**Chandra Shekhar**

**SUMMARY:**

* Over 10+ years of experience in, Privilege Identity and Access management solutions, in PAM, IAM, PAS, IDAAS and End Point Security Solutions using tools such as Thycotic Secrets Server Cloud, Thycotic Privilege Manger Cloud, CyberArk, AUTOIT, RADIUS, OKTA and on AWS Cloud, Azure MFA, SIEM, Azure Cloud, SASS, Qradar servers, SMTP, PASS, IAAS, Hybrid and On-Prem Solutions and integrating and Securing SASS Cloud solutions to Privilege Identity and Access management administration solutions.
* Administered full solution of CyberArk. Including pre-installation requisites, knowledge gathering, and implementation of a full CyberArk Solution.
* Administration of CyberArk Privileged Accounts and Vaulting services.
* Built Safes and added privileged accounts into the safes as needed.
* Provided troubleshooting and fixed all problems that arose in CyberArk due to ill-usage of the CyberArk from different users.
* Maintained and monitored integration with CyberArk module (AAM).
* Maintained PSM recording and checked the session recorded and the log.
* Maintained Privilege Vault Web Access (PVWA) for RDP/VPN users, security, and decryption.
* Creating & Managing Safes via Private Ark client & PVWA.
* Maintained Active Direction for Privilege Users, groups, and users.
* Bulk onboard Accounts in Vault using Password Upload Utility.
* Integrated Splunk with CyberArk to monitor Vault, PSM, CPM logs.
* Monitored configurations with Ldap and work on Secure AUTH.
* Integration of Secure AUTH Application accounts with CyberArk.
* Managing PAM’s Primary and Disaster Recovery Infrastructure.
* Defined access control and user access policy management according to company needs
* Developed project plan and the timeline for development of key deliverables
* Review company implementation of CyberArk and make recommendations for improvement based on industry best practices.
* Managing policies and platforms. Creating and assigning Safes, reconciling accounts, rotating passwords.
* On-boarding of Privileged accounts to CyberArk using the Password Upload Utility (PUU)
* Integration of CyberArk Conjur/Dynamic Access Protection.

**Technical Skills:**

|  |  |
| --- | --- |
| IDE/ Tools | Eclipse, Net Beans, Edit Plus, Macromedia Dreamweaver, XML SPY, JBuilder, RAD 7.0/6.0, WSAD, ITCAM, SIEM, Tivoli, RADIUS, UML (Rational Rose, RUP), VSS, CVS. |
| RDBMS | Microsoft SQL Server 2008/2012, |
| Platforms and Misc. | Microsoft Visual Studio 2008/2010/2012, Windows: XP /Vista / 7 / Server 2003/2008, Linux, HP Quality Centre, Azure MFA, Qradar servers, Active Directory, SMTP, ADCS, ADFS, SCCM. |
| Security Tools | IBM Identity Management and p6, CyberArk Privileged Account security 12.6, IBM Tivoli Access Manager 6.1.1, Tivoli Federated Identity Manager 6.2.2, Thycotic secret server 10.6.000027, Thycotic privilege Manager. |
| Operating Systems: | SUSE Linux 9/10/11, Windows Server 2000/2003/2008, Unix |
| Databases: | MSQL, MS Access, MySQL |
| Web Servers: | Sun One 4.1/5.1/6.1, Apache 2.0/2.2.4, IIS 5.0/6.0/6.5, Tomcat 4/5 |
| Directory Services (LDAP): | Novel eDirectory 8.7.x/8.8.1/8.8.5, Sun One/I Planet DS 5.x/6. x., eDirectory 8.X, Active directory (ADLDS), Tivoli Identity Management, Forefront Identity Manager, |

