**Sreeja Immadi**

**imran@zelecloud.com**

**+1 910-593-2336‬**

**IAM/PAM | Senior Cyber Security Engineer| Information Security**

**Professional Summary:**

* Senior Cybersecurity Engineer with 10 years of experience in designing and implementing robust security solutions. Expertise in Data Loss Prevention (DLP), policy-based access control, and secure software development.
* Proven track record of optimizing security measures and ensuring compliance with industry regulations.
* Having knowledge on creating policies in conjur.
* Developed **Ping Federate.** Having Good exposure in integrating **CyberArk** Vault with Conjur.
* Experienced in **IAM/PAM** tools with deployment, configuration, integration and troubleshooting **CyberArk** Privileged Account Security product suite - Enterprise Password Vault, Password Vault Web Access, Central Policy Manager, Privileged Session Manager, Application Identity Manager, and Privileged Threat Analytics
* Experienced **Identity and Access Management (IAM) professional** with 2 years of expertise in implementing and managing privileged access solutions using Saviynt SecureONE and Just-in-Time (JIT) Access methodologies. Proven ability to secure critical systems, reduce attack surfaces, and ensure compliance with industry standards like SOX, GDPR, and HIPAA.
* Installed, configured, deployment, support and maintained of **SITEMINDER** components.
* Experience as a security professional in installing, managing, and monitoring of **CyberArk** Privileged account security tool modules. Part of **Privileged Access Management (PAM)** Remediation and Engineering team whose role is to secure Web Based applications on user access and authorization.
* Managed more than 25000 privilege accounts in **CyberArk** Vault.
* Managing Roles and Permission levels of Users Groups, Privileged Commands and resolving Incident on Access Issues.
* Having Knowledge on creating CPM Plugins to handle Password Management.
* Good experience in Deploying custom PSM Connectors using Auto IT script.
* Having good Understanding on AWS architecture.
* Coordinate with professional & technical development team leaders in defining technical goals.
* Involved in helping other teams to on-board their accounts, troubleshoot day to day issues and engage **CyberArk** Support team when required.
* Administration experience of **CyberArk** vault with Safe creation, integration with SIEM, LDAP and other **authentication**  methods.
* On boarding applications and configuration of privileged accounts in **CyberArk**.
* Administration of Service Accounts and Groups in **CyberArk**
* Manual Resets of accounts where CPM fails to reconcile within the given SLA.
* Creating proper safes before onboarding the accounts into PVWA
* Perform health check monitoring on all **CyberArk** severs to ensure consistent availability of system to end user.
* User Management in Active Directory (Account unlocking, password resets Active Directory)
* Onboarded Service Accounts and AWS Instances in Saviynt C**PAM**
* Created Access Visibility Controls in **CPAM** to restrict endpoints users based on User Entitlements.
* Having Knowledge on Saviynt **CPAM PAM** Config file.
* Creating Technical Rules in Saviynt and integrating connected applications.
* Good Knowledge on Incident Management (ITSM) like ServiceNow, JIRA.
* User ID creations and management and Administration of user accounts and groups on AD.
* Capable of handling the deliverables of a Team. and Implementation of Process within the Team.
* Sharing knowledge amongst the Team Members thus increasing the Overall Productivity.
* Knowledge of CPM/EPV/PSM Recorder for RDP connections and session.
* Experience in Troubleshooting production issues.
* Keep updates with password rotations, password malfunctions, account creations, account changes,
* maintaining/creating new safes, and **CyberArk** policies.
* Produced deliverables for client signoff such as PowerShell Scripts, installation plans, configuration plans, documentation.
* Developing Application instances and entitlements and Integrating New Application (Connected and disconnected) with OIM. Have good knowledge in troubleshooting various issues related to **CyberArk**.
* Good knowledge in Active Directory and Involved in AD integration and adding user to with their privileges. Identified and tested vulnerabilities and conducted research in the areas of information system and network security.

**Certifications:**

* **CyberArk** Defender certified.
* **CyberArk** Sentry certified.

