**Name: Raghavendran**

**SUMMARY:**

* Experience in System Administration, Maintenance, installation, configuration, trouble shooting and network security, and Privileged Access Management.
* Worked on Disaster Recovery Vault (DR) and CyberArk Enterprise vault.
* Good at understanding and communicate CyberArk's role in the privileged account security space.
* Developed and implemented processes and procedures for onboarding users and Privilege Accounts to CyberArk.
* Extensive experience in implementation and deployment of Privileged Account Security solution for Windows, UNIX, Database servers, Security, Networks and Websites.
* Integration of Event Notification Engine (ENE) & Service now ticketing system to CyberArk in PVWA.
* On-boarding of Privilege Accounts to Cyber-Ark, Configured Cyber-ark to MySQL, Oracle databases.
* Well experienced in CyberArk Administration and troubleshooting.
* Manage Identity Access management of Azure Subscriptions, Azure AD, Azure AD Application Proxy, Azure AD Connect, Azure AD Pass through Authentication.
* Having Experience Configuring and managing AzureAD Connect, AzureAD Connect health, Microsoft Azure Active Directory.
* Resolved Azure AD issues relating to Office 365, Active Directory to AzureAD and CAIDM to Active Directory.
* Good knowledge in Active Directory and managing Users, Groups, Computers, Organizational Units.
* Have good knowledge of network switches, routers, firewalls of market leading vendors and have in-depth knowledge of network protocols. Experience in Linux and Windows systems to provision new ids and find the RCA in system level and troubleshooting. Good knowledge on Shell script and windows PowerShell.
* Good analytical and communication skills and ability to work independently with minimal supervision and perform as part of a team.

**TECHNICAL SKILLS:**

|  |  |
| --- | --- |
| **Networking** | Conversant in LAN, WAN, Wi-Fi, DNS, WINS, DHCP, TCP/IP, ISCSI, Fiber, Firewalls/IPS/IDS |
| **Hardware** | Dell, HP, CISCO, IBM, SUN, CheckPoint, SonicWall, Barracuda Appliances, SOPHOS email appliances, Arcsight ESM, Arcsight Express, Logger, Connector |
| **Operating Systems** | Windows, NT, MS-DOS, Linux, Microsoft Windows 2008 R2/2008/2003/2000/2012 NOS family, Microsoft Active directory 2008/2003/2000, VMware ESX/ESXi server, Cisco ISO, RHEL 7.0 |
| **Application Servers** | DNS, DHCP, Windows Active Directory Services, FTP, SFTP, Microsoft Exchange 2003/2007/2010, Microsoft SharePoint 2007/2010, HP Ilo |
| **Infrastructure Hardware** | IBM, HP, Compaq, Dell desktops\laptops\servers, Cabling, Network printers, IP KVM Switches, Cisco Routers & Switches, 802.11x Wireless gateways, Access Points, Network UPS, Storage Area Network, NAS, iSCSI SAN |
| **Switching** | VLAN, VTP, STP, Inter VLAN routing & Multi-Layer Switching, Multicast operations, Layer 3 Switches, Ether channels, Transparent Bridging |
| **Protocols** | TCP/IP, L2TP, PPTP, IPsec, IKE, SSL, SSH, UDP, DHCP, DNS |
| **VPN** | ASA 5520, Cisco Concentrator 3030, Nortel Contivity Extranet 1500 |
| **Security Tools** | Wireshark, MBSA, MS Visio, Apache, VMWare ESXi 3.5, VMware Server, Encase, Symantec Endpoint Protection |

**PROFESSIONAL EXPERIENCE:**

**CyberArk Engineer-Anthem, Atlanta, GA (Jan-18 to Till Date)**

**Responsibilities:**

* Implementing & Managing Master Policy, Directory Mapping, LDAP integration, Platform and Safe via Private Ark client & PVWA.
* Installation and configuration of CyberArk Vault, Password Vault Web Access (PVWA), Central Password Manager (CPM) and Privileged Session Manager (PSM) in Prod.
* Troubleshooting and maintenance of the Password Vault, Central Password Manager (CPM), Privileged Session Manager (PSM), Application Identity Manager(AIM), DR Vault in DR Server.
* Perform as the subject matter expert for information security technology, processes and practices internally to the plan provided by the client. Providing access to shared drives and administrating the inactivity of the internal users through Active Directory.
* Privileged Access Management (PAM) project which includes implementing CyberArk Password Vault, Web Access, Central Password Manager and Privileged Session Management.
* Generating Inactive users report from Stealth Audit for further auditing and maintaining the data for Active Directory.
* Worked on EPM tools for improved operational efficiencies through an automated workflow approval and provisioning engine that integrates authorization and authentication.
* Experience in CyberArk Privileged Account Security product suite - Enterprise, Password Vault, Password Vault Web Access, Central Policy Manager, Privileged.
* Manage the day to day operations of CyberArk solutions including adding and deleting accts.
* Managing policies and platforms.
* Creating and assigning Safes, reconciling accounts, rotating passwords.
* Create AD users and groups for safe delegation and updates.
* Conduct workshops with application and infrastructure teams about on-boarding privileged accounts.
* Assist application teams with CyberArk application Identity Manager integrations and linked accounts.
* Deployment of Privileged Identity Management (PIM), LDAP directories, Privileged Access Management (PAM).
* Successfully established and tested Azure AD Tenant for production. Provided technical direction to allow Active Directory on-Prem group to populate users
* Experience in Syncing the Objects Users, Groups, Workstation from active directory to azure active directory.
* Resolved CyberArk issue's in CPM to communicate with a host to accommodate credentials.
* Troubleshooting and maintenance of the Password Vault, Central Password Manager (CPM), Privileged Session Manager (PSM), Application Identity Manager(AIM), DR Vault in DR Server.
* Worked on Endpoint Privilege Manager (EPM) tools to enforce endpoint least privilege across physical and virtual Windows and Mac endpoint, ensure security by revealing application and asset vulnerabilities before delegating privileges, elevate privileges to applications, not users, for complete control, automatically discover, manage and monitor privileged passwords, report on password, user and account behavior.
* Experienced in day to day operational support in adding and deleting accounts, applying policies, assigning safes, synchronizing failed accounts, Password rotations.