**EDUCATION:**

* Bachelors in Electronics and Communication Engineering JNTU, Hyderabad

**CERTIFICATIONS:**

* CyberArk trustee certification
* Cisco Certified Network Associate

**Professional experience:**

**Role: Sr. IAM/CyberArk Integration Analyst Mar 2023 to Till Date**

**Client: MUFG, Dallas, TX**

**Responsibilities:**

* Involved in Developing, Testing and evaluating Code Logics for Custom plugins like CISCO ISE, RADIUS, SIEM, SMTP, Viptela, Open gear, Azure MFA, AUTOIT, Qradar servers Hitachi and SQL using PACLI Scripting to get integrated to CyberArk and work efficiently.
* Implemented CyberArk Privileged Identity management suite and session management suite for version 12.6 .and ready to implement to version 13.0. Prime in providing problem resolution to authentication issues to PVWA and directory sync problems. Worked on Cyber Ark Enterprise Password Vault and PVWA Involved in application-to-application credential management.
* Privileged Access Management (PAM) project which includes implementing CyberArk Password Vault, Web Access, Central Password Manager and Privileged Session Management. Monitored Applications and WAS performance through Tivoli Performance Viewer and tuned the system caching, queuing, JVM parameters, DB Connection Pooling. Manage the day-to-day operations of CyberArk solutions including adding and deleting accts.
* Performed Manage, Resume, Release Privileged Credential using CyberArk Privileged Management Vault Administration, configuration, troubleshooting and installation of Windows 2003, 2008, 2008 R2, 2012,2016 worked on Configurations including AD integration and Management of CyberArk.
* Evaluated the clients existing security infrastructure by interviewing various technical leads from different departments and recommended CyberArk as the best fit for their current security needs.
* Successfully upgraded CyberArk PIM suite from v8 to v8.6, Worked with CyberArk utilities like password upload, PAR explicate, PACLI and PAR client. Installed and Configured IBM Web Sphere Application Server5.0 on Solaris. Installed, configured and administered Tivoli Access and Identity Manager. Automated Identity Management tasks such as user provisioning and application access based on each user’s role within our organization using Tivoli Identity Manager. Managing policies and platforms. Creating and assigning Safes, reconciling accounts, rotating passwords.
* Developed and implemented processes and procedures for Onboarding users and Privilege Accounts to CyberArk.
* Working with IT infrastructure teams to enhance the PAM (ePAM) solutions to integrate with other IT enterprise systems and support regulatory requirements. Responding to access control requests (on-boarding/new access, off-boarding/access removal, access changes, etc.).
* Developed scripts in bash and shell needed to automate the process in deployments, streamlining tasks during the storing of the data, used them during patch works and other day to day operations on servers. Apply application updates, patches, and configuration change, verifying the integrity and availability of the data and software.
* Developing maintainable/scalable, effective, defect free source code that meets business requirements and team standards. Documenting the steps/procedures to maintain backup for all the changes that take place, also providing as reference for the future.
* Performing initial log analysis and troubleshooting to identify cause of application issues/Root Cause Analysis, contacting support teams to triage bug report and guide the implementation of fixes. Involve in documentation after finding cause for the issues and troubleshooting, and the Documents include all new application functionality, including workflow diagrams, and assists in training Production Control.
* Performing UAT (user access testing), Identifying gaps in security architecture and recommend best practice processes and technologies. Preparing user compliance and validation reporting for process improvement, internal and external audits, and regulatory compliance.
* Understanding the issues from the security point of view or configuring on the application side, Involved Monitors and analyses day to day performance of assigned platforms to ensure required performance is maintained.
* Configured and maintained multi-factor authentication policies and procedures in CyberArk's Privileged Access Security solutions.
* Monitor request and ticket queues to ensure approved modifications are fulfilled in accordance with defined service level agreements, working with business and tech teams to ensure systems are configured to leverage the Privileged access management solution for access and account rotation

