Jay Muzein, CISSP

Summary

IT professional with over 18 years of experience as Risk Architect and Lead Security Engineer. Risk mitigation by designing and deploying highly available enterprise Network security solutions per architectural guidelines and industry best practices. Technical expertise in the design, deployment and management of network security technologies such as Firewalls, Proxies, SEIM, Cloud Secure Gateways, Cloud Access Security Brokers and Threat Intelligence tools. Drive implementation and adoption of new tools, capabilities, frameworks, and methodologies across all teams within the SOC. Enterprise virtualization, Web Applications, Data Lake deployment and performance management. WAN, LAN and Infrastructure consolidation and cloud migration. Technical expertise in Vulnerability management and remediation, IT Auditing, technical controls per NIST SP 800.53, ISO 27000. STIG Compliance, A&A Accreditation. Effective thought leader and communicator for team environment and present complex concepts to management.

WORK history

NASA GSFC – Goddard Space Flight Center – Greenbelt, MD April 2022 – Present

Lead Security Engineer & Architect

**Description of Environment:** NASA GSFC environment consists of premier space flight physical and cloud-based platforms and infrastructure on distributed datacenters across multiple States and Countries.

**Description of Responsibilities:** Lead a team of Information System Security Officers (ISSO) and Information Systems Security Engineers (ISSE) for Federal Information Security Management Act (FISMA) Information System Security Plans following the NIST Risk Management Framework (RMF) supporting the Goddard Space Flight Facility (GSFC). Maintain systems security plans, contingency plan testing and associated system accreditation activities required to maintain Authority to Operate (ATO) per the NSSC Guidelines. Coordinate directly with the NASA Information System Owner (ISO), Management Team, and other Security related resources to address IT System Security concerns or issues related to the Information Systems. Manage and facilitate the Plan of Action and Milestones (POA&Ms) and Risk Based Decisions (RBDs) in the NASA RSA Archer Risk Information Security Compliance System (RISCS) associated with the Information Systems. Development, implementation, and continuous improvement of security operational procedures (SOPs),

tailored to organizational circumstances and regulatory compliance obligations as applicable (e.g., HITRUST,SOC, HIPAA, ISO-27001/2, PCI, GLBA, FedRAMP)

Implement and perform credentialed vulnerability scans against the Information Systems utilizing the Tenable Nessus Security Center Vulnerability Scanning System. Create work orders assigned to the Systems and Network Administrators for remediation of discovered vulnerabilities. Identify vulnerabilities using tools such as Tenable Nessus, BigFix, ForeScout, Incident Management System, Splunk or other IT Security Tools. Implement vulnerability remediation timelines in accordance with NASA policy. Participate in Security Controls reviews and Assessment preparations as a part of Continuous Monitoring and annual Assessment and Authorization (A&A). Review and update Implementation Details of Security Controls in the RISCS (Archer) systems. Review and implement remediation requirements set forth by NASA Security Operations Center Mitigation Action Requirements and Situational Awareness Reports (SOC MARs and SARs) when applicable. Assist with the execution integration testing to ensure safeguards supporting data protections and system connections are functioning as expected and producing desired results.

Leidos – Washington, DC November 2021 – April 2022

US Department of Homeland Security – Washington, DC March 2020 – November 2021

Lead Security Engineer & Architect

**Description of Environment:** DHS HQ environment consists of physical and cloud-based platforms and infrastructure on distributed datacenters. The environment supports production and development SaaS applications and platforms, virtual desktop Infrastructure, mobile applications, proxies, load balancers and other end user applications.

