**mcp**

**Sergei Yakushko**

(British Citizen)

**Glocestershire**

**07851316675**

**01684 560 884**

**dan.ace@talk21.com**

**Profile**: Microsoft Certified Professional Wintel/ Azure Cloud Security consultant with over 18 years’ commercial experience supporting all round infrastructure for major clients in commercial, banking and government sector.

**Core Technical Skill Set**

* Azure – Strong knowledge and experience in Azure cloud security
* DevOps Azure Cloud Security
* Strong knowledge of Azure cloud security monitoring tools
* Experience in cloud security architecture
* Experience in delivery of security design and building and deployment of security infrastructures
* Experience in providing Azure cloud security advice to commercial organisations
* Experience in Windows server security and hardening
* Strong knowledge in Windows servers and infrastructure support
* Experience in hardening Azure applications
* Experience in Azure cloud logging and monitoring
* Experience in cloud vulnerability assessment and risk mitigation
* Azure ARM tooling, Azure PowerShell, Azure DSC, Azure Log Analytics
* Advanced Azure PowerShell skills, JSON
* Advanced knowledge in Azure Security Centre monitoring and configuration
* Experience in Azure OMS and Microsoft System Centre 2012 R2 (SCOM R2 and SCVMM)
* Experience in VSTS CI/CD (continuous integration and deployment)
* Strong knowledge of Azure Active directory (AAD)
* Experience in Azure cloud secure automation
* Active Directory Management, ADFS, Group Policies
* VMware vSphere 6, Power CLI
* Experienced in IBM and HP Server Hardware
* Experience of implementing, maintaining and managing Hyper-V environment
* Strong experience of working in ITIL compliant environment

**Professional Experience**

**August 2018 – Now** **KPMG** Canary Warf

**MS Azure Security DevOps consultant**

* Acted as Azure Cloud Security consultant for GSOC (Global Security Operations Centre)
* Delivered and implemented logging and alerting solutions - PowerShell, JSON
* Conducted cloud security audit to prepare and document vulnerability assessment reports - PowerShell
* Conducted cloud infrastructure inventory security focused – PowerShell, Azure Security Centre (ASC)
* Identified the gaps and misconfigurations in the current designs and recommended changes to enhance security and reduce risks
* Conducted cloud security controls audit on subscriptions level, produced and documented the reports on for Azure subscriptions - Secure Azure DevOps Kit
* Reviewed baseline security policies including Azure Security Centre, Azure policy and produced and documented reports – PowerShell
* Implemented Azure security policies (PowerShell, JSON)
* Prepared and documented recommendations on the tuning of security controls
* Engaged in developing a solution for streaming Azure Security Centre logs into customer security solution Microsoft Graph Security API and JSON
* Conducted with Cloud security monitoring on a daily basis - ASC, AADIP, ATP, CAS, Office 365 Security
* WDATP (Windows defender advanced threat protection) and Sentinel (Azure SIEM)
* Helped to establish good practise in security monitoring and response processes for the cloud security monitoring
* Prepared and documented cloud incident response procedures for various use cases
* Provided GSOC team with trainign on Azure security centre monitoring and management, Azure IaaS, Log analytics (Kusto Query Language) and Azure PowerShell
* Assisted the GSOC team in dealing with High and Medium severity security alerts
* Conducted threat hunting on a regular basis and assisted in applying cloud security threat hunting to the SOC
* Everyday support and maintenance of security tooling
* Reviewed new technologies to define the strategic roadmap

**November 2017 – July 2018 Evolve Azure Services (SFA- GOV.UK)**  Coventry

**MS Azure Security DevOps consultant**

Acted as Azure Cloud Security Operations engineer on a security remediation project

* Azure cloud infrastructure hardening based on CIS Benchmarks
  + ASC (Azure Security Centre) as a SOC (security operations centre) implementation
  + Azure security centre alerts monitoring, incidents investigation
  + Conducted cloud assets risk and security assessment
  + Automated vulnerability identification
  + CAS (Cloud application security) and ATP (Advanced threat protection)
  + Cloud Assets compliance assessment
  + Created IAAS compliance profiles ( Qualys and Policy Azure Security Centre )
  + Developed PS scripts and introduced it as a part of security toolkit for End Points, NSGs, Disc Encryption, Ports exposure assessment and reporting
  + Developed and introduced the script to produce monthly Azure Security Centre Status Reports.
  + Introduced Secure DevOps Kit for Azure (AzSDK) to produce security assessment and recommendation reports
  + Produced security policy and procedure documentation
  + Produced detailed Azure Security Centre documentation
  + Cloud Security controls implementation
  + Created standards for technical architectures to support secure cloud environments across Azure
  + Discussed cloud security/best practices with architects and technical teams
  + Researched and recommended best practices around cloud compliance
  + Azure Security Centre ( ASC ), OMS and Log Analytics monitoring