**Environment:** Thycotic Secret Server, Thycotic Privilege Manager, Azure, CyberArk 12.6 Web Agent QMR7 Password Reset Server, Account Lifecycle Manager, SailPoint IIQ 8.1p1/7.3p3, Hibernate, jQuery, MYSQL, Tomcat 6, Apache, XML., SailPoint INOW SaaS, PAM, SIEM, SMTP, RADIUS, Custom Connector, ServiceNow, Salesforce, Workday. Governance, OKTA, SSO, OpenID connect, Qradar servers, SAML2.0, Oauth2.0

**Role: IAM CyberArk Consultant Aug 2021 to Feb 2023**

**Client: LTI Infotech, Torrance, CA**

**Responsibilities:**

* The core day-to-day activity involved in design, implementation, and process documentation of a Privileged Account Management (PAM) solution IBM (Thycotic) Secret Server for a phased deployment in an enterprise environment and report directly to the lead PAM Architect but engaged with both project management and key client stakeholders to support customer success.
* Implemented Thycotic secret server and Thycotic privileged manager for version 10.6. Primarily in providing problem resolution to authentication issues to passwords and LDAP accounts and directory sync problems. Restricting privileged access within an existing Active Directory environment.
* Experience in Cyber-Ark Implementation and Installation on Cyber-Ark 10.6
* Installation, configuration, and maintenance of the Thycotic Secret Server PAM environment and responsible for documenting, designing, and administering the PAM infrastructure in alignment with the overall IT strategy.
* Responsible for the support of application integrations as required and Served as the subject matter expert (SME) for the Thycotic Secret Server PAM toolset.
* Provide overall direction and oversight into the PAM, SIEM functions across the organization, including Password Vaulting of elevated user and application service accounts.
* Assist application/business unit teams with privileged accounts on-boarding into Thycotic Secret Server.
* Develops and maintains PAM documentation including providing relevant training to team members.
* Responds to crisis or urgent situations to mitigate immediate and potential threats.
* Demonstrate an understanding of risk and change management, security policies and controls, user account life-cycle management and role-based access and experience with Windows Active Directory Administration.
* Configured SAML-based authentication and Identity Provider (IdP) settings within Azure Active Directory to enable SSO.
* Coordinate changes with members from Infrastructure along with external teams including IAM, DBAs, Network, Desktop, Application Support Teams, Qradar servers, Information Security. Perform other duties and/or special projects as assigned.
* Strong implementation knowledge, administration, and design knowledge of Privileged access management
* Automated user provisioning and de-provisioning processes in Splunk to streamline onboarding and offboarding of employees.
* Proposes system architecture and design standards / guidelines for new identity management service / PAM projects.
* Excellent documentation skills ensured HLD and detailed LLD's for every implementation, communication, and people skills. Discuss Business Applications with Business Owners with a focus on Access Control requirements.
* Discuss Applications with Application Owners with a focus on Access Control requirements.
* Agent installation and configurations and error resolution for the Thycotic Privilege manager
* Service account life cycle onboarding and issues related to lifecycle resolution in Thycotic Account Lifecycle manger.
* Configured user authentication, authorization, and single sign-on (SSO) capabilities within the Splunk platform.
* Local / Group level administrator access provisioning and deprovisioning
* Involved in initiation kickoff along with requirements gathering workshops, to start the project, set the expectations, review the timeline, understand the business use cases, and most importantly conduct a series of requirements gathering workshops. All this data was collected, along with the completed questionnaires, system analysis conducted and ad-hoc emails to clarify details are the basis for this design.
* Implemented and managed CyberArk SMTP, RADIUS, MFA solutions to enhance authentication security for privileged accounts.
* Developed and enforced security policies and procedures related to IAM within the Splunk environment.
* Created the solution deployment, high level design, and architecture documentation for the SailPoint IIQ solution. This document is intended for the project team members, and production support and operations personnel to provide sufficient details to understand what will be installed and configured.
* Implemented and maintained RBAC policies in Splunk to ensure that users have the appropriate level of access based on their roles and responsibilities.
* High level design document, this document describes the intent and the functionality to be delivered rather than presenting detailed configuration and/or installation and configuration steps. Detailed configuration was addressed in a subsequent update to this document which will transition it from a Design Document to an As-Built Document.
* Work with Offshore team and ensure seamless delivery of all PAM projects, participate in demand planning meetings, and drive the implementation based on business priorities.
* Excellent documentation, communication, and people skill