**Description of Responsibilities: Lead a team of Security Architects and Engineers on projects and initiatives involving modernization of DHS HQ’s infrastructure. Subject matter expert responsible for providing expert level technical analysis to enhance Security Authorization requirements compliant with Federal regulations and policy. Assist in building, assessing, and documenting security architecture roadmap to transform current state to an improved and effective end state compliant with FISMA Authorization.** Drive implementation and adoption of new tools, capabilities, frameworks, and methodologies across all teams within the SOC. **Team lead developing Initial Operating Capability (IoC) for modernizing DHS HQ’s legacy Trusted Internet Connection (TIC) architecture to TIC3 using tools such as Zscaler cloud and McAfee CASB. Integrate collected cloud logs with CISA’s Cloud Log Aggregation Warehouse (CLAW) as well as export to DHS HQ’s enterprise Splunk log aggregation tools. Collaborate, facilitate, and conduct infrastructure and network assessment, coordination, monitoring, traffic analysis, optimization technology such as SolarWinds Orion, Splunk, FireEye Mandiant, Nessus. Support in the migration security tools to cloud environment such as AWS and Azure.**

Systegra – Washington, DC November 2019 – March 2020

Sr. Systems Security Engineer **US Department of Treasury**

**Description of Environment:** US Treasury Department Offices (DO) environment consists of cloud-based networks and FedRAMP certified AWS infrastructure on redundant datacenters. The environment supports production and development SaaS applications and platforms, virtual desktop Infrastructure, mobile applications, proxies, load balancers and other end user applications.

**Description of Responsibilities: Architect the scanning infrastructure, interface with government client, and collaborate with team of engineers and ISSOs to ensure effective operations and security gaps remediation. Program lead for escalation and SME for addressing failed, incomplete and contested scan results. Oversight of Tenable, Qualys, DB Protect and Websense scanning within policy framework. Create custom dashboard and feed vulnerability scan data into a common dashboard on Splunk. Architect solutions to expand the scans to other areas and departments. Collaborate with Internal IT control testing of Security Architecture, Identity and Access management. Assess gaps in security function design, security infrastructure, datacenters, dataflows and encryption. Review POAM artifacts, IT control testing and operational auditing per NIST SP.**

Robert Half Technology – Washington, DC October 2019 – February 2020

Information Assurance Assessor **Salesforce**

**Description of Environment:** Salesforce environment consists of cloud-based networks and FedRAMP certified AWS infrastructure on redundant datacenters. The environment supports production and development SaaS applications and platforms, virtual desktop Infrastructure, mobile applications, proxies, load balancers and other end user applications.

**Description of Responsibilities: Internal IT control testing of Security Architecture, Identity and Access management, large and complex security program execution and implementation. Assess gaps in security function design, security infrastructure, datacenters, dataflows and encryption. Review POAM artifacts, IT control testing and operational auditing per NIST SP, PCI and ISO 27000 series controls.**

Edison Electric Institute – Washington, DC September 2015 – November 2019

Network Security Architect

**Description of Environment:** EEI environment consists of highly available network and virtualization infrastructure on redundant datacenters. The environment supports production and development SharePoint solutions such as Corporate Intranet and Public Internet sites, virtual desktop Infrastructure, mobile applications, proxies, load balancers and other end user applications as well as cloud-based SaaS applications.

**Description of Responsibilities: Technical lead in migrating legacy Managed Service Provider (MSP) supported infrastructure tools such as DNS, AD, Mail gateways, Firewalls and Threat prevention tools to a modern and cost-effective MSP environment utilizing cloud solutions such as AWS, Mimecast, Azure and third-party DDoS protection and Reverse proxy services.** Network security and vulnerability management including threat monitoring and analysis, asset management, Incident response and Information management using tools such as Nessus, QualysGuard, CheckPoint Enterprise Firewalls, Cisco Umbrella, Cylance Anti-Malware and AWS Route53 DNS. Technical expertise in the Design, deployment and management of network security infrastructure including firewalls, routers, IPS/IDS/DLP, Application and web filters, NetScaler load balancers, Enterprise Anti-malware, Network access control devices and SaaS based Mail filters. Team lead IT security self-assessment, vulnerability scanning and risk mitigation using compliance standards such as PCI-DSS, CIS and NIST. Assisted in the excellent achievement of the organization’s security assessment performed by third party assessors in 2019. Responsible for datacenter security, business continuity and Disaster Recovery planning and implementation.

