Sr. Security Engineer Sr. Security Engineer Sr. Security Engineer - Tasacom Technologies Burlington, MA Over 11+ years of experience in Web Application Security, Security Architecture & Design, Penetration Testing and Secure Coding. In-depth knowledge of Mobile Application Security, Application Security Controls and Validation, IT Risk Assessments, Regulatory Compliance and Secure Software Development Life Cycle (secure SDLC) and Continuous Integration (CI) and Continuous Delivery (CD) of security scanning. Hands-on with Penetration Testing, DAST, SAST and manual ethical hacking. Experience in conducting IT Security Risk Assessments in accordance to NIST and FFIEC framework. Working knowledge of AWS and MS Azure Cloud Security. Worked with global security teams performing application and IT infrastructure security assessments. In-depth knowledge of penetration testing for web and mobile (iOS and An-droid) applications. Hands on Experience building physical servers from a bare metal and VM, perform server hardening, and deliver them to the respective teams. Experience in Installing patches and software upgrades recommended by IIS server. Configured and managed IIS 7.0/8.0 Technical knowledge & proficiency in Windows Servers, VMware and Network Administration, Window Servers. Experience with Virtualization technologies like Installing, Configuring, and Administering VMware ESX/ESXi. Experience in iSCSI Experience in Developing and Implementing of Information Security Policies and Guidelines as per OWASP (Open Web application Projects), SANS Secure Coding guidelines Hands on Experience on vulnerability assessment and penetration testing using various tools like Burp Suite, Fiddler, ZAP Proxy, SQL map, HP Web Inspect and IBM App Scan,checkmarx, HP fortify. Having experience in identifying SQL Injection, Script Injection, XSS, Phishing and CSRFattacks. Having 9+yearsof experience with expertise in Windows Administration and VMware administration, Implementation, Installing, Monitoring and Troubleshooting of network and communication equipment. Practical work experience in Installing, Maintaining, Monitoring, Troubleshooting and Managing Blade Center server, Configuring and Zoning Storage Area Networks and SAN Switches and VMware ESX Server Administration. Build an Release HPE Proliant(DL/BL) physical and VMware Virtual servers using windows servers 2008/2012 R2. SAN, NAS, NFS storage and RAID Concept.. Expertise in area of virtualization

with vSphere, VMware ESX 6.x, 5.x, hosts& Virtual Center server till 6.0. Deployed key VMware ESX/ESXi technologies, expertise with HA/DRS, P2V. ESX migrations from 4.1 to 6.0 to VSphere 5.0, 6.0. Worked on HA and DRS cluster configurations and applying FT for business-critical applications. Resource Monitoring for vCPU, RAM, Network and Storage in vCenter Server. Expanding disk space (LUN) for hosts running on VMs and physical ESXi. Create, configure, manage ports, port groups, vLAN, NIC teaming using vSphere standard(vSS) and distributed switches. Installing McAfee Antivirus and updating the client DAT version on the physical and virtual servers as a part of hardening process. Good exposure to Solar Winds Patch manager for patching the windows servers. Configured Solar windows patch management with WSUS for the first time after installing. Remote Management and troubleshooting of Dell BL on M1000e chasing using iDRAC7 console. Remote deploy, update, monitor and maintain Dell PowerEdge Servers using iDRAC7 console. Proficient in transferring and seizing of FSMO/AD roles between domain controllers. Experience on Red hat Linux Server & Desktop Environment using through Virtual Machine under VMware. Experience in Package management using RPM and YUM in Red Hat Linux. Installing, upgrading, and configuring RHEL 3, 4, 5 and 6 using Kickstart. Experience in Managing Multiple Windows Systems with Microsoft SCCM 2007 &2012 providing Patch Management, Remote Control, Software Distribution and OS deployment. Good experience on Microsoft Azure and Create a Virtual Network on Windows Azure to connect all the servers. Strong Experience on Administration and Troubleshooting of Azure IAAS Components (VM, Storage, VNET, OMS, NSG, Site to Site VPN, RBAC, Load Balancers, Availability Sets). Experienced in Office 365 activities. Design complex solutions which integrate AWS cloud, on premise physical & Virtual server, EC2, S3 storage, networking and security. Experience in installing, configuring, supporting and troubleshooting Unix/Linux Networking. Experience with Virtualization technologies like Installing, Configuring, and Administering VMware ESX/ESXi. Experience working on IBM P/E series, IBM XSeries 346, 3650, 3650m2/m3, HP and Dell PowerEdge hardware. Experienced in configuring DNS, DHCP, WINS and Active Directory Services in Windows based server environments. Experience with deployment to VDI environment such as