**Technical Skills:**

|  |  |
| --- | --- |
| **Security tools** | **CyberArk** 7.x,8.x,9.x,10.x, CA Identity Manager 12.5.x/12.6.x,  Microsoft Active Directory, Saviynt SecureONE **PAM** ,Just-in-Time (JIT) |
| **Web & J2EE Technologies** | XML, HTML, **CyberArk**, OPM (On-demand Privileged Manager),  **PAM (Privileged Access Management).** |
| **Operating Systems** | Linux, Windows, UNIX AIX/HP-UX/ |
| **Network Protocols** | TCP/IP, HTTP, FTP, SNMP, and SMTP |
| **Web/App Servers** | Tomcat, Apache Web Server, WebSphere, WebLogic |
| **Databases** | Oracle, Microsoft SQL Server, MS Access, MySQL |

**Professional Experience:**

**Client: Walmart, Chicago, IL Jan 2023 – Present**

**Role: Senior Cyber Security Engineer**

**Responsibilities:**

* Designed and implemented DLP solutions, reduced data breaches over two years
* Collaborated in an Agile environment to deliver security features on time and within budget for 95% of projects
* Developed synthetic data generation tools for rigorous security control testing, improving test coverage
* Led the development and enhancement of Policy Enforcement Point, resulting in improvement in policy-based access control efficiency.
* Implemented advanced features for tracking test cases and logging requests, increasing system transparency
* Collaborated with cross-functional teams to ensure compliance with industry regulations, achieving 100% adherence to security standards
* Optimized tool performance, reducing response time and improved scalability to handle more concurrent requests
* Developed and implemented data mining techniques for various repositories, enhancing sensitive data identification accuracy by 50%
* Day-to-day activities include working with customer teams and supporting current tasks and activities.
* Integration of different on-premises application with Saviynt design and implement.
* Worked closely with customer's network and operations team to resolve issues or security concerns of tools/services.
* Produced deliverables for client signoff such as PowerShell Scripts, installation plans, configuration plans, documentation.
* Good knowledge on API calls using postman and PowerShell scripts.
* Automated Onboarding process using PowerShell.

**Client: GeekyAnts, India May 2019 – Dec 2023**

**Role: Senior CyberArk Engineer**

**Responsibilities:**

* Deployment of Privileged Identity Management (PIM), LDAP directories, **Privileged Access Management** (**PAM)**.
* Resolved **CyberArk** issues in CPM to communicate with a host to accommodate credentials.
* Troubleshoot and maintenance of the **Password Vault, Central Password Manager (CPM), Privileged Session Manager (PSM), Application Identity Manager (AIM), DR Vault in DR Server**.
* Experienced in day-to-day operational support in adding and deleting accounts, applying policies, assigning safes, synchronizing failed accounts, Password rotations.
* Administration experience of **CyberArk** vault with Safe creation, integration with LDAP and other **authentication** methods.
* Planned and upgraded the environment from **CyberArk** version 9.7 to 10.4 and 10.4 to 11.6.
* Perform the UNIT test for all the components of **CyberArk** to validate whether the upgrade is successful.
* Manage the identity and access management application and debug for system changes and updates.
* Assigned as **SITEMINDER** Engineer for upgradation, configuration, and deployments of CA **SITEMINDER** policy server and support **SITEMINDER** infrastructure.
* Design, develop, deploy, maintain, and administer Enterprise-wide application security using CA's SiteMinder, Oracle Access Manager, Oracle Identity Manager, and Ping Identity.
* Design and implement Single-Sing on between **SITEMINDER** and OAM integrated applications using Federation.
* Developed and Implemented **Oauth 2.0** with different Grant Types on **Ping Federate** acting as Authorization Server to support Web service based SSO and Mobile based apps.
* Managed client requirements and configured SailPoint IIQ connectors.
* Configuring the Applications (Authoritative and Non-Authoritative) using AD, Flat file, JDBC and LDAP connectors to load the Identity Cubes.
* Connector types used included: JDBC, AD/LDAP, Windows, Unix/Linux, Delimited File, Logical
* Designed and implemented custom solution for end users to request IdentityIQ capabilities following proper approval and auditing process. This feature is not available to end users by out of box.
* Recommended technical solution to fine tune performance in few of the out of box SailPoint component.
* Worked on multi factor **authentication** s 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-boarded privileged accounts and application ids with **CyberArk** using Password upload utility and manually from PVWA.
* Performed bulk upload using DNA, Account discovery, and Accounts feed.
* 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.
* On boarding windows, oracle database, mainframe, and Linux accounts.
* Worked on active Directory (AD) and group policy Management (GPO).