**System Network Engineer-Maximus, Dallas, Tx (Jan-17 to Dec-17)**

**Responsibilities:**

* Administration experience of Cyber Ark vault with Safe creation, integration with LDAP and other authentication methods.
* Worked on multi factor authentications in CyberArk using LDAP, PKI, RSA SecurID, RADIUS, and Oracle SSO.
* Experience with Application Identity Manger (AIM) which provides the solution to eliminate need of hard-coded credentials from application, scripts or configuration files.
* Coordinated LDAP combination with AD and system security group to open firewall ports.
* On-board privileged accounts and application ids with CyberArk Password upload utility or PVWA.
* Good experience in ticketing system like Service Now, SMTP, SIEM, NTP integration.
* Experience in performing Privileged Account Management with fair understanding the underlying business processes.
* Monitoring the Licenses for Azure Ad issues, resolving the Licenses Issue for Azure AD Users. Assigning the licenses Group based.
* Familiarity in the following areas: single sign-on, enterprise directory architecture and design, directory schema, namespace, replication topology, resource provisioning, role-based access Control, user lifecycle.
* Resolved Azure AD issues relating to Office 365(MMSSPP), Active Directory to AzureAD identity and user permissions.
* Knowledge on testing the application Various bethods and Deploy the application in to cloud.
* Configured and resolved Azure AD Connect sync issues,Various types of Data issues and Atrribute issues.
* Having Experience of Creating and Managing the users and groups in Azure AD.
* Configured platforms, master policies, created Safes & On-Boarded 1000's of Privileged Accounts, connection components, transparent components, access control through AD Group Nesting's
* Daily administration and maintenance of company's E-Directory
* Creation of policies and reports in PVWA.
* Administration experience of CyberArk vault with Safe creation, integration with LDAP and other authentication methods.
* Integrated with Active Directory (LDAP), 2 Factor Authentication (RADIUS).
* Defined, developed, and documented IDAM services including Single Sign-on, Self-Service registration, workflows, user management, management dashboard, Role Base Access Control (RBAC), Attribute Base Access Control (ABAC), resource and business layers Provisioning, credentialing, federation, and auditing.
* Involved in application to application credential management.
* Defined user account settings through Active Directory and used Active Directory to create, modify, and manage user, computers, and group account.
* Experience in performing Privileged Account Management with fair understanding the underlying business processes.
* Responsible for determining the target Privileged Session Management (PSM) audience. Determine what infrastructure and systems PSM will target (servers, virtual servers, database)
* Performed internal configuration of PSM to the vault itself.

**CyberArk Consultant-Ri-Out InfoTech, India (Dec-12-June-16)**

**Responsibilities:**

* Migration of current corporate infrastructure into CyberArk and previous pam solution (Xceedium).
* Configuration and customization of CyberArk system to fit corporate needs.
* Documentations for cyberark related pam infrastructure, processes, and troubleshooting knowledge base

specific for current corporate setup.

* Some scripting for admin duties and automating tasks leveraging PACLI (Private Ark CLI)
* Troubleshooting and maintenance of CyberArk systems.
* Day to day operational duties for CyberArk System and knowledge transfer of administrational duties.
* Separate company network in to different VLAN's using CISCO 3750, 2900 switches
* Execution, migration from VMware ESX to vSphere
* Plan, configure, and migrate to Microsoft Exchange 2010, Microsoft Exchange DAG
* Implementation of Microsoft DFS for company fileserver
* Design, test and implement Primary and Backup Domain Controllers
* Create Domain Forests, DHCP and Backup DHCP, create DNS, manage users and groups, as well as assign

rights and permissions.

* Assist in the scripting of AD user and contact object updates using PowerShell to facilitate synchronization to Azure AD.Havingexpericne with Various Powershell module (Azure ad, Active Directory and exchange online)
* Having Experience of troubleshooting of user account provisioning between legacy Client directories and CSC active directory and LDAP directories
* Experience Configuring and managing AzureAD Connect, AzureAD Connect health, Microsoft Azure Active Directory.
* Examine and develop group policy objects to automate user activity
* Manage and configure boot image files, and write Access Control Lists for security purposes
* Lead in configuring and managing VOIP phone system deployment for internal and external users
* Configure, deploy, maintain Blackberry Enterprise Server
* Install and maintain network availability, performance monitoring and notification systems
* Analyze, audit and implement network security and network threat protection
* Implement and maintain Sonicwall NSA 240, 2400, 3500, 5500, Sonicwall TZ200.
* Responsible for maintenance and addition of any Remote VPN client, and Site-to-SiteVPN Tunnel
* Install and configure several new Windows servers using Windows 2003 and 2008.