Robert Half Technology / 1901 Group, Inc March 2015 – September 2015

Senior Security Engineer **US Department of Health & Human Services**

**Description of Environment:** DHHS OIG program consists of FedRAMP certified private cloud, physical datacenter and DR site, and over 80 regional sites. Support modernization and migration of datacenters to USDA NITC private cloud. Subject matter expert for deployment and migration of Firewalls and security infrastructure. Maintain security controls and coordinate the remediation of security vulnerabilities.

**Description of Responsibilities:** Support consolidation of Network security infrastructure and migration of datacenter assets to FedRAMP certified Federal private cloud infrastructure. Apply NIST’s FISMA guidance in the design, modernization and consolidation of enterprise security infrastructure including firewalls, Intrusion prevention devices, and content filtering and VPN appliances. Subject matter expert for the design, implementation and maintenance of enterprise Check Point firewalls. Participate in regular meetings to correct weaknesses and deficiencies of security controls. Update System Security Plan remediate POAM and collect artifacts for closure. Network security and endpoint devices troubleshooting, monitoring and optimization. Design network and security infrastructure diagrams using MS Visio, technical update of project plans, disaster recovery plans and standard operating procedures.

SAIC April 2014 – March 2015

NTTData Dec. 2012 – April 2014

Senior Security Engineer **US Securities and Exchange Commission.**

**Description of Project Environment:** SEC EDGAR program consists of highly available CheckPoint enterprise firewalls, McAfee enterprise firewalls and security devices in distributed environment. The environment included hundreds of high-end servers and blades supporting Solaris, Linux and Windows systems in physical and virtual environment. Security devices include Tipping Point IPS, Splunk, Skybox, Qualys enterprise scanners, Application and database scanners and clustered firewalls.

**Description of Project Responsibilities:** As a Security Engineer and Analyst, identified security risks, threats and vulnerabilities of networks, systems, applications, and new technology initiatives. Provide technical support in the design, development, testing and operation of enterprise firewalls, IPS, anti-virus, Vulnerability scanners, Windows Servers and software deployment tools. Build, configure, maintain and support highly available CheckPoint Enterprise firewalls, McAfee Enterprise firewalls (Sidewinders) and Bind based Internal and External DNS resolvers, Tipping Point IPS, Skybox, Qualys Vulnerability Scanner, Splunk, ArcSight, Guardium, AppDetective, Akamai web filter. Identify and oversee the installation, consolidation or modernization of hardware and software components and any configuration changes that affect security. Migration of security appliances to VMware virtual platform. Migration of Bluecoat Web Application filters to cloud based Web Application Firewalls such as Akamai Luna.

AT-Tech, Inc. May 2012 – Dec. 2012

Network/Systems Analyst Host Marriot Services (HMS) Corporation

**Description of Project Environment:** Enterasys switches, Windows 2003/2008 Servers, Xerox WorkCentre printers, Point-of-Sale terminals and SonicWALL firewall support at 100 client sites.

**Description of Project Responsibilities:** As Network Systems Analyst identified and analyzed a component’s existing or new peripheral, network, and telecommunications systems requirements. Troubleshot and resolved trouble tickets with network infrastructure, including routers, switches, firewalls, VPN, Proxy servers, Windows servers. Applied operating system patches and software upgrades, and performed routine hardware configuration tasks. Maintained computer networks and related computing environments including computer hardware, network printers, system software, applications software, and configurations. Implemented network security measures to protect data, software, and hardware. Escalated problems and coordinated with senior level support group or vendors to monitor progress. Supported AD user account maintenance, Exchange email, OS migration, and Point of Sale related issues.

Radiant Systems, Inc. May 2008 – May 2012

Systems Deployment Engineer Radiant Systems, Inc

**Description of Project Environment:** 150 client sites in Washington, DC metro area supporting Remote office network and systems deployment. Design, deploy and maintain Hotel management Systems, Network Security and payment card devices. Supported Windows 2003/2008 AD users and computers, Windows XP, and Windows 7 Professional workstations, branch office VPN and wireless devices.