Updates/patches/Applications. Extensive understanding of networking concepts, (IE. Configuration of networks, TCP/IP, VPN, VLANs, and routing in LAN/WAN, Ethernet Port, Patch Panel). Strong understanding of VMware Networking concepts like creation of vSwitches, different types of Port groups, NIC Teaming and VLAN Problem management. Experience in Upgrading ESX 5.0 to 6.0-using VMware Update Manager. Experienced in performing Cloning, Cold Migrations and Hot Migrations and taking Snapshots. Experienced in creating Virtual Machine Templates and deploy virtual machines from templates and allocate resources. Exposure on vMotion migration, High Availability feature, DRS feature and Setting VM priorities on CPU and Memory resources. Troubleshooting BSOD, OS, RAM, CPU, Disk space, RDS, trust relationship, MS Office tools, Windows services, network and storage issues in Windows environment. Authorized to work in the US for any employer Work Experience Sr. Security Engineer Tasacom Technologies - Burlington, MA September 2018 to Present Responsibilities: Configuring, implementing and maintaining all security platforms and their associated software, such as routers, switches, firewalls, intrusion detection/intrusion prevention, anti-virus, and SIEM. Involved in Security Operation, Vulnerability and Risk Assessment, alerting report generation and analysis with various security tools (Splunk, McAfee ePO, Symantec DLP, Imperva, Sourcefire (IDS/IPS), FireEye. Bluecoat Proxy, etc Leverage Qradar, Security Onion, and Bro to gather network forensic artifacts and for retrospective analysis. Performed retrospective analysis, incident response, and network forensics with Bro, Suricata, and Sourcefire IPS in an enterprise Upgrading the code from Pan OS 6.0.X to 7.1.X. Experience working on Panorama M100. Migration from Cisco ASA to PA firewalls. Palo Alto design and installation (Application and URL filtering, Threat Prevention, Data Filtering). Configured and maintained IPSEC and SSL Global Protect on Palo Alto Firewalls Designed and configured Palo Alto Central Management Platform with Panorama and Wildfire Deployment. Perform network forensic analysis on acquired pcap and Bro metadata. Analyzed network traffic for malicious attacks using an internal kit with Bro,Suricata, ELK, and Snort. Use of Security Onion (Sguil, Elsa, bro), for network alerts, data correlation and analytics Utilize Mcafee EPO for Data Loss Prevention (DLP). Responsible for performing application whitelisting using Microsoft and

Mcafee Applocker tools. Consolidating analysis of suspicious Splunk data security event logs (Windows Defender, AppLocker, Audit Events, successful malicious. Analysis of multiple log sources including firewalls, routers, switches, web servers and multiple networking devices. Responsible for assisting with deployment of network infrastructure configurations across multiple product and technologies. Acted as the primary responder for managed security incidents pertaining to client firewalls and all network infrastructure components. Part of the Blue Team to identify the vulnerabilities and have a defense mechanism in place. Learned and helped IR team with Log collections, analysis, and forensic activities. Investigating logs and payloads for server crashes/core dumps, DDoS attacks, SQL/XSS, SPAM, etc. Installing and configuring Qualys in premises and on cloud environment. Responsible for performing vulnerability assessment on critical systems using Qualys. Configured and scheduled Qualys Scanner in QRadar to perform scan on regular intervals. Collaborate with team members in tuning SIEM applications to establish a baseline for network activity and rule out false positive events. Coordinate with SMEs to resolve any security incidents and correlate threat assessment data as needed. Support in the detection, understanding and resolving information security incidents affecting information systems & the business. Research and recommend corrective actions to ensure information dissemination regarding targeted or potentially targeted attacks. Investigate, document and recommend appropriate corrective action plans relating to IT security. Provide root cause analysis and remediation techniques for management regarding security incidents and governance documents Installed, configured and maintained of Cisco 7206/3660/3640/2600/2500 series routers LAN/WAN hardware including Cisco Switches, switches panel's installation, configuration and troubleshooting.

