

Mohammad Arabieh

Network & Security Operations Engineer | BTL1 Certified

Amman, Jordan

+962-780969260 | mohammadissam410@gmail.com

linkedin.com/in/mohammad-issam-a803b1259 | github.com/Mohammadissam | Portfolio

Professional Summary

Network and security operations engineer with six years in live telecom operations: installing, maintaining, and troubleshooting 2G/3G/4G/5G radio and microwave networks on Huawei and Ericsson equipment, and leading field teams through fault isolation, root-cause analysis, and escalation. Moved into security operations in 2024: alert triage in Elastic SIEM and ArcSight during a bank internship, a Wazuh-based hybrid SOC lab with MITRE ATT&CK-mapped detections, and an AI email-threat extension co-built at AMAN Security. BTL1 certified and CCNA-trained, with a B.Sc. in Cyber Security (2026).

Skills

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

Telecom & Radio: 2G/3G/4G LTE/5G, Huawei, Ericsson, microwave links, tower infrastructure, site integration

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

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

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

Forensics: Volatility, Autopsy, FTK Imager, Magnet AXIOM

Cloud & Systems: Google Cloud (IAM, Cloud Logging, VPC networking), Linux administration and hardening, Windows Server, Docker

Automation: Python, Bash, n8n SOAR, Java, C++, Shuffle SOAR

Network & Telecom Experience

Team Lead / Site Coordinator, Telecom & Network Operations

ICCCC Company | Jordan | 2020 - 2024

- Monitored performance and connectivity across live cellular sites, identifying faults and service degradation through continuous surveillance.
- Installed, configured, and maintained 2G/3G/4G/5G radio access equipment on Huawei and Ericsson platforms, including microwave links and tower-mounted infrastructure.
- Ran root-cause analysis on connectivity and infrastructure incidents, then escalated and tracked faults to resolution with engineering teams.
- Coordinated field, installation, and maintenance work across technicians, engineers, and operational stakeholders.
- Maintained documentation of site changes, equipment status, and operational activity.

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 kept technical documentation of site activity and equipment changes.

Security Experience

Co-founder & SOC / Cybersecurity Engineer

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

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

Cyber Security Intern

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

- Monitored and triaged security alerts using Elastic SIEM and ArcSight in a financial-sector environment.
- Supported incident investigation, escalation, and technical documentation, analyzing logs and events to identify suspicious activity.

Cybersecurity Trainee (Masar Program)

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

- Completed a 200-hour program covering network security, SOC operations, threat detection, incident handling, and penetration testing.
- Performed authorized network analysis, security testing, and CTF challenges in controlled training environments.

Other Experience

Customer Service Advisor

Concentrix | Amman, Jordan | May 2026 - Sep 2026

- Investigated customer issues, identified root causes, and explained solutions to non-technical users in a shift-based, KPI-driven environment.

Projects

Advanced SOC Simulation - Hybrid XDR & Automation

Team graduation project

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

AI-Powered Email Threat Detection Browser Extension

AMAN Security

- Co-developed a Gmail and Outlook extension that classifies incoming email in real time with an AI model and blocks interaction with flagged messages until the warning is acknowledged.
- Built detection logic for phishing links, spoofed sender domains, malicious attachments, social-engineering and urgency-based language, and look-alike or BEC-style domains.
- Applied privacy-by-design by processing email content without storing or retaining it, and maintained the system in production from 2025.

Education

Bachelor's Degree in Cyber Security

Al-Zaytoonah University of Jordan | Amman, Jordan | Mar 2022 - Jan 2026

Certifications

- Blue Team Level 1 (BTL1), Security Blue Team (now Centri) - 2026
 - Elastic Security for SIEM - Certification
 - CCNA (Cisco Certified Network Associate) - 88-hour training course
-

Training & Courses

- CEH (Certified Ethical Hacker) - Training completed
 - CompTIA Security+ - Training completed
 - Google Cloud Fundamentals: Core Infrastructure
 - Architecting with Google Compute Engine
 - GCP Security & Networking
-

Achievements

- **Google Gemini Pro Challenge 2026** - 1st Place, Middle East & Turkey
 - **TryHackMe** - Top 2% Global Ranking
 - **Competitions (2025)** - IEEE CTF rank 6; NASA Space Apps rank 11; RLCTF v3 rank 22; Black Hat MEA Riyadh CTF rank 40
-

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

Arabic - Native

English - Professional Working Proficiency (C1)