**Environment:** CA SiteMinder Policy Server v 6.0/12.51, CyberArk 10.6 Web Agent QMR7, Apache Web Server 2, CA Identity Minder 10.6.x, WebSphere 8.4, SIEM, OKTA, RSA, Azure MFA, RADIUS, SMTP, Oracle RDMS, Qradar servers, Korn shell scripting, Perl, XML, UNIX, Windows Active Directory.

**Role: IAM CyberArk Consultant Jan 2020-July 2021**

**Client: Iron Mountain, Dallas, TX**

**Responsibilities:**

* Implemented CyberArk Privileged Identity management suite and session management suite for version 9.7. Prime in providing problem resolution to authentication issues to PVWA and directory sync problems. Worked on Cyber Ark Enterprise Password Vault and PVWA Involved in application-to-application credential management.
* Experienced in day-to-day operational support in adding and deleting accounts, applying policies, assigning safes, synchronizing failed accounts, Password rotations. Managing, monitoring and Supporting systems hardware, software, and applications. Resolved CyberArk issues in CPM communicate with host to reconcile credentials
* Experience in Implementation, installation and maintenance of CyberArk 9.6 & 9.8 PIM Suite, Experience in implementing application account management by CyberArk on Windows, Azure MFA, Data bases and Linux servers using AIM module.
* Implemented Thycotic secret server and Thycotic privileged manager for version 10.6. Primarily in providing problem resolution to authentication issues to passwords and LDAP accounts and directory sync problems., restricting privileged access within an existing Active Directory environment.
* Administration experience of Cyber Ark vault with Safe creation, integration with LDAP and other authentication methods. Installed, managed and troubleshot DNS in multiple zone environments. Troubleshot DNS integration with Active Directory. Installed, configured and administered WINS, DHCP, IIS and WSFTP, SMTP, SIEM, File, Qradar servers and Print servers
* Provided technical support for CyberArk MFA and Azure SSO integration, addressing issues, and ensuring a smooth user experience.
* Ability to install, configure and support identity and access management related tools such CA SiteMinder, CA Identity Manager (IDM), and Oracle Internet Directory (OID). Created the Federation service between SiteMinder federated web services to Ping federate for classic migration of applications that are SAML and WS-FED based applications.
* Patching & Monitoring Vault, Central Password Manager, Two-factor authentication, Privileged Session Manager, Password Vault Web Access servers and services. Design build and support processes on Windows Servers and Cyber Ark Security Platform. Providing support to Server owners on the security Servers.
* Involved in gathering technical requirements and establish clear definition of clients CyberArk’s responsibilities and Maintenance. Experience in Implementation, installation and maintenance of CyberArk 9.5 PIM Suite. Primary point of contact for CyberArk Operational and Maintenance Tasks.

**Environment:** CyberArk 9.6 & 9.8 Web Agent QMR7, Apache Web Server 2, SMTP, CA Identity Minder 12.6.x, WebSphere 8.4, OKTA, RSA, Thycotic secret server 9.1.0, Oracle RDMS, RADIUS, Azure, Korn shell scripting, Perl, XML, UNIX, Windows Active Directory.