Performed switching technology administration including VLANs, inter-VLAN routing, Trucking, STP, RSTP, port aggregation & link negotiation. Worked with network services like DNS, DHCP, DDNS, IP4, IP6, IPSec, VPN etc., Involved in Design, implementation and operational support of routing/switching protocols in complex environments including BGP, OSPF, EIGRP, Spanning Tree, 802.1q, etc. Design and implement Catalyst/ASA Firewall Service Module for various LAN's. Key contributions include troubleshooting of complex LAN/WAN infrastructure that include routing

protocols EIGRP, OSPF & BGP. Configured Client VPN technologies including Cisco's VPN client via IPSEC. Configuring ACL to allow only authorized users to access the servers. Participated in on call support in troubleshooting the configuration and installation issues. Installation, Maintenance, Troubleshooting Local and Wide Areas Network (ISDN, Frame relay, DDR, NAT, DHCP, TCP/IP). Provided Technical support in terms of upgrading, improving and expanding the network. Providing technical security proposals, detailed RFP responses, security presentation, installing and configuring ASA firewalls, VPN networks and redesigning customer security architectures. Used Enterasys Dragon, Snort/Sourcefire, ISS Site Protector and Symantec Manhunt to detect, assess and report network intrusions Worked in a project of migrating environment to Cloud (AWS). Automated the task with PowerShell Script to download, Install SSL Certificate and Redirect HTTP to HTTPS to remediate the vulnerability. Configured Uptime Monitoring tool to monitor the Windows Services, IIS Websites, Windows Event Logs. Created Alert Profiles, Notification Groups, Action Profiles, and Service Monitors on single host and to multiple hosts to monitor the Windows Servers. Worked on Task Scheduler to Automate the installations of Software's and Security Tools. Installed Carbon Black and Bit 9 Security Tools on around 300+ window servers using the Task Scheduler in Group Policy. Fixed the issue in Installing LAPS Tool in Windows Server 2016 using Scheduled Task in Group Policy. Automated the Tasks of Uploading SQL Backup Files from Local Machine to S3 Bucket in AWS using PowerShell Scripting. Resolved the High, Medium, Low tickets raised by customers in Service Desk Manage Plus. Worked deeply In-Service Desk Manager Plus Ticketing tool to document the defects in SDMP. Created Change Request, Incident tickets with all levels of priority in Service Desk. Implemented Fine Grained Password Policy across all the domains to comply with the Security Compliance. Documented the Existing Group Policy Settings across 4 domains and compared with CIS Benchmark to remediate the vulnerabilities. Worked interactively in Various SOX Audit tasks to Pass the Audit. Documented the List of all SQL Jobs and Windows Scheduled Jobs which are related to SOX Audit and configured alerts to the jobs which are not monitored. Disabled the "SA" Account and deleted the existing windows accounts, Local SQL accounts and

added the Security Group to the SQL as a part of Audit Requirement and to overcome attacks by the hackers. Resolved the issue to login to SQL Server (Domain A) from Local Machine (Domain B) and documented the process for future reference in Wiki (Confluence). Experience in managing Microsoft Windows server infrastructure and data-Centre operations by effectively planning, installing, configuring and optimize the IT infrastructure to achieve high availability and performance.

