Viacheslav T.
Senior Principal Security Architect | Microsoft Security Stack Specialist

SUMMARY

- Principal-level Security Architect with 15+ years engineering enterprise-scale Microsoft security solutions across Azure and hybrid environments.
- Expertise in Microsoft Sentinel, Defender Suite, Entra ID, Azure Policy, and Infrastructure-as-Code (Bicep, ARM, YAML) integrated into CI/CD pipelines.
- Experienced in architecting Zero Trust solutions, automating security operations, and enforcing compliance with NZISM, NIST, and CIS frameworks.
- Background in security automation using PowerShell, Azure DevOps, and Azure Functions, enhancing threat detection and incident response.
- Skills in cloud security, identity management, network security, and vulnerability management.

TECHNICAL SKILLS

Main Technical Skills	Azure VM, Azure DevOps, Azure
Java Frameworks	Apache Spark
Scala Frameworks	Apache Spark
AI & Machine Learning	NLP
Data Analysis and Visualization Technologies	Apache Spark
Security	AWS Security Groups, Conditional Access, Crowdstrike, Defender, GPO (Group Policy Object), Microsoft Entra, Microsoft Intune, Nessus, NIST, Privileged Identity Management (PIM), RBAC, SCCM, Sentinel, Sentinel (Microsoft Sentinel)
Databases & Management Systems / ORM	Apache Spark, Query
Cloud Platforms, Services & Computing	ARM (Azure Resource Manager), Azure
Amazon Web Services	AWS IAM, AWS Security Groups
Azure Cloud Services	Azure Cloud Functions, Azure DevOps, Azure Firewall, Azure Function Apps, Azure infrastructure, Azure Logic Apps, Azure security, Azure Virtual Desktop, Azure VM, Entra ID, Hyper-V

Deployment, CI/CD & Administration	Active Directory, CD DevOps pipelines, CI/CD
SDK / API and Integrations	API
QA, Test Automation, Security	Crowdstrike, Nessus, PKI, Tenable
Web/App Servers, Middleware	Internet Information Services (IIS), Windows Server
Platforms	Microsoft, PIM
Third Party Tools / IDEs / SDK / Services	Office 365
Scripting and Command Line Interfaces	PowerShell, YAML
Methodologies, Paradigms and Patterns	Solution Architecture Design
Mail / Network Protocols / Data transfer	TLS
Other Technical Skills	Bicep, CIS Benchmarks, CommVault, Kusto, SCOM, SOAR

WORK EXPERIENCE

Senior Security Engineer, Financial Markets Authority (Azure Security Architecture and Zero Trust Implementation)

Duration: May 2023 - May 2025

Summary: Implementation of Azure Virtual Desktop for Privileged Access Workstations and comprehensive Azure security architectures integrating Zero Trust controls aligned with NZISM and CIS standards. The project aimed to enhance security posture and compliance in a financial regulatory environment.

Responsibilities:

- Deployed Azure Virtual Desktop to create hardened PAWs for secure access.
- Engineered Azure security architectures with Conditional Access, PIM, NSGs, and Azure Firewall.
- Implemented advanced Microsoft Entra ID Conditional Access policies and RBAC models.
- Led threat protection strategies using Microsoft Defender Suite and Microsoft Sentinel.
- Conducted continuous security posture assessments and vulnerability management.
- Developed Bicep templates and automated deployment pipelines for Azure infrastructure.
- Designed secure network architectures including virtual networks, Azure Firewall, and NSGs.

Technologies: Azure Virtual Desktop, Microsoft Entra ID, Conditional Access, Privileged Identity Management, Network Security Groups, Azure Firewall, Microsoft Defender Suite

(Defender for Cloud, Endpoint, Identity, Office 365), Microsoft Sentinel, Microsoft Intune, Bicep, Azure DevOps, PowerShell.