**Role: CyberArk Engineer Jan 2018 – Dec 2019**

**Client: Freddie Mac, McLean, Virginia**

**Responsibilities:**

* Responsible for optimizing the existing security infrastructure of our client and assist the Security Practice Architect in selection, design, architecture, automation enhancement, and best practices in regard to the Privilege Access Management products.
* Analyse and record how different people in the organization authenticate and authorize themselves to gain access to target systems.
* Experience in Cyber-Ark Implementation and Installation on Cyber-Ark 8.0
* Involved in Developing, Testing and evaluating Code Logics for Custom plugins like CISCO ISE, Viptela, Open gear, Hitachi and SQL using PACLI Scripting to get integrated to CyberArk and work efficiently
* Responsible for implementing, integrating, and engineering Privileged identity and access management solution for both privileged and standard users.
* Involved in scripting the commands for CP agents as a part of AAM solution for the most critical applications in the organization. PowerShell scripts and Linux commands are used successfully for AAM CP solutions
* Troubleshooting system and application accounts in a diverse systems/application architecture.
* Responsible for CPM configurations that supports remote password management and change on the following IIS Application Pools
* Involved in implementation of a range of Technical Security projects across CyberArk / Conjur where we have used Conjur SDK from a handful of client libraries to a complete OpenAI implementation.
* Involved in POC for AAM CCP integration to one of the internal applications.
* Involved in making calls through REST API
* Implemented Thycotic secret server and Thycotic privileged manager for version 8.14.0. Primarily in providing problem resolution to authentication issues to passwords and LDAP accounts and directory sync problems., restricting privileged access within an existing Active Directory environment.
* Responsible for password policy creation, password rotations, account creation, account changes, account integrations, maintaining/creating new safes, and PAM policies.
* Responsible for managing Enterprise Password Vault with respect to information/systems security and identity/access management.
* Evaluated the clients existing security infrastructure by interviewing various technical leads from different departments and recommended CyberArk as the best fit for their current security needs.
* Perform Risk Assessment and drive the closures of identified risks. Perform migration user accounts into Password Vault using Bulk upload utility.
* Responsible for providing end-user training on PAM infrastructure management.
* Following and maintaining in-house documentation for repeatable processes, including the implementation, patching and upgrading PAM components, disaster recovery, as well as change management processes.
* Provide best practice approaches for Onboarding privileged accounts for Privileged Access Management. Provide expertise in workflow, policy, and external integrations with Privileged Access Management tool.
* Worked on creating and changing the group policy of EPM server.
* Troubleshooting and maintenance of the Password Vault, Central Password Manager (CPM), Privileged Session Manager (PSM), Endpoint Privilege Manager (EPM), 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 behaviour.
* Be aware of emerging trends and best practices with the Identity Management, Privileged Access Management arena. Share and mentor this knowledge with the security team.
* Act as an escalation point for the security team and help remove barriers that prevent PAM policies and processes from moving forward. Integrated with Active Directory (LDAP), 2 Factor Authentication (RADIUS), Exchange (SMTP) & Splunk (SIEM) and Private Ark command line interface (PACLI).
* Experience in System Administration, Maintenance, Installation, Configuration, Trouble Shooting and Network Security, Privileged Access Management.
* 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.
* 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.

**Environment:** CyberArk, SMTP, Tivoli Identity Management Active Directory, Web agents 5.x/6x, IBM WebSphere Application Server 5.x/6.x/7.x/8.x, CA Wily 8.x, Thycotic secret server 8.14.0, J2EE, JDBC, XML, JBOSS 7, SAML 2.0, Sun ONE Directory Server 5.X/6.X, CA Identity Manager r8/r12, Apache 2.x, Ping Federate IIS 5.0/6.0, Solaris 8/9/10, Red hat Linux 5.x, Oracle 10g/11g, SQL Server 2005, DB2 8.X.