Deployed Azure IaaS virtual machines (VMs) and Cloud services (PaaS role instances) into secure Vnets and subnets. Implemented operational efficiencies using scripting tools (PowerShell). Azure Cloud Infrastructure design and implementation utilizing ARM templates Created users and groups using IAM and assigned individual policies to each group. Creating Azure Backup vault and protecting required VMs to take the VM level backups. Involved in creation of virtual switches and configuration of NIC for a clustered environment. Disabled the TLS 1.0 Version and Enabled the TLS 1.2 Versions in all windows servers to remediate the vulnerability. Sr. Security Engineer ManTech International - Washington, DC April 2016 to August 2018 Responsibilities: Expertise in Cisco ASA 5525 firewalls with ACL security in a multi-VLAN environment. Implement and configured firewall rules in Checkpoint Gaia R77.20, R75, R70, VSX and Palo Alto Pa-500, Pa- 3000 series. Performed multiple firewall changes on the PIX, ASA, and Palo Alto firewall based on the requirements and monitored firewall changes using firemon Tool. Involved in importing the ASA rules to Palo Alto Networks Firewall rules using migration tool. Administered IDS / IPS to maximize network security, pushing and updating policies, and analyzing traffic. Worked extensively in configuring, Monitoring and Troubleshooting Check Point R77.XX Security appliance, Failover DMZ zoning & configuring VLANs / Routing / NATing with the firewalls as per the design. Implemented Zone Based Firewalling and Security Rules on the Palo Alto Firewall. Configuring and troubleshooting of Palo Alto, Juniper NetScreen & SRX Firewalls and their implementation. Configured network using routing protocols such as ISIS, RIP, OSPF, BGP and troubleshooting L2/L3 issues. Time to time upgrade network connectivity between branch office and regional office with multiple link paths and routers running HSRP, EIGRP in unequal cost load balancing to build resilient network. Design, implement and administer IPv4/IPv6 enterprise

network infrastructure utilizing Juniper routers. Responsible for supporting Palo Alto, ASA firewalls and Cisco Anyconnect VPN firewalls, utilizing Panorama centralized management and Cisco ASDM.

Built several Software Defined Networking (SDN) systems with Pica8 SDN switches and Controllers including ONOS. Co-ordinated with global Security Management teams and support teams as required and completed Palo Alto and Checkpoint Firewall rule add, modification, and delete. Planning, deploying, monitoring, and maintaining Amazon AWS cloud infrastructure consisting of multiple EC2 nodes and VMware Vm's as required in the environment. Responsible for adding Policies to the SRX 3600 Implemented Access lists and policy mapping on Juniper router installed in each branch across all the states. Verify feature changes and bug fixes done by developers and write test cases for all bugs, product changes and enhancements. Create separate test cases for the SourceFire product. Installed Juniper Firewalls, ISS /IPS, Snort intrusion detection with configurations. Configure and Troubleshoot Juniper Router (J2320) with IOS (JUNOS 9.3). Performed IP address planning, designing, installation, configuration, testing, maintenance, and troubleshooting in complete LAN, WAN development Configured Juniper routers for VRRP network routing redundancy. Migrated Cisco Secure ACS 4.2 for Windows to ACS 5.3. Staging of CRS-8/16, ASR9K/1K, Juniper/Cisco Firewalls, CMTS, Cisco 10K etc. Switching related tasks included configuring VTP for Inter-VLAN Routing, EtherChannel (LACP & PAgP) and RPVST for loop avoidance. Configure / Troubleshoot CISCO 12000, 7500, 3800 series router and 3560 series Switch for LAN/WAN connectivity. Actively involved in Switching technology Administration including creating and managing VLANS, Port security- 802.1x, Trunking 802.1Q, RPVST+, Inter-VLAN routing, and LAN security on Cisco Catalyst Switches 4507R+E, 6509-E and Cisco Nexus Switches 2232, 5596, 7009. Worked on configuration and commissioning of the MPLS circuits for various branch offices. Providing daily network support for national wide area network consisting of MPLS, VPN and point-to point site. Implemented Site-to Site IPSecVPN between two branch offices and also SSL VPN for user's connecting from various locations. Performed Network Security Assessment and implemented security improvements such as network filtering, SSH, AAA, SNMP access lists, VTY access lists, EIGRP MD5 authentication, and HSRP

