**A close up of a sign

Description automatically generatedHari Reddy**

**Email:** [**hari.cbark@gmail.com**](mailto:hari.cbark@gmail.com)

**Ph No: 510-925-3696**

**Professional Summary:**

* 9+ years of IT experience including **System Administration, Maintenance, installation, configuration, trouble shooting and network security, database systems, and Privileged Access Management.**
* **Experienced in PAM** deployment, configuration, integration and troubleshooting of **CyberArk Privileged Account Security (PAS) product suite - Enterprise Password Vault, Password Vault Web Access, Central Policy Manager, Privileged Session Manager, Application Identity Manager, Privileged Threat Analytics.**
* Experienced in CyberArk installation, upgrade and implementation of **CyberArk version 9.x, 10.x, 11.x, 12.x** and **13.x.**
* 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, CPM, PVWA, PSM, PSMP, DR Vault, AAM and EPM.**
* Worked on **AWS cloud** services like **EC2, S3 Bucket, Cloud Formation Templates (CFT), IAM Roles** etc. and deployed CyberArk components on AWS instances.
* Performed Manage, Release Privileged Credential using Cyber Ark Privileged Management **Vault Administration, configuration, troubleshooting** and installation of **Windows 2008, 2012 R2**, **2016**, **AD and LDAP.**
* Experienced with PAM Operational Tasks - defining **access control,** user entitlements, **manage applications, credentials,** and user access policy management.
* Good analytical and **communication skills** and ability to work independently with minimal supervision and perform as part of a team.

**Certifications:**

* **CyberArk Defender**
* **CyberArk Sentry**

**Professional Experience:**

**U.S. Bank, Irving TX June 2023 – till date**

**Sr. CyberArk Engineer**

**Responsibilities:**

* Conducted quarterly resiliency exercises to test failover capabilities between the primary master vault and candidate vault.
* Managed PVWA vulnerability patching and upgraded Vault and component servers from version **12.2.10** to **12.6.12**.
* Upgraded the vault and components from 12.2 to 12.6
* Handled **ServiceNow** tickets, incidents, and change requests, providing Level 4 support for complex technical issues.
* Participated in weekly **on-call rotations** to ensure application support after business hours, minimizing potential impact.
* Worked closely with end users to onboard their applications to CyberArk as part of audit-related initiatives.
* Led remediation efforts for failed accounts and generated detailed weekly and monthly metrics reports.
* Upgraded and migrated PSM components from version **12.x to 14.x**, to remediate vulnerabilities related to patch.
* Worked on **EPM** and implemented least privilege policies and configured privilege elevation rules using **CyberArk EPM** to secure endpoints, reducing the risk of unauthorized access and ensuring compliance with security best practices.

**Capital One, Plano TX May 2021 – June 2023**

**Sr. CyberArk Engineer**

**Responsibilities:**

* Worked on various components of **CyberArk** PAS Solution that **Vault, PSM, CPM, PVWA, PSM SSH Proxy (PSMP) and Application Access Manager (AAM).**
* Implemented installation, upgrade, and maintenance of **CyberArk 12.2.4 and 11.4 PIM Suite.**
* Involved in designing and implementation of end-to-end security solutions using different security products.
* Worked on Service now tickets, Incidents and change requests.
* Coordinated with CyberArk support teams for escalation and resolution issues.
* Worked as **level 3** support to assist end users and resolve the issues, tickets regarding access issues, password failures, account issues etc. and on-boarding new **Windows, Linux, database, network devices and AD domain accounts.**
* Worked on vaulting database accounts (**Oracle, SQL, Postgres) Unix accounts** and Windows accounts and worked on account remediation effort for accounts to comply with enterprise password policy.
* Worked on **audit requests** and provided the required reports, data to internal and external audit teams
* Created Windows, Linux instances on **AWS cloud** using **CFT’s** and automated installation of components using silent installation by integrating **PowerShell** scripts in the CFT’s using **S3** Bucket.
* Create and manage **Safes** and onboard privileged accounts to EPV.