**Role: IAM/CyberArk Consultant Jan 2016 – Dec 2016**

**Client: TCS Technologies, India**

**Responsibilities:**

* Involved Installation on CyberArk component on various servers and Setup Privileged password management Policies for CPM component.
* Integrate LDAP/S, Active Directory, Radius, SSO authentication methods using CyberArk.
* OPM and AIM provider Installations on PSM and testing for Installation Qualification and Involved in AD integration and adding a user to with their privileges.
* Creating safes and adding users and groups to them for privileged access in CyberArk and Creation of policies and Reports in PVWA.
* Installation and configuration of CyberArk Private Ark client and Private Ark server and CPM, PVWA, PSM, PSMP, DR, good understanding of policies in CyberArk Central Policy Manager (CPM) and (PSM), Resolved CyberArk issues in CPM to communicate with a host to reconcile credentials, Prepared tickets about the issue and informed to the higher specialists.
* Alerting DXB Bank to suspicious activity or instances observed on their networks, such as DDoS attempts, Cross-Site Scripting, or malware infections, then providing recommendations and solutions to handle them.
* Provided guidance in adding, removing, change and lifecycle of Privileged Identity Management (PIM) in order to provide the highest quality levels of Security.
* Retrieved CyberArk system and application password's and assist Database, Linux, and Core Application Support teams when passwords are needed.
* Good knowledge in Active Directory and Involved in AD integration and adding user to with their privileges, monitoring the servers and making servers up and down as required.
* Running ant scripts for automation of moving files from one server to server.
* Taking backups of files and directories and changing permissions to directories and files.
* Creating Users.

**Environment:** NetIQ Access Manager 3.2/4.2/4.3, Ping Federate 7/8, RSA, MS SQL 2005/2008, Active Directory, iManager 2.7, Windows 2012 and Windows 7, JSP.

**Role: IT Security/Analyst/CyberArk June 2013 -Dec2015**

**Client:YIT SOL Technologies, India**

**Responsibilities:**

* On PAM project Implementation team, supported designing PAM Solution in the environment.
* Responsible for Monitoring and enforcing information security program and policies.
* Prepare project activities and work packages in regard to PAM implementation and tracking operating and/or product changes.
* Worked on creating the Identity access to the employees and managing the certifications and provisioning accordingly with the Sail point IdentityIQ.
* CyberArk Upgrade, PAM CyberArk Implementation, SOC/SIEM Replacement Project (FireEye), IAM Implementation.
* Identified Security Target and Target of Evaluation using CyberArk Privileged Account Security Solution v9.1
* Scripted mass policy, target application and ID creation in CA PAM, reducing initial rollout time. Also held virtual workshops and training sessions which ensured CA PAM user productivity and acceptance globally.
* Worked closely with CA PAM product support team providing feedback on defects and improving user experience.
* Managed CyberArk PAS to enable company to secure, provision and monitor all the activities associated with enterprise systems and applications.
* Serve as the primary point of contact on CyberArk implementation, maintenance, management and Pilot programs between the client and CyberArk.
* Conducts briefings with Fortune 500 C-Suite executives for unstructured data security, identity access management, privileged access management and advisory services.
* 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.
* Integrated with Active Directory (LDAP), 2 Factor Authentication (RADIUS), Exchange (SMTP) & Splunk (SIEM) and Private Ark command line interface (PACLI).
* Have good Experience with PAM suite components installation and implementation.
* Delivered identified privileged accounts into the CyberArk management solution.
* Included Onboarding of privileged User IDs into CyberArk from UNIX, Linux and Windows systems.
* Assisted in and perform the day-day activities related to CyberArk including the development, testing and roll-out phase activities of the implementation.
* Implementation and installation of Cyber Ark 6.0 and latest implementation of Cyber-Ark 6.0.1 and CyberArk 6.0.2
* Address Audit & Compliance remediation with enterprise projects (Ex. O365, Multi-Factor Authentication, CyberArk Implementation etc.)
* Privileged Access Management of CyberArk, including working with components such as vaults, CPMs, accounts, policies, safes, usages, PACLI and providers.

**Environment:** Cyber Ark 6.0 PIM, LDAD, AD Integration, UNIX, Firewall, IDS/IPS, SIEM, IIS, IBM HTTP SERVER, PVWA, PSM, AIM or CCP, CPM, PTA ACS, DNS, TCP/IP, Security, VB script, Powershell.