Senior Security Engineer, LAB3 (Microsoft Sentinel and Security Assessments)

Duration: Jun. 2022 - May 2023

Summary: Conducted deep technical security assessments and implemented Microsoft Sentinel solutions for clients across various sectors. The project focused on enhancing threat detection, security monitoring, and risk mitigation through tailored security architectures and automation.

Responsibilities:

- Performed security assessments including configuration reviews and vulnerability analysis using Nessus.
- Designed and implemented Microsoft Sentinel data ingestion pipelines and KQL analytics rules.
- Developed custom Sentinel SOAR playbooks integrating external threat intelligence APIs.
- Implemented Active Directory Domain Controller hardening based on CIS benchmarks.
- Architected risk mitigation strategies and provided actionable security recommendations.

Technologies: Microsoft Sentinel, Kusto Query Language (KQL), Azure Logic Apps, Azure Function Apps, VirusTotal API, Nessus, Active Directory, Group Policy Objects.

Security Engineer, Defend (Security Architecture & Vulnerability Management)

Duration: Jan. 2022 - Jun. 2022

Summary: Provided security architecture consultation and led vulnerability management programs for Azure and on-premises environments. The project aimed to enhance security across infrastructure, applications, cloud, and OT environments using Zero Trust principles.

Responsibilities:

- Consulted on security architecture based on Zero Trust for Azure and on-premises.
- Led Cyber Security Vulnerability Management practice across diverse client technology stacks.
- Conducted security analysis and remediation for Microsoft Entra ID and Microsoft 365 tenants.
- Developed strategies to assess and enhance Active Directory Domain Services security posture.
- Delivered technical security expertise across client IT functions.

Technologies: Microsoft Entra ID, Microsoft 365, Active Directory Domain Services, Zero Trust Architecture.

Senior Systems Engineer - Health Alliance (Security Architecture and Infrastructure Hardening for Healthcare)

Duration: Feb. 2021 - Jan. 2022

Summary: Designed and implemented security architectures and hardening strategies for healthcare backup and monitoring systems to protect critical healthcare data and infrastructure.

Responsibilities:

- Designed security architectures for Commvault backup systems and System Center Operations Manager monitoring infrastructure.
- Executed OS hardening for Windows Server and Hyper-V based on CIS benchmarks.
- Led vulnerability analysis and remediation using Tenable SecurityCenter.
- Engineered migration and automation of server monitoring platform from SCOM 2012 to SCOM 2019.
- Provided security operations support including incident response and threat analysis.

Technologies: Commvault, System Center Operations Manager (SCOM), Windows Server, Hyper-V, CIS Benchmarks, Tenable SecurityCenter.

Microsoft Systems Engineer, Revera (Acquired by Spark) (Enterprise PKI and Security Architecture)

Duration: Dec. 2016 - Feb. 2021

Summary: Led security architecture and management of enterprise PKI and Microsoft infrastructure, ensuring compliance with government standards and optimizing security operations across the organization.

Responsibilities:

- Provided strategic security architecture guidance for Microsoft technologies including Servers, PKI, SCOM, and SCCM.
- Designed, deployed, and managed centralized tiered PKI compliant with NZISM and DIA requirements.
- Developed and automated system hardening standards enforced via SCCM and Group Policy.
- Architected enhanced security for Active Directory, PKI, and System Center infrastructure.
- Introduced automated patch management using SCCM.
- Managed and optimized Microsoft SCCM, SCOM, and PKI solutions focusing on automation and reliability.
- Optimized SCOM monitoring infrastructure reducing false positives through alert tuning.

Technologies: Public Key Infrastructure (PKI), Microsoft System Center Configuration Manager (SCCM), System Center Operations Manager (SCOM), Group Policy Objects, Nessus, TLS 1.2, Microsoft Servers.

EDUCATION

- **Graduate Diploma in Business Studies**
  Massey University
  2015 - 2016
- **Master's Degree of Mathematician**
  State University
  1997 - 2002

CERTIFICATION

- **Certificate of Excellence in Professional and E-Business Writing**