

MAHYAR TAJDINI, Ph.D. Candidate

Security & Cloud Architect / DevSecOps Specialist

Kyiv, Ukraine | Email: Mahyar@TajDini.net | Phone: +38 (073) 064 73 88

Languages: English (Fluent), Persian (Native), Russian (Intermediate), Ukrainian (Elementary)



PROFESSIONAL SUMMARY

Versatile, high-impact **Security & Cloud Architect / DevSecOps Specialist** with 15+ years of hands-on technical and leadership experience spanning enterprise cloud security architecture, automated CI/CD pipeline protection, vulnerability management, and infrastructure security engineering. Proven track record in shifting security left by embedding SAST/DAST, secret scanning, container security tools, and mTLS architectures directly into cloud-native deployments across AWS and Azure environments. Certified Azure Security Engineer (AZ-500) and ISO 27001 Lead Auditor with extensive expertise in container orchestration (Docker, Kubernetes), Infrastructure as Code (Terraform), Zero Trust architecture, and DevSecOps governance.

CORE DEVSECOPS & CLOUD COMPETENCIES

Domain / Category	Technologies, Frameworks & Technical Capabilities
Cloud Architecture & Security	AWS (EC2, S3, RDS, IAM, CloudWatch, VPC, EventBridge, KMS, GuardDuty), Microsoft Azure (Entra ID / Azure AD, Sentinel SIEM, Azure Key Vault, EventHub, Intune, Azure Policy, Security Center), Hybrid Cloud Security posture management.
DevSecOps & CI/CD Pipelines	Shift-Left Security Engineering, CI/CD Pipeline Integration (Bitbucket Pipelines, GitHub Actions, GitLab CI), Automated SAST/DAST/IAST Analysis, Secret Detection & Prevention, Dependency Scanning, Artifact Signing, Automated Vulnerability Triage & Remediation Workflows.
Container & Kubernetes Security	Docker, Docker Compose, Kubernetes (K8s), Helm, Container Image Hardening, Vulnerability Scanning (Trivy, Gype), Kubernetes Network Policies, Pod Security Standards, Container Registry Security.
Infrastructure as Code & Automation	Terraform, Ansible, Shell Scripting (Bash), PowerShell, Python Security Automation, RESTful API Security Gateways, Automated Compliance Enforcement.
Network Security & Edge Protection	Cloudflare WAF, Custom Security Rulesets, Anti-DDoS Mitigation, Mutual TLS (mTLS), Zero Trust Architecture, Micro-segmentation, Ingress/Egress Controller Security, VPN & IPsec Tunnels.
SIEM, Monitoring & Incident Response	ELK Stack (Elasticsearch, Logstash, Kibana), Datadog SIEM, Splunk, Crowdstrike EDR, Threat Hunting, Log Aggregation & Correlation, Automated Incident Response & Runbook Execution.
Governance, Risk & Compliance	ISO/IEC 27001 Audit & Implementation, Vulnerability Assessment & Management (VAM), Red/Blue Teaming Management, Bug Bounty Operations,

Domain / Category	Technologies, Frameworks & Technical Capabilities
	Security Code Review, OWASP Top 10 Safeguards.

PROFESSIONAL EXPERIENCE

Security Solution Architect

Capgemini (Ericsson Project) | Project-Based Experience | Less than a year

- Defined security requirements and controls across cloud, infrastructure, networking, applications, and system integrations.
- Conducted security architecture reviews and risk assessments, identifying design weaknesses and recommending appropriate security controls.
- Worked with engineering and architecture teams on secure solution design, including identity, access control, network security, encryption, and secure communications.

Cloud Security Analyst

Intellias (JoinForma Project) | Project-Based Experience | Less than a year

- Performed cloud security assessments to identify security risks, configuration weaknesses, and potential vulnerabilities across cloud environments.
- Reviewed cloud architecture, infrastructure, IAM, networking, and security configurations against security best practices.
- Conducted security and risk analysis, providing recommendations for remediation and improvement of the overall cloud security posture.
- Collaborated with cloud, DevOps, and engineering teams to integrate security controls and best practices into cloud infrastructure and deployment processes.
- Supported the implementation of Cloud Security and DevSecOps practices, focusing on secure architecture, access control, monitoring, and vulnerability management.

Security Engineer

Linumlabs (Hibachi & Hashflow Projects) | 1 Year Experience

- Integrated Static Application Security Testing (**SAST**) and secret scanning directly into active **CI/CD pipelines**, establishing automated security gates before deployment.
- Architected and implemented **mutual TLS (mTLS)** communication protocols across microservices within cloud environments to enforce Zero Trust network access.
- Managed **Cloudflare** infrastructure, creating custom Web Application Firewall (**WAF**) rules, anti-DDoS mitigation policies, and fine-tuning edge security configurations.
- Analyzed real-time security events and application telemetry in **Datadog**, building automated threat detection and anomaly alerts.
- Managed private bug bounty programs and coordinated end-to-end vulnerability triage and remediation with engineering teams.