**August – November 2017 KCOM (NFU)** Stratford-upon-Avon

**DevOps Engineer**

* Acted as a DevOps engineer on web application migration from on-premises to the cloud (PaaS) and provided IaaS support
* Setting up infrastructure as a code: ARM Templates, JSON, VSTS, PowerShell, VS
* Designed and created ARM templates for orchestrated deployment (Linked templates)
* Added and configure the following resources within an ARM template:
* AppService, AppService plan, NSGs, VNet, VNet, Gateway, VMs, Storage Accounts, PowerShell DSC Extensions
* Deployed the templates using VSTS
* API migration, API management DR
* Business to Business (B2B) automation
* Prepared hand-over documentation

**April 2016 –July 2017 The Co-op Group** Manchester

**Wintel and Cloud Engineer**

Working as Wintel\Cloud support resource for systems administration, developers and network engineering groups on different Co-op Bank projects and BAU

Azure IaaS Security:

* Validated IT infrastructure and other reference architectures for cloud security best practices
* Determined baseline security configuration standards for operating systems
* Assisted in identifying security design gaps in existing and proposed architectures and recommend changes or enhancements.
* Azure Cloud security implementation
* Authoring ARM templates
* NSGs (Network Security groups)
* Azure Security Automation
* RBAC (Role Based Access Control)
* Hardening Azure applications

**January 2015- April 2016 Capgemini (HMRC account**) Telford

**Wintel and MS Azure consultant**

* Working as Wintel\Cloud support engineer provided support and maintained server infrastructure at all sites, consisting of 400+ servers
* IAAS Environment setup, configuration and management
* Provisioned VMs using ARM and PS DSC
* Setup Apps performance monitoring, alerts, scaling, diagnostics
* Configuring Group Policies in accordance with CESG guidelines for windows 10
* Provisioned 3rd /4th line support and resolution for escalated or critical IT infrastructure-related incidents, service requests
* Provisioned physical and virtual servers (Azure Cloud, Hyper-V and VMware)
* Proactively monitored infrastructure via System Centre 2012 Operations Manager
* SCOM administration
* Used PowerShell Scripting to automate various tasks
* AD management, troubleshoot and automation
* Managed capacity on customer servers
* Troubleshooted and maintained IBM, HP and Fujitsu servers
* Involved in servers patching
* Identified areas of improvement and implemented various automation tasks
* Delivered various proposals making recommendations for improvements of the existing technical environment
* Shared best practices and improved processes within the team and across the infrastructure.
* Provided training for junior engineers

**March.2013- November 2014 IBM (RPA and DEFRA Account)** Reading

**Senior Wintel Engineer**

* Maintained, configured and monitored 800 + physical and virtual Windows servers across a multi-site, 2000 users infrastructure
* Provided second and third line troubleshooting, diagnosis, and timely problem resolution for all of the above systems
* Implemented new service requests, reviewed and impact assess new business requirements
* AD administration and automation
* Hyper-V environment administration
* Capacity management
* Backup management, backup Configuring\troubleshooting
* Major incidents root cause analysis
* GPO upgrade and troubleshoot
* Hardware upgrades on HP Servers
* Hardware troubleshoot
* Physical and virtual servers provisioning, activation and on-boarding
* Provided out of hours support via the on-call rota if required

**Feb. 2010- October 2013 IBM (RPA and DEFRA Account)** Reading

**Wintel Infrastructure Support Engineer (project and BAU work)**

* Provided day-to-day business as usual support and administration of Wintel infrastructure (800+ Servers 2003 and 2008 R2/2012, Servers 2008 Server Core and 1500+ users base), Writable and Read-Only DCs
* Hyper-V infrastructure build
* Infrastructure refresh: server migration from 2003 to 2008R2
* Provided various lines of support for Wintel servers issues
* Upgraded customer infrastructure to Windows Server 2008 R2 and Server Core, servers deployment, post-build configuration and service activation (project), servers decom.
* HP and IBM Servers (HP DL380 G6 AND DL580 G5) build and roll-out using Windows Deployment Services, MDT and HP Rapid Deployment Tool (project)
* SCVMM, SCCM R2 and SCOM deployment, set-up and testing (project)
* Virtualized regionals sites to Hyper-V, installed, configured and managed SCVMM
* Hyper-v VMs (virtual servers) build, configuration and roll-out (project)
* Read Only DCs build and configuration for regional sites (project)
* GPO changes roll-out
* Provided post-deployment support and administration
* Administration of backups and recoveries (Backup Exec and NetBackup, DPM)
* IIS support and troubleshooting
* DNS and DHCP management
* AD administration (BAU and AD project related work)
* IIS support
* VMware infrastructure support
* HP and IBM server hardware troubleshooting

