Ziad Shab Kalieh

Cybersecurity Engineer | SOC & Incident Response | Penetration Testing | Cloud Security

Germany | **+49 1637292811** | **Email:** zshabkalieh@gmail.com

Portfolio: zsktech.pro | **LinkedIn:** linkedin.com/in/zsktech | **Github:** github.com/zieadshabkalieh

PROFESSIONAL SUMMARY

Collaborative and team-oriented Cybersecurity Engineer with 5+ years of success in reducing **SOC alert fatigue** by 70% and **vulnerabilities** by 30%. Specializing in **SOC Operations**, **Incident Response**, **Penetration Testing**, and **Cloud Security** (**AWS**, **Azure**). Skilled in **SIEM** (**Splunk**, **IBM QRadar**), **IDS/IPS**, **Zero Trust architectures**, **APT detection**, **Threat Hunting**, and advanced **Incident Response** methodologies (**MITRE ATT&CK**, **Cyber Kill Chain**). Passionate mentor and security innovator, aiming to drive threat detection innovation and protect organizations from sophisticated cyber threats.

SKILLS:

- **SOC & Incident Response**: SIEM, EDR, SOAR, APT Analysis, Threat Hunting
- **Penetration Testing**: OWASP Top 10, Metasploit, Nessus, Nmap, Burp Suite, OWASP ZAP
- **Cloud Security**: AWS (EC2, S3, IAM), Azure (Security Center, Defender), Docker, Kubernetes, Terraform
- **Networking & Infrastructure**: Cisco Routers/Switches, VLANs, Firewall Management (Cisco ASA, PfSense), VPNs, Zero-Trust
- **Risk & Compliance**: ISO 27001, NIST 800-53, SOC 2, PCI-DSS, GDPR, CIS Benchmarks
- **Automation & Scripting**: Python, Bash, PowerShell, Java, C#, .NET
- **Security Policy & Governance**: Security Awareness Training, Security Policy Development, Purple Teaming

WORK EXPERIENCE:

SOC Engineer | Threat Detection Specialist
DefendLab, Full-time | *January 2023 – August 2023*

- **Optimized SIEM** correlation rules (MITRE ATT&CK-aligned), reducing SOC alert fatigue by 30%.
- Investigated and contained **APTs** leveraging EDR, threat intelligence feeds, and anomaly detection.
- Deployed **SOAR workflows** to **automate** triage and cut incident response time by 40%.
- Led Purple Team exercises to refine defenses and Zero Trust architectures.

Cyber Security Engineer | Penetration Tester & Cloud Security Specialist
Mademoiselle, Remote | *June 2024 – September 2024*

- Performed **penetration testing** on AWS VPCs, Supabase, and Windows Server 2022 (OWASP Top 10).
- Integrated Attack Surface Management tools to reduce cloud misconfigurations and exposure.
- Designed **IAM Governance** with RBAC policies and least-privilege enforcement.
- Developed **Terraform security templates** with automated remediation pipelines.

IT Infrastructure & Security Engineer
United Nations Development Programme (UNDP), On-site | *September 2024 – February 2025*

- Achieved 98% compliance with **ISO 27001**, **NIST 800-53**, bolstering SOC 2 and PCI-DSS readiness.
- Led **Threat Modeling** exercises to identify risk scenarios and define mitigation.
- Strengthened **network segmentation**, firewall policies, and endpoint controls under zero-trust.
- Integrated **Business Continuity Planning (BCP)** and disaster recovery solutions for hybrid environments.

Penetration Testing Specialist
New Horizons Computer Learning Centers, On-site | *February 2023 – August 2023*

- Executed **penetration tests** on networks, web apps, and databases (Metasploit, OWASP ZAP, Nmap).
- Deployed **Attack Surface Reduction** (patch management, secure coding, system hardening).
- Delivered **Threat Modeling** workshops, integrating SDLC security best practices.