**Manulife, Boston MA Nov 2020 – May 2021**

**CyberArk Engineer**

**Responsibilities:**

* Involved in CyberArk **PAS** implementation that includes components **Vault, PSM, CPM, PVWA, PSM SSH Proxy (PSMP) and Application Access Manager (AAM).**
* Worked on service now tickets for safe creation and accounts onboarding to the vault.
* Worked on vaulting various types of credentials like **Windows Accounts, Linux Accounts, Database accounts** and other cloud-based credentials.
* Worked on **AAM** implementation of **Credential Provider** and enabled secured authentication mechanisms with **Path, OS user, Hash authentication**.
* Implement **Central Credential Provider** for retrieving the credentials of application service accounts using RestApi call.

Used CyberArk Restful web services (REST Api) for various CyberArk related tasks for automating day to day activities.

* Managed safes and Server/ host addresses in EPV. Resolved issues with CyberArk's CPM to communicate with hosts to reconcile credentials.
* Responsible for **PAM Operational tasks** defining **access control**, **user entitlements, managing applications credentials and user access policy.**

**Capital One, Plano TX Apr 2018 – Oct 2020**

**CyberArk Consultant**

**Responsibilities:**

* Implemented installation, upgrade, and maintenance of **CyberArk 10.2, 10.3, 10.5 and 10.8, 11.1 and 11.4 PIM Suite.**
* Coordinated with support teams for escalation and resolution of issues.
* Worked as **level 3** support to assist end users and resolve the issues, tickets regarding access issues, password failures, account issues etc. and on-boarding new **Windows, Linux, database, network devices and AD domain accounts.**
* Worked on vaulting database accounts (**Oracle, SQL, Postgres) Unix accounts** and Windows accounts and worked on account remediation effort for accounts to comply with enterprise password policy.
* Worked on **audit requests** and provided the required reports, data to internal and external audit teams
* Implemented **multi factor authentication (MFA)**using **RADIUS** to ensure that the only authorized users can access their privileged accounts.
* Implemented **SAML** authentication for integrating CyberArk with **Ping Federate** for MFA authentication and coordinated with SSO team.
* Implemented **PTA** POC and coordinated with the team and documented the steps
* Uploaded multiple password objects to the vault using **Password Upload Utility**.
* Developed scripts to generate various reports as per organizational needs using PowerShell, **PACLI, AIM, Export Vault Data (EVD) utility.**
* Worked on Audit requests and provided requested evidence to the auditing teams.

**MBFS, Farmington Hills, MI Jul 2016 – Mar 2018**

**CyberArk Consultant**

**Responsibilities:**

* Experience in Implementation, installation, and maintenance of **CyberArk 8.x, 9.x PIM Suite**
* Experience in **CyberArk PAS suite** which includes **Enterprise Password Vault, Password Vault Web Access, Central Policy Manager, Privileged Session Manager, Proxy and PACLI.**
* Worked on Privileged **Access Reviews, Compliance Reporting, Access Control** Processes**,** and other associated tasks with **Privileged User Management.**
* Creating safes and adding users and groups to them for privileged access in CyberArk
* Administration of **User accounts, Group memberships** and **Organizational Units** using Active Directory. Installation, configuration and troubleshooting of **AIM clients** for various teams.
* Worked on Application Identity manager to securely facilitate access to privileged passwords in applications or configuration files. Lead offshore team about day-to-day operations.
* Troubleshooting and maintenance of **the Password Vault, CPM, PSM, AIM and DR Vault**
* Migrated user accounts into **Password Vault** using Bulk upload utility.
* Knowledge in **Active Directory** mapping connection to provision users and groups into Cyber-Ark vault and e-mail notification failures
* Good Experience in working with Ticketing system **(Service Now)** and Log Management Tool **(Splunk).**
* Monitor **CyberArk** reports and respond to failed password verification alerts and work with system account owners to resolve failure alerts.
* Ensure that all **CyberArk** accounts communicate with Servers and correct any discrepancies or errors that are found.

**MNIT Services, St. Paul, MN Mar 2015 – Jun 2016**

**System Administrator**

**Responsibilities:**

* Planned and assessed the integration of new technical requirements with existing processes and skills.
* Collaborated with management to define and map business processes during the Scope and Blueprint phases.
* Created targeted questionnaires for SMEs and performed thorough requirement and gap analyses.
* Developed Technical and Functional Requirements from BRDs and produced Functional Specifications Documents.
* Participated in software testing and worked with QA Analysts to identify and resolve bugs.

**Education:**

MS (Computer Science) from NPU California (Sept 2013 – Dec 2014)