**October 2005- Sept.09 IBM (DEFRA Account)** Farnborough

**Wintel Infrastructure Support Engineer**

* Provided 2nd and 3rd line support on-site and remotely for more than 800 Windows File and Exchange Servers
* Proactively monitored all core server operations, services and performance using various monitoring tools including:
* Compaq Insight Manager, IBM Director, Microsoft Operations Manager 2005SP1, Perfmon and PAL, Sysinternals Tool, Virtual Centre Performance tools
* Provided technical guidance, incident monitoring and resolution for escalated support issues, raised by the Service Management/Helpdesk to specific operating systems problems via Assyst Helpdesk Software and Tivoli Monitoring fault tracking system
* Carried root cause analysis of the incident, identified the root cause and rolled out solutions. Dealt with majority MIs (Major Incidents)
* Build new (2K, 3K and 2008) servers on the project manager’s request. Used server network image, Altiris and Smart Start, building remotely and on site as required
* Had been involved in full cycle newly build servers activation and decommissioning NT4 servers
* Raised Change Requests with Change Management and after approval applied all necessary changes to AD, DNS, WINS, Server Monitoring software, Morning Checks scripts and Backup Schedule
* Involved in servers move from Guildford office to IBM data centre. Carried out racking, patching, pre and post move reconfiguration and changes. Run post move checks
* Installed and Configured ESX3.5 and VSphere4 servers, Virtual Centre and vClients
* Created new VMs using ISO image and master template Managed ESX Hosts and VMs resources via vCenter
* Involved in securing ESX hosts, vCenter and VMs
* Monitored and troubleshooted vCenter, ESX hosts and VMs
* Run ESX Hosts and VMs performance monitoring
* Monitored and troubleshooted xSeries IBM Servers, Blade Centres and HP Servers locally and remotely. Analysed PFAs and system alerts, raised calls with hardware suppliers, replaced failing parts, carried out system upgrades. Upgraded server memory, hard disks, networking cards and firmware. Carried out RAID and remote server access management cards reconfiguration as required
* Proactively monitored use of shared systems for capacity and utilization using Tree Size and Tembria. Provide Service Management with capacity utilization reports for entire estate on a monthly basis
* Administered and maintained end user accounts, permissions, and access rights. AD administration.
* Outlook support. Mailboxes restore. Mail delivery trouble-shoot. PSTs recovery and repair. Exchange server users administration and monitoring
* Monitored and tested server software performance and provided statistics and reports
* Dealt with backups administration and restore tasks using Backup Exec and Tivoli (TSM) client
* Carried out user’s data and accounts migration from NT4 to W2003 servers using scripts and Quest
* Vista post-deployment support and troubleshooting
* Applied change control procedures to all service areas
* Made sure privileged users, newly build servers and applications are GCSx compliant
* Provided junior members of staff with guidance and support

**March 2005 – September 2005 State Street Bank and Trust** Canary Wharf

**3rd Line Infrastructure Support Engineer**

* Provided 3rd line support for more than 500 servers.
* Monitored server performance, availability and health via NetIQ AppManager 5.0.1 and HP Insight Manager.
* Dealt with SLA server related tickets and incidents
* Servers build and activation. Servers decommissioning.
* AD administration
* RIBs install and configuration.
* Servers racking and patching.
* Infrastructure morning checks and taking appropriate action should the problem arise.
* Blackberry server user administration.

**October 2004 – Feb.2005 Force Techi (Credit Suisse First Boston Account**) Canary Wharf

* Post Deployment support and roll-out Engineer
* Servers, Desktops and laptops build, configuration and roll-out
* Post-deployment support on-site and remotely

**June 2002- October 2004 XANSA UK PLC** Thames Valley Park

**Infrastructure support engineer**

* Provided 2nd and 3rd line infrastructure with 250 servers
* Dealt with SLA desktop and server related calls
* Proactively administered and supported Windows NT4, 2K and 2003 servers
* Provided support for Exchange Server5.5 and Outlook client
* Dealt with backups and restores using Backup Exec8.6, Arc Backup Server
* Carried out printer’s installation and support
* Provided management with the root cause analysis of major incidents assigned.
* Supported and maintained Dell and Compaq Servers
* Carried out hardware upgrades and replacement
* Server builds configuration and activation.
* Desktop and laptop build using Ghost imaging
* Provided advice to users and colleagues, supported by documentation as appropriate aimed at reducing the frequency and impacts of incidents.
* Arranged return and repair of faulty equipment.

**February 2001 – June 2002 Effective Solutions for Businesses** London

**IT Engineer**

* Provided mixture of first, second and third line support for 25 small and medium size businesses (250 users) around London
* Provided support of Windows (95-98, Windows2K, XP), Windows NT4, Server NT4, SBS, Backup Exec7.0,
* Server and client’s hardware upgrades and replacement
* Server NAV7.5 clients roll-out. NAV server administration
* Network connectivity troubleshoot
* Local and network printer’s setup

Employment history before February 2001 is available on request.

**Education:**

**Current** Studying towards Microsoft Azure and AWS Security certifications

**Sep 2004 Reading College of Art**

UNIX Management and programming course

**Feb.2000 Azlan Limited**

Small Business Server

**Sep.99-Nov. 99 Stepping Stones LTD**

MCP NT4 Workstation and Server4

**1986-1993 Moscow State Institute of International Relations (MGIMO)** BH in Economics

**References:** Available on request

**Security Clearance:** BC +, Scotland disclosure

**Availability:** Four weeks’ notice

**Mobility:** Flexible, car owner

**Travel:** Flexible

**Languages:** English, Russian and basic Arabic