**Description of Project Responsibilities:** As Systems Support and Deployment Engineer, implemented comprehensive security programs based on industry best practices of PCI-DSS and PA-DSS guidelines with regard to enterprise application, payment card systems, (AD) Directory users and computers, firewalls, and Routers. Conducted patch management on network and onsite to ensure servers and workstations have current up to date OS, applications, patches and Anti-virus software. Performed vulnerability assessment, anti-virus and malware scan on systems. Configured and installed network devices including SonicWALL and WatchGuard Firewalls, and Cisco Series Routers and switches. Installed and supported servers, workstations, remote printers, and laptops. Performed post-deployment quality control on systems and hardware. Administered backup/recovery solutions using RAID, Ghost Image Server and Aloha Command Center systems management tool. Resolved merchant, database, application user roles and back office management systems issues.

Menu Hospitality, Inc. June 2006 – May 2008

Systems Administrator Washington, DC

**Description of Project Responsibilities: Administer user accounts, email, network setup. Configure and manage System policies. User profiles and Remote access for workstations. Ensure the overall performance and utilization of IT resources. Responsible for networking, server configuration, installation and migration, data archiving and system recovery. Prepare workstations and laptops for deployment by installing operating systems, drivers, application software and TCP/IP connections. Troubleshoot, repair and support service desktops, laptop, printers and other network equipment. User training on utility application software and company specific applications. Resolve POP3, Outlook Express, Mail2000, Email and Network issues.**

NavStar, Inc. January 2000 – July 2002

Systems Administrator Washington, DC

**Description of Project Responsibilities: Install, configure and maintain Antivirus software and updates. Responsible for networking, server configuration, patching, installation and migration, Data archiving and System recovery. Deploy and administer user applications such as, GoldMine data mining, QuickBooks and Peach Tree accounting software. Configure and manage system policies, user profile and Remote access on NT4 Enterprise servers. Upgrade and replate hardware components, Network devices and cabling. Troubleshoot Windows 95, Windows 98 and Windows NT4.0 Workstations and Servers.**

Education

|  |  |  |  |
| --- | --- | --- | --- |
| School Name | Years Attended | Type and Year of Degree | Major |
| George Washington University | 2018-2020 | M.S. Engineering, 08/2020 | Information Systems-Cybersecurity Engineering & Management |
| Strayer University | 2009-2011 | B.S., 04/2011 | Information Systems-Cybersecurity |

certifications

|  |  |  |
| --- | --- | --- |
| Certification | Certifying Organization | Year of Certification |
| CISM (Certified Information Security Manager) – 1842191 | ISACA | 2018 |
| CISA (Certified Information Systems Auditor) – 18149468 | ISACA | 2018 |
| CCSP (Certified Cloud Security Professional) #415639 | (ISC)2 | 2017 |
| CISSP (#415639) | (ISC)2 | 2012 |
| VCP-DCV (VMW-01592704Z-00507137) | VMware | 2015 |
| CCSE R77 (#CP0000083478) –Enterprise Firewall | Check Point | 2015 |
| CCNA +Security (#CSCO12114600) | Cisco | 2013 |
| MCITP Server Administrator (#9299889) | Microsoft | 2012 |
| CompTIA Security+ (#COMP001020345476) | CompTIA | 2011 |

Awards

|  |  |  |
| --- | --- | --- |
| Institution | Type | Year |
| Strayer University | Suma Cum Laude, GPA 3.92 B.S. | 2011 |
| The George Washington University | Cum Laude, GPA 3.65 M.Eng | 2020 |

Technical training

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Title | Type | Hours | Training Vendor | Year Completed |
| Mobile & Cloud Security | Masters Course-Classroom | 30 hours | GWU | 2019 |
| Audit & Risk Assessment | Masters Course-Classroom | 30 hours | GWU | 2019 |
| Check Point Firewall | Computer-based | 50 hours | CheckPoint Technologies | 2015 |
| Amazon AWS Cloud Architect | Boot Camp | 40 hours | AWS | 2019 |
| VMware vSphere 5.5 | Boot Camp | 40 hours | VMware, Inc | 2015 |
| Cisco ASA | Vendor Training | 30 | Cisco | 2018 |
| Disaster Recovery | Classroom | 50 hours | Strayer University | 2010 |

Membership

Check Point Firewall expert network

InfraGard Greater Washington

ISACA Greater Washington

(ISC)2 Volunteer