Co-Founder | High-Security VPN Services
AToZ VPN, Remote | *March 2023 – January 2025*

- Architected secure **VPN infrastructure** with DLP enforcement, IAM segregation, and MFA.
- Integrated **SIEM** correlation, intrusion detection, and EDR telemetry across VPN nodes.
- Applied **Cyber Kill Chain** concepts to detect advanced threats and insider behaviors.
- Maintained BCP protocols as part of a cross-functional security team, ensuring uptime and compliance.

PROJECTS:

- **Penetration Testing (Ebla Private University)**: Detected and mitigated 15+ critical vulnerabilities, reducing attack surface by 40%.
- **Cloud Security Hardening (Retail Client)**: Hardened Docker containers, implemented IAM policies, and automated S3 backups, improving disaster recovery by 60%.
- **Dual Firewall Redundancy**: Deployed HA firewalls (Cisco ASA, PfSense) with near-zero downtime; improved segmentation and resilience.
- **VPN Threat Detection (AToZ VPN)**: Built a real-time alerting engine integrating SIEM, EDR, and firewall logs.
- **AWS Cloud Cost Optimization (Personal Lab)**: Reduced projected monthly billing by 45% using right-sizing and storage tier reclassification.

CERTIFICATIONS:

- **Ethical Hacking Essentials (EHE)** – EC-Council
- **Cisco Certified Network Associate (CCNA)** – Cisco
- **Microsoft Azure Administrator (AZ-104)** – Microsoft
- **IELTS Academic** – British Council | *Band 6*

TRAINING:

- **Certified Ethical Hacker (CEH)** – EC-Council (Training completed)
- **Offensive Security Certified Professional (OSCP)** – Offensive Security (Training completed)
- **CompTIA Security+ (SY0-601)** – CompTIA (Training completed)
- **AWS Certified Security – Specialty** – Amazon Web Services (Training completed)

EDUCATION:

Ebla Private University, *Aleppo, Syria*

Bachelor of Science in Information Technology and Communication Engineering *(2019 – 2024)*

- Specialized in Cybersecurity, Network Security, and Cloud Infrastructure.
- Final Project: **Design & Security of Satellite Communication Systems** using encrypted antennas for secure data transmission.

VOLUNTEER EXPERIENCE:

- **Cybersecurity & Cloud Awareness Campaigns** (Aleppo University, Al Shahba University, Al Ittihad University, Kortoba University, Ebla Private University):
  Conducted seminars and workshops to raise cybersecurity and cloud awareness.
- **Programming Contester (ICPC)** (Mar 2023 – Jul 2024):
  Participated in Codeforces, enhancing algorithmic and problem-solving skills.

LANGUAGES:

- **Arabic** – Native
- **English** – Fluent
- **French** – Intermediate
- **German** – Intermediate
- **Turkish** – Intermediate
- **Russian** – Basic

ADDITIONAL INFORMATION:

- Skilled in leading **security projects** and **mentoring junior engineers**.
- Dedicated to **Threat Detection Innovation** and advanced cybersecurity solutions.
- **Effective communicator** and **adaptable team player**, experienced in coordinating with **cross-functional security teams** to support **joint threat modeling** and **Purple Team exercises**.
- **Target Roles**: Senior SOC Engineer, Cybersecurity Consultant, Cloud Security Specialist, Threat Detection Lead.
- **Keywords:** Red Team, Ethical Hacking, Offensive Security, Cobalt Strike, Web Application Security, Exploitation, Post-Exploitation, Phishing Simulation, Exploit Development, Privilege Escalation, Lateral Movement, Persistence, Command and Control (C2), Threat Emulation, EDR Evasion, Active Directory Attacks, Credential Dumping, Network Pivoting, SQL Injection, CVE Exploitation, Linux Exploitation, Windows Exploitation, Purple Teaming, Cloud Pentesting, IAM Exploitation, DevSecOps, Firewall Evasion, IDS Evasion, Ethical Hacker, Collaborative, Team-Oriented, Effective Communicator, Adaptable