authentication Established test environment for prototype PRL Project comprises of Solaris 2.5 Responsible for Data Center Migrations and its operations. Implemented antivirus and web filtering on Juniper SRX 240 at the web server Implementation and Configuration (Profiles, iRules) of F5 Big-IP LTM-6400 load balancers Provided Layer-3 redundancy by implementing HSRP and GLBP for High availability Worked in a project for shutting down one date center and migration of all Virtual Machines residing on Xen Racks to another data center. Installed Windows Servers using P2V console on top of Xen Racks as per business requirement. Configured Group Policy Objects to create a secure Windows Infrastructure. Provided third level help desk support for problems relating to Active Directory. Knowledge of DNS, Kerberos and Windows Authentication, to include authentication with other technologies for Single Sign-On. Good Experience in AD management including architecting Group policy, integration of multiple AD domains, AD-integrated DNS, AD operational level upgrades, AD migrations, AD object automation with scripting. Administered Splunk to collect the Memory and CPU utilization graphs for the past few months for the VM's. Deployed Packages from Altiris Configuration Manager to install the latest Microsoft updates. Installed the Graphical User Interface on all Core Windows Servers using the Power Shell and Vice Versa. Remediated the Critical Vulnerabilities for more than 3000 Virtual Machines including Windows and Linux Servers. Patched all the Operating System Critical updates in windows servers 2012, 2016 from the WSUS Server.. Resolved the High, Medium, Low tickets raised by customers in JIRA. Administered Microsoft Windows Servers (Active Directory), Microsoft Work Stations for 800 users. Had Experience with Cisco Jabber and Norton Slack for Communication Purpose. Migrated one disk of a VM to another LUN in the same cluster. Remediated around 1000 Vulnerabilities in all the windows servers to support the SLA. Building and hardening Windows Server 2008SP2, 2008R2, 201R2 environments on physical hardware. Pushed the updates from WSUS to all the window servers' clients to fix any OS related issues. Supported in fixing the memory utilization issue for application servers due to the crash of application. Supported in Decommissioning of the End of Life servers as they are no longer supported in organization. Senior Windows Admin Twenty Recruitment Group - New York, NY September 2014

to March 2016 Responsibilities: Installation of Windows servers 2008, 2008R2, 2012, 2012R2, 2016 Datacenter Versions with Activation tasks. Administered Microsoft Windows Servers (Active Directory), Microsoft Workstations,for 800 users. Deployed packages from SCCM configuration manager. Supported 800+ total users in 5 locations nationwide, as well as corporate office users. Upgraded 100+ ESX hosts from ESX 5.0 to ESX 6.x using VMware Update Manager tool. Design and Management of Public and Private cloud offerings providing IaaS/ SaaS/ PaaS using VCloud Director, Hyper-V. Provided planning, installing, configuring, and upgrading support for vRealize Automation & vRealize Orchestrator. Installed and/or upgraded VMware Tools on 8,000+ Servers including windows servers 2008,2012 and 2016. Installed CA workload Agent (ESP Agent) and Riverbed Steel Agent on more than 800 windows servers using SCCM and Manual Installation. Installed Remote Desktop Services Roles and Features and configured the license to RDS for all the windows servers. Managed Active Directory by creating new accounts, resetting passwords, unlocking accounts, adding users and GP. Remediated the Birthday Attack Sweet 32 vulnerability in windows servers. Disabled the TLS 1.0 Version and Enabled the TLS 1.2 Versions in all windows servers to remediate the vulnerability. Took Training on Zerto for migration of VM's from VMware to Hyper-V. Reconfiguring virtual machine resources like CPU, Memory and Disk space. Upgraded the CPU, Memory for more than10,000 VM's using vSphere Web client and Thin Client. Added/upgraded the new mount points in windows servers to increase the performance of SQL Server Applications. Upgraded and added the disks in Windows servers 2008, 2012, 2016 upon business requirement. Administered around 6 vCenter Servers and more than 150 ESXI servers. Worked on TSR (Technical Security Requirements) Remediation's for more than 10,000 Windows Servers. Updated the SSL Certificates on port 443. Performed Migration of Virtual Machines: vMotion and Storage Migration. Migrated the Virtual Machines from One host to another host, One cluster to another cluster. Performed the Swing Host Migration between two vCenter Servers. Deployed vRealize Operations Manager (VCOPs/VROPs), leveraging its capability for proactive monitoring of health of the entire virtual environment. Worked on VRealize Operations manager(VROPS) for monitoring the vcenter alerts. Creating and managing endpoints using Azure