Security Architecture Engineer & Cloud Security Analyst

Pharmbills | +6 Years Experience

- Architected and secured enterprise **Microsoft Azure** cloud environments, managing **Azure AD / Entra ID, Microsoft Sentinel (SIEM), Azure Key Vault, EventHub, and Intune**.
- Built centralized cloud monitoring and visualization platforms using the **ELK Stack (Elasticsearch, Logstash, Kibana)** for continuous auditing and threat hunting.
- Performed deep security code reviews, container isolation audits, and automated log analysis.
- Led and trained the internal **SOC team** in cloud incident triage, Crowdstrike EDR analysis, digital forensics, and malware investigations.

Chief Information Security Officer (CISO)

Fairo (RBI Group) | 1.5 Years Experience

- Directed cloud security posture management, regulatory compliance (ISO 27001), and vulnerability management programs across enterprise cloud workloads.
- Spearheaded DevSecOps policies, establishing secure coding guidelines, container scanning protocols, and incident response runbooks for hybrid-cloud infrastructure.
- Managed red teaming, penetration testing, and rapid mitigation strategies to increase operational resilience.

Researcher & Professor of Information & Cyber Security

Borys Grinchenko Kyiv University | 7+ Years Experience (Part-Time)

- Taught advanced courses in Cloud & Web Application Security, IoT/Wireless Security, and Sensitive Data Protection.
- Active author of peer-reviewed research papers and technical books in cybersecurity.

CISO & Smart Contract / Cloud Engineer

DMM & Creditor Group Corp | 2 Years Experience

- Designed and deployed secure blockchain dApp backends on AWS using containerized microservices (Docker).
- Performed code auditing, dynamic analysis, and penetration testing on decentralized architectures (Ethereum, BSC, Solana).
- Managed database optimization, log auditing, and secure transaction layer APIs.

CTO & CISO

Femto IT Group | 1.5 Years Experience

- Oversaw full cloud and on-premise infrastructure setup, enterprise network hardening, and security monitoring.
- Administered and secured client Azure environments, firewall appliances, and virtualization clusters (ESXi, Citrix).
- Building Full Microsoft Active Directory hybrid Environment with Certificate Authority and DNS, WSUS, L2-L3 Switches with Security Features, VoIP Service, Remote Desktop and RD-Gateways with NPS (Network Policy Server) and etc.

Network & Information Security Consultant

Petro Gas Co. | 3 Years Experience

- Consulted on ISO 27001 implementation, analyzed network security across all OSI layers, and designed/implemented two enterprise-scale data centers.
- Organized security simulation maneuvers and trained IT department personnel on threat prevention.

CERTIFICATIONS & EDUCATION

Certifications

- **Azure Security Engineer Associate (AZ-500)**
- **ISO/IEC 27001 Lead Auditor** (IRCA / Bureau Veritas)
- **LPI3** – Linux Professional Institute Certification
- **CCNP Routing & Switching | CCNP Security**
- **EC-Council Certifications:** CHFI v10, ECIH v2, CSA (Certified SOC Analyst), ECSA, CEH
- **CompTIA:** Security+, Network+
- **Microsoft Certified Professional (MCP):** MCSA, MCSE, MCTS, MCITP (Transcript ID: 776196)

Education

- **Ph.D. Candidate in Cybersecurity** | Institute of Telecommunication and Global Information Space, National Academy of Sciences of Ukraine
- **M.Sc. in Cybersecurity (RED Diploma / Honors)** | State University of Telecommunications of Kyiv
- **B.Sc. in Computer Network Engineering** | City International University

ADDITIONAL TECHNICAL SKILLS

- **Programming & Scripting Languages:** Python, Bash, PowerShell, GoLang, Node.js, PHP, JavaScript, Solidity.
- **Virtualization & Systems Engineering:** VMware ESXi, Proxmox, Citrix, Linux (Debian, Ubuntu, CentOS, RHEL), Windows Server, Active Directory, PKI / Certificate Authorities.
- **Databases & High-Availability Storage:** MySQL, PostgreSQL, MS-SQL (High Availability & Clustering), Redis, MongoDB, Elasticsearch.
- **Applied AI & Security Automation:** AI/ML API security testing (OpenAI/GPT), log anomaly detection models, automated threat intelligence processing.