# Ziead Shab Kalieh

☎ +963956404766 ✉ zshabkalieh@gmail.com linkedin.com/in/zskcyber github.com/zieadshabkalieh 🌐 zsktech.info

## Target Role

**Cybersecurity Engineer** Open to: SOC / Blue Team, Network Security, Cloud Security, Vulnerability Management, Application Security

## Professional Summary

**Cybersecurity Engineer** with **5+ years** securing enterprise networks, infrastructure, and web applications across government, international, and private-sector environments. Hands-on in **network defense**, **security hardening**, **vulnerability assessment**, **web application security testing**, and **incident detection** (log review, monitoring, triage). Strong foundation in **networking** (CCNA) and **cloud administration** (Azure AZ-104), with proven ability to deliver security improvements through clear documentation, practical risk reduction, and cross-team collaboration.

## Core Skills

**Security Domains:** Network Security, Security Engineering, Security Architecture, Security Controls, Defense-in-Depth, Segmentation, Access Control, Least Privilege, Vulnerability Management, Risk Assessment, Security Policies & Procedures, Incident Detection & Response (Triage), Threat Monitoring, Secure Communications
**AppSec / Offensive:** Web Application Security Testing, OWASP Top 10, API Security Testing, Authentication & Authorization Testing, Session Management, Business Logic Testing, Responsible Disclosure, Remediation Validation
**Systems / Cloud:** Microsoft Azure (AZ-104), Windows Server 2016 (Compute/Networking/Identity), Linux (Kali), Identity & Access Management (IAM concepts), Backup & Recovery
**Security Tools:** Qualys (Vulnerability Scanning), Burp Suite, DVWA, Network Monitoring (concepts), IDS/IPS (concepts), Documentation & Reporting
**Strengths:** Analytical Thinking, Problem Solving, Attention to Detail, Ownership, Clear Communication, Teamwork, Time Management, Integrity

## Professional Experience

**Ministry of Defense** **Nov 2025 – Present**
*Network Security Engineer (Full-Time, On-site)* *Syria*

- Support secure network operations in a **high-security government environment**, contributing to network defense procedures, access control practices, and secure communications readiness.
- Assist with **monitoring network activity** and reviewing security-relevant events to identify anomalies and reduce operational risk.
- Contribute to **change management** by validating security impact of network modifications and maintaining operational documentation and checklists.
- Perform security administration tasks including **asset tracking**, access reviews, and compliance-aligned routine checks supporting continuous readiness.

**SWB Group** **Aug 2025 – Dec 2025**
*Cybersecurity & IT Infrastructure Lead — Network & Systems Security (Hybrid)* *Syria*

- Led cybersecurity and infrastructure operations across **multi-site environments** (branch, factory, academy), strengthening access control, asset visibility, and secure operations.
- Designed and documented internal network topology and security controls, supporting segmentation decisions, secure connectivity, and operational troubleshooting.
- Administered NAS recovery and data restructuring after failures; enforced **least-privilege permissions**, improved backup readiness, and reduced data access risk.
- Conducted ethical security testing for internal ERP (Odoo), identified **access-control weaknesses**, supported remediation, and validated fixes.
- Standardized security documentation (inventories, diagrams, procedures), improving response speed for audits, incidents, and change approvals.

**Click 2 Speed (UAE-based)** **May 2025 – Aug 2025**
*Secure Application Development & Testing (Freelance, Remote)* *UAE*

- Executed security testing across critical web workflows, focusing on **authentication**, **authorization**, **API access control**, and business-logic abuse scenarios.
- Produced vulnerability documentation with reproducible steps and remediation guidance; **retested** fixes after patch deployment to confirm closure.
- Aligned test cases to **OWASP Top 10** and common API risks, improving consistency and coverage across release cycles.
- Supported secure design decisions to reduce data exposure, client-side manipulation risk, and transaction bypass scenarios.

**Prootech Agency (UAE-based)** **Apr 2025 – May 2025**

*Security QA Engineer — Application Security Testing (Contract, On-site)* *UAE*

- Performed manual application security testing on authentication and authorization workflows for a live production web application.
- Identified a **critical authentication bypass** (URL manipulation), documented impact and reproduction steps, and validated remediation through retesting.
- Collaborated with stakeholders to communicate risk severity, verify fixes, and reduce recurrence through stronger testing checklists.

**UNDP (United Nations Development Programme)** **Sep 2024 – Jan 2025**

*IT Infrastructure & Security Engineer (Contract, On-site)* *Syria*

- Supported secure IT operations in an international environment, contributing to infrastructure hardening, operational reliability, and policy-aligned access practices.
- Assisted with monitoring, backup readiness, and risk-aware support activities to maintain service availability and reduce operational disruptions.
- Maintained clear technical documentation and user support processes aligned with organizational standards.

## Training & Knowledge Sharing

**Ebla Private University** **Apr 2025**

*Cybersecurity Trainer — Web Penetration Testing Bootcamp* *Syria*

- Designed and delivered an intensive hands-on bootcamp covering **OWASP Top 10** through labs, real-world vulnerability analysis, and CTF-style challenges.
- Guided participants from fundamentals to practical exploitation and mitigation, emphasizing root-cause understanding and secure coding thinking.
- Conducted vulnerability walkthroughs using DVWA and web testing methodology with tools such as **Burp Suite** and **Kali Linux**.
- Promoted ethical hacking principles, responsible disclosure, and professional conduct throughout the program.

## Selected Cybersecurity Projects

**Comprehensive Network and Device Vulnerability Assessment** **Portfolio**

- Executed a structured vulnerability assessment across network and endpoint assets; analyzed findings, prioritized risk, and produced remediation recommendations.
- Built remediation guidance with practical hardening actions and verification steps to support vulnerability closure.
- **Keywords:** Vulnerability Management, Qualys, Risk Prioritization, Network Security, Endpoint Hardening, Reporting.

**Automated Penetration Testing Tool (APTT)** **Portfolio**

- Developed a security automation concept/tooling to standardize penetration testing workflows and improve report consistency.
- Focused on repeatable execution, evidence collection, and structured outputs to reduce manual overhead in engagements.
- **Keywords:** Security Automation, Penetration Testing, Reporting, Workflow Standardization.

**Windows Server Penetration Testing & Hardening Project** **Portfolio**

- Assessed Windows Server attack surface and mapped prioritized hardening actions for identity, access control, and configuration risk reduction.
- Produced a hardening checklist that aligned configuration changes with security objectives and validation steps.
- **Keywords:** Windows Server Security, Identity & Access, Privilege Management, Hardening, Systems Security.

## Certifications

**CCNA** (New Horizons)
**AZ-104: Microsoft Azure Administrator Associate** (New Horizons)
**Ethical Hacking Essentials** (EC-Council)
**Qualys Scanning Strategies and Best Practices** (Qualys DefendLab)
**Windows Server 2016:** 20740C Installation/Storage/Compute; 20741B Networking; 20742B Identity

## Education

**Ebla Private University** **Jan 2019 – Jul 2024**

*B.Sc. in Information Technology and Communication Engineering* *Syria*

- Relevant focus: cybersecurity, networking, systems administration, cloud fundamentals, and applied software engineering.