - AI-Powered Email Threat Detection Browser Extension

- Co-developed and maintained a browser extension for Gmail and Outlook that analyzes incoming emails in real time using an AI classification model.
- Built detection logic for phishing links, spoofed sender domains, malicious attachments, social-engineering language, urgency-based language, and look-alike or BEC-style domains.
- Implemented protective controls that block user interaction with detected threats until the warning is acknowledged.
- Applied privacy-by-design principles by processing email content without storing or retaining user data.
- Achieved 98% detection accuracy during internal testing of the classification model.
- Maintained the system in production since 2025 to protect users against email-based threats.

Achievements

- **Google Gemini Pro Challenge 2026** - 1st Place, Middle East & Turkey
- **TryHackMe** - Top 2% Global Ranking
- **RLCTF v3 2025** - Rank 22
- **IEEE CTF 2025** - Rank 6
- **BlackHat MEA Riyadh 2025** - Rank 40
- **NASA Space Apps 2025** - Rank 11
- **GEW 2026 (Global Entrepreneurship Week) with AMAN**

Leadership & Community Involvement

- **IEEE ZUJ Student Branch - Treasurer** Managed budgeting and financial reporting for student-led technical and cybersecurity activities.
- **GDGoC ZUJ (Google Developer Group on Campus) - Core Team, Media & Marketing** Supported the organization and promotion of technical and developer-focused events.

Languages