Traffic Manager. Validation of HPE ProLiant iLO access to the physical servers and virtual servers running on VMware vSphere ESX/ESXi 5.5/6.x. Adding and Managing Co-Admins for all the subscriptions in the Windows Azure Platform. Updating the instance counts in the production in the Azure platform Administration of VMware ESX and ESXi Servers on HP Chassis 7000, DL380P GN8, BL 460C/Gen9. Performed ESXi Hosts and Virtual Machine migrations between Development, Integration and Production environments and across Datacenters. Hands on experience with configuring Cisco UCS. Build and release HPE ProLiant (DL/BL) physical and VMware virtual servers using Windows Server 2008R2/2012R2. Worked on ITIL/ITSM (Remedy, Viper), Incident Management, Change Management, Release Management, Problem Management, Task Management. Worked on Service Now ticketing tool, Created Incident, Change Request, Problem and Task Management in Service Now. Experienced in performing Cloning, Cold Migrations and Hot Migrations and taking Snapshots. Azure Cloud Administrator TracFone Wireless, Inc - Miami, FL March 2013 to August 2014 Responsibilities: Managing/Deploying the Windows Azure based applications. Infrastructure Migrations: Drive Operational efforts to migrate all legacy services to a fully Virtualized Infrastructure. Designed client server telemetry adopting latest monitoring techniques. Build of new environments for development and test in Azure. Experience in dealing with Windows Azure IaaS - Virtual Networks, Virtual Machines, Cloud Services, Resource Groups, Express Route, Traffic Manager, Site-to- Site VPN, Load Balancing, Application Gateways, Auto-Scaling. Designed and configured Azure Virtual Networks (VNets), Peering, subnets, Azure network settings, DHCP address blocks, DNS settings, security policies and routing. Established connection from Azure to On-premise datacenter using Azure Express Route and Site-to-Site for Single and Multi-Subscription. Developed a migration approach to move workloads from On-Premises AD to Windows Azure or develop new cloud-ready application solutions. Having Experience of Creating and Managing the users and groups in Azure AD. Deployed Azure IaaS virtual machines (VMs) and Cloud services (PaaS role instances) into secure VNets and subnets. Provided high availability for IaaS VMs and PaaS role instances for access from other services in the VNet with Azure Internal Load Balancer. Designed Network Security

Groups (NSGs) to control inbound and outbound access to network interfaces (NICs), VMs and subnets. Implemented HA deployment models with Azure Classic and Azure Resource Manager. Implemented operational efficiencies using scripting tools (Python and PowerShell). Designed database HA solutions using SQL 2014 AOAG, Mirroring and Replication to build the high availability solutions. Supporting for Enterprise customers on Microsoft Azure (IAAS, PAAS, SAAS). Protecting on Premise& Cloud Workloads using Azure Backup. Responsible for support Azure Resource Manager (ARM), Azure IaaS VM Backup & Hyper-V virtual machines. Managing/Deploying the Windows Azure based applications. Deployed Azure IaaS virtual machines (VMs) and Cloud services (PaaS role instances) into secure VNets and subnets. Implemented operational efficiencies using scripting tools (Python and PowerShell). Azure Cloud Infrastructure design and implementation utilizing ARM templates Created users and groups using IAM and assigned individual policies to each group. Creating Azure Backup vault and protecting required VMs to take the VM level backups. Developed a migration approach to move workloads from On-Premises to Windows Azure and develop new cloud-ready application solutions. Good exposure to Azure AAD and Azure App Proxy. Excellent work exposure to Azure AD PIM to work on users and their roles and privileges. Script, debug and automate PowerShell scripts to reduce manual administration tasks and cloud deployments. Configure Implement, Secure and support Virtual Network and best security practices for single and multi-regional data centers. Architect, develop and migrate servers, relational databases (SQL) &websites to Microsoft azure cloud. Deployed Azure Iaas virtual machines (VMs)& Cloud services (PaaS role instances) into secure VNets subnets. Designed Network Security Groups (NSGs) to control inbound and outbound access to network interfaces (NICs), VMs and subnets. Provided high availability for Iaas VMs and PaaS role instances for access from other services in the VNet with Azure Internal Load Balancer. Creating and Managing Virtual Machines in Windows Azure and setting up communication with the help of endpoints. System & Network Administrator CoStar Realty Information, Inc - Washington, DC August 2010 to February 2013 Responsibilities: Configured, Monitored and Maintained Virtual server farms consisting VMWARE and Hyper V. Assisted with VMware planning, consolidation