**Client: DXC, India Sep 2017 – Apr 2019**

**Role: CyberArk Engineer**

**Responsibilities:**

* Perform as the subject matter expert for information security technology, processes, and practices internally to the plan provided by the client.
* **Privileged Access Management** (**PAM)** project which includes implementing **CyberArk** Password Vault, Web Access, Central Password Manager and Privileged Session Management.
* 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, and Privileged Session Manager.
* Manage the day-to-day operations of **CyberArk** solutions including adding and deleting accounts.
* Managing policies and platforms.
* Worked with CI/CD pipeline for Ansible.
* 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.
* On-board privileged accounts and application ids with **CyberArk** upload utility or PVWA.
* Worked on Shared account privilege management (SAPM) like Windows, Unix etc.
* Ensure ongoing **CyberArk** system Maintenance is scheduled and completed on time.
* Design build and support processes on Windows Servers and Cyber Ark Security Platform. Providing support to Server owners on the security Servers.
* Ensure that all Identity and access management services are secure, available, and efficient and meet defined corporate services levels.
* Co-ordination with the offshore support teams to address technical or business requirements related queries.
* Involved in both Sever System analyzes and Security support on **CyberArk** as well as Support on Security on Windows servers.
* Monitoring logs, analyzing logs, and Troubleshooting issues with the server and the environment.
* Documenting the patterns for new configurations.
* Implemented **CyberArk** core component i.e., CPM, PSM, EPV, PVWA (9.3) in a new dev environment.
* Upgraded **CyberArk** version to 8.9 in production from 8.5.

**Client: Broad Ridge, India Jun 2015 – Aug 2017**

**Role: CyberArk Admin**

**Responsibilities:**

* Interacted with clients in gathering requirements, designed, and delivered solutions to install and integrate with the existing **CyberArk** implementations and managed high privileged accounts to automate Privileges Access Management process.
* Involved with Identity & Access Management Services on deployment, implementation and operations of Privileged Identity tool, **CyberArk**.
* Designed access control, user entitlements, application credentials, user access policy management, session management related to Privileged Access Management.
* Performed daily operations, support and defined access control, user entitlements, applications credentials, and user access policy management.
* Worked on Active Directory involving users, computers, groups, policies.
* Used SSIS transformations such as Lookup. Derived column. Data conversion, Aggregate, Conditional split, SQL task, Script task and Send Mail task etc.
* Worked with **CyberArk** components such as vaults, CPMs, accounts, policies, safes, usages, PACLI and providers.
* Installed & configured of components of **CyberArk**, like Vault, PVWA, PSM, AIM or CCP and Primary Vault, DR Vault, CPM, PVWAs, PSM, PTA, Secure Replicator, and Password Upload Utility.
* Worked on DR Drill.
* Diagnosed, isolate, debug problems, and perform problem resolution
* Defined Access Control, User Entitlements, Manage Applications Credentials, User Access Policy Management.
* Knowledge of security and systems standards, access management, authorization/ permissions management, network protocols, system management applications, and system & network security.
* Worked with account management on various platforms such a Windows, Unix, Active Directory, LDAP, SNMP monitoring, databases, and storage systems.
* Installed, configured, deployment, and maintained of **SITEMINDER** components like the Policy Server, Web Agent, Policy Store and Federation Security Services for SAML 2.0 implementation.
* Troubleshoot issues related to SSO, **authentication**  and authorization.
* Configured CA **SITEMINDER** System objects like Agents, Agent Conf Objects, Host Conf Objects, User Directories, Domains, Administrators and Schemas.
* Responsible for the replication, chaining, load balancing and other administration task.
* Involved with AD related Services including DNS, Group Management, Group Policy Management, Domain Trusts, and Kerberos.
* Involved in the areas of server log analysis and understanding of common analysis techniques and tools on Unix and Windows servers.
* Knowledge in AIM solutions to manage Windows and Linux application account passwords.
* Worked with Network Engineer's in the installation and configuration of firewalls.
* Knowledge of Scripting (VB script, PowerShell).

**Education:**

Completed Bachelor of Technology in Electronics and Communication Engineering from JNTU-H(2016) University.