and upgrades Performed cost analysis supporting consolidation of physical servers into VMware Responsible for the planning, testing and implementation of server software patches and upgrades as scheduled. Implementing security restrictions to users, groups, computers, OUs using Group Policies (GPM) including GPO precedence, enforcing and blocking. Perform server hardening, join to domain and provisioning servers to application teams for validation. Troubleshooted the .net framework when the applications are not working. Creating local and roaming profiles, home folders, security and sharing permissions for folders and files. Configuring quotas, shared resources, implementing file screening, generating storage reports in FSRM. Creating shares under CIFS, providing permissions to shares and checking activity logs in the data domain network using EMC Data Domain System Manager. Worked on Active Directory, GPOs, DNS, DHCP, File & Print Server, IIS (Web Server), FTP,Terminal Server, WSUS, Microsoft Clustering. Experience with administration and oversight of GPOs and their relationship to OUs in a large multi-region environment. Proficiency with common Windows System administration and AD tools essential, scripting. Worked closely with Microsoft to identify risks and perform remediation involving domain health and future strategy (ADRaaS). Created/modified user account, security groups, and distribution list to protect company proprietary information. Managed Active Directory by creating new accounts, resetting passwords, unlocking accounts, adding users and GP. Supported Application and Development team in troubleshooting the issues related to windows servers and their applications. Worked with Forests and Domains; Restructuring a Forest and Renaming Domains as per company requirement. Maintains the Group Policy infrastructure based on the policies and guidelines provided to follow the Technical Security Requirements. Administered DHCP Server creation of reservation and under reservation options, configuring of router IP address. Involved in Monitoring and basic troubleshooting of storage devices. Created, developed, and tested preventative procedures and software to improve efficiency of overall Data Center operations. Collaborated with multiple support teams to resolve critical time-sensitive issues and responded to system emergencies. Performed troubleshooting of operating system and software infrastructure issues on Domain Controllers, Member Servers, Server Clusters, and

Virtual Machine Farms. Performed server incident root cause, service, and crash dump analysis. Handled user account transfers from one field site to another moving client data to different servers, to ensure user accessibility. Planned and executed on Active Directory computer migration to new forest. Troubleshooting BSOD, OS, RAM, CPU, Disk space, RDS, trust relationship, MS Office tools, Office Communicator 2007 R2, Windows services, network and storage issues in Windows environment. Remediated the Web Server Uses Plain Text Based Authentication. Renewed the SSL Expired Certificated to fix the vulnerability. Disabled the SSL V3 to protect the environment from attackers as SSL v3 uses the weak RC4 Cipher. Hands-on vSphere ESX/ESXi 4.x,5.x administration experience via vCenter and vSphere Web Client. Proficient creating new VMs and deploying guest OS, VMware Tools, also managing VMs using Cloning, Templates and Snapshots. Assist with implementing solutions for hardware and software. Implement common preventive maintenance practices for hardware and software Work with a highly secure environment using RSAT tools. Assist in management and support of internal and external DNS systems. Assist in management and support of internal DHCP architecture and scoping. Upgraded the windows client machines from windows 7 to windows 10 and Windows 10 to windows 10. Worked with CIS benchmarks to remediate the vulnerabilities and keep the environment safe. Configuring Windows Server roles and features like of Active Directory (ADDS), ADFS, DHCP, DNS, IIS, FSRM, DFS, .NET, etc. Hands-on experience administering AD users, computers, sites, replication, global catalog in a multi-site and multi-domain organization. Configuring DHCP scope, scope options, IP reservations, DHCP backup and failover in DHCP Server. Configuring host (A), alias, pointer (PTR) records, forward and reverse lookup zones in DNS. Implementing security restrictions to users, groups, computers, OUs using Group. Network Engineer Presidio Networked Solutions Group, LLC - King of Prussia, PA January 2008 to July 2010 Responsibilities: Administration of Xen Hypervisors on Xen Rack servers using Xen Center. Served as a senior system center configuration manager(SCCM) Administrator Created custom reports and collections using TSQL and WQL queries against the SCCM database for upper management and /or other business associates. Designed and supported Windows based servers using VMware, HP hardware and

blade center technology. Deploying, maintaining and troubleshooting Dell hardware M1000e Blade Chassis Rack mount servers (PowerEdge, iDRAC) Successfully remediated SCCM site and client issues regarding boundaries, replication, application deployment, patching, group policy and WMI using Configuration manager trace log tool. Provided Tier 3 support for issues in relation to all aspects of SCCM infrastructure including proper escalation, communication and management of production system problems. Creation of multiple delivery groups for corresponding departments within organizations. Installed and/or upgraded VMware Tools on 8,000+ Servers including windows servers 2008,2012 and 2016. Administered Altiris for Patching of Windows Servers and creation of VM's. Administered Solar windows patch management for addressing the vulnerabilities. Worked on OPSCON3 console for viewing the Virtual Machine's and Xen Hypervisors Configurations. Worked on Zabbix Monitoring tool to generate the Graphical Interpretation of RAM, CPU, Storage utilizations for the Virtual Machines residing on Xen Hypervisors. Performed cross platform audits of Active Directory (AD) objects and user permissions. Managed User Accounts on Windows NT and UNIX Platform (Creation, Deletion, Permissions, and VPN Access). Script, debug and automate PowerShell scripts to reduce manual administration tasks and cloud deployments. Experience with DCPROMO process and configuring AD Site, OU structure, Site Link, DNS, DHCP, WINS, Global Catalog servers, directory services, subnet mask, DNS forwarders, Reverse Lookup. Troubleshooting problems related to Active directory Database (NTDS.DIT replication, Capacity and Logging). Deployed Domain controller in Azure and joined to On-prem domain controllers. Provisioning Windows Operating systems and Applications on physical servers HP BL 460C G8, G9 and ensuring all Physical servers are updated with latest drivers and Firmware. Resolved all computer related problems, monitored and maintained system functionality and reliability by identifying ways to prevent system failures Performed replacements of failed hardware and upgraded software Performed scheduled Virus Checks & Updates on all Servers & Desktops Configured VLANS to isolate different departments Upgraded IOS on Cisco Catalyst Switches 2960 and 3560 to fix problems related with IOS bugs Upgrades and backups of Cisco routers and switches configuration files to a TFTP server Installed,

configured and maintained HP Servers, Enclosures and Server Blades such as HP BL460c G10, HP BL460c G9, HP BL380P G8, HP Blade Systems C7000 Enclosures. Performing tasks such as vMotion, SvMotion and EVC. Configured HA, DRS clusters, FT for important VM's. Performed functional testing of security solutions like RSA two factor authentication, Novel single sign on, DLP and SIEM. Worked on various business development activities like drafting response to RFP's and preparing SOW's documents. Acquainted with various approaches to Grey & Black box security testing. Proficient in understanding application level vulnerabilities like XSS, SQL Injection, CSRF, authentication bypass, cryptographic attacks, authentication flaws etc. Identifying the critical, High, Medium, Low vulnerabilities in the web applications based on OWASP Top10 and prioritizing them based on their criticality. Conducted security assessment of PKI Enabled Applications. Good knowledge on IBM Appscan to enhance the web application security. User ID reconciliation on quarterly basis. Update with the new hackings and latest vulnerabilities to ensure no such loopholes are present in the existing system. Threat modeling of the Project by involving before development and improving the security at the initial phase. STRIDE assessment of the applications during the design phase, identifying the threats possible and providing security requirements. Training the development team on the most common vulnerabilities and common code review issues and explaining the remediation. Developed organizational units in Active Directory (AD) and managed user security with group policies. Education Bachelor's Skills net (2 years), AJAX (Less than 1 year), ASE (Less than 1 year), AWS (2 years), BMC (Less than 1 year), C (Less than 1 year), Cracking (Less than 1 year), databases (1 year), DHTML (Less than 1 year), DNS (9 years), HTML (Less than 1 year), Java (Less than 1 year), JAVASCRIPT (Less than 1 year), Linux (2 years), Python (1 year), Scripting. (7 years), Security (10+ years), SIEM. (3 years), SQL (6 years), UNIX (2 years)

Name: Alexander Robinson

Email: samuel39@example.net

Phone: (250)933-2183