A PROJECT ON

CYBERARK IN CYBERSECURITY

Submitted in partial fulfillment of the requirement for the award of the degree of

BACHELOR OF TECHNOLOGY

IN

COMPUTER SCIENCE & ENGINEERING

Submitted by:

Pranjal Saxena   **2019576**

Under the Guidance of

Mr. Akshay Rajput

Associate Professor

Department of Computer Science and Engineering

Graphic Era (Deemed to be University)

Dehradun, Uttarakhand

June-2025

CANDIDATE'S DECLARATION

I hereby certify that the work which is being presented in the Project Report entitled **"CyberArk in Cybersecurity"** in partial fulfillment of the requirements for the award of the Degree of Bachelor of Technology in Computer Science and Engineering and submitted in the Department of Computer Science and Engineering of the Graphic Era (Deemed to be University), Dehradun is an authentic record of my own work carried out during a period from **February-2025 to June-2025** under the supervision of **Mr. Akshay Rajput, Associate Director.**

The matter presented in this dissertation has been submitted by me for the award of Internship at Cognizant.

Pranjal Saxena   2019576

This is to certify that the above statement made by the candidate is correct to the best of our knowledge.

Supervisor   **Head of the Department**

External Viva

Name of the Examiners: **Signature with Date**

1.

2.

CyberArk **University**

Pranjal Saxena

has successfully completed the course
**CyberArk (PAM) Install and Configure
for Partners**

CPE \ Hours: 32.00

Date: 10, May 2025

CYBERARK

CyberArk **University**

Pranjal Saxena

has successfully completed the course
**Privileged Access Management (PAM)
Administration for Partners**

CPE \ Hours: 32.00

Date: 09, May 2025

CYBERARK

Abstract

The modern era of cyber security has transformed the protection of privileged accounts into a critical component of a company's security framework. Attackers who attempt to compromise a network or destroy infrastructure often take aim at high value targets that are associated with special accounts which provide more extensive privileges and access to critical systems. CyberArk has earned worldwide recognition as a market leader in privileged access management (PAM). It provides a complete platform for safeguarding, controlling, and managing privileged access within on-premises, cloud, and hybrid environments.

This project focuses on the design and operations of CyberArk with special attention to its core components Digital Safe, Password Vault Web Access (PVWA), Central Policy Manager (CPM), and Privileged Session Manager (PSM). SAFE is a secure repository for registration information, whereas PVWA is a web-based management console that offers controlled access through an ergonomic interface. CPM ensures compliance through the optimization of password rotation and the implementation of guidelines. PSM enables corporates to conduct privileged meetings without exposing the registration details of the end-users to obtain nominal control over the registration information.

This enhancement in the exercise of responsibility diminishes abuse potential. With the level of cyberattacks we have witnessed so far, having a comprehensive PAM solution, like CyberArk, is not just good to have, but rather essential.

Keywords:
- CyberArk
- Privileged Access Management
- Identity Security
- Credential Vault
- Session Monitoring

Acknowledgement

Any achievement, being scholastic or otherwise does not depend solely on the individual effort but on the guidance, encouragement and co-operation of intellectuals, elderly and friends. A few personalities in their own capacity have helped me in carrying out this project work.

Our sincere thanks to project guide **Mr. Akshay Rajput, Associate Professor** and trainer **Vinoth PalaniSwami, Associate Director – Projects Cybersecurity IDAM - Cognizant,** for his valuable guidance and support throughout the course of project work and for being a constant source of inspiration.

We extend our thanks to **Dr. Deepak Gaur**, Project coordinator, Department of Computer Science and Engineering, Graphic Era (Deemed to be University), for his valuable suggestions throughout all the phases of the Project Work.

We are extremely grateful to **Prof. (Dr.) D. P. Singh**, HOD of the Computer Science and Engineering Department, Graphic Era (Deemed to be University), for his moral support and encouragement.

We thank the **management of Graphic Era (Deemed to be University)** for the support throughout the course of our Bachelor's Degree and for all the facilities they have provided.

Last, but certainly not least, we thank all teaching and non-teaching staff of the Graphic Era (Deemed to be University) for guiding us in the right path. Most importantly we wish to thank our parents for their support and encouragement.

Pranjal Saxena   2019576

Table of Contents

List of Figures

Chapter 1

Introduction

In the following sections, a brief introduction and the problem statement for the work have been included.

1.1 Project Introduction

As industries undergo rapid digital transformation, they increasingly depend on intricate IT ecosystems to manage their daily operations, communication channels, and data repositories. While this digital dependency brings operational advantages, it also introduces heightened cybersecurity risks—chief among them being unauthorized access to critical information and infrastructure. A particularly vulnerable point within these systems is the presence of privileged accounts, which offer elevated access rights. When exploited or misused, these accounts can cause massive data leaks, system failures, and damage to an organization's reputation.

To mitigate such threats, CyberArk delivers a focused solution through its Privileged Access Management (PAM) platform. This system is designed to secure, track, and control privileged credentials and access used by IT administrators, system services, applications, and automated processes.
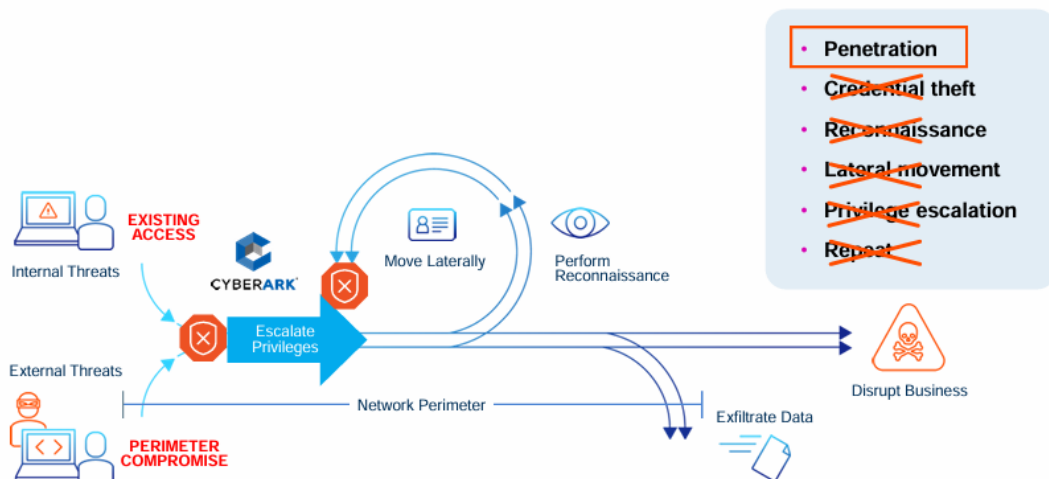

Fig. 1.1 CyberArk Prevents Attack Chain

This project aims to examine the core components, architectural design, and real-world implementations of CyberArk. It outlines how CyberArk enhances security by encrypting and safeguarding credentials, automating password updates, observing privileged sessions in real time, and flagging suspicious activities. Tools like the Digital Vault, Password Vault Web Access (PVWA), Central Policy Manager (CPM), and Privileged Session Manager (PSM) collectively help ensure strict access control and regulatory adherence.

With the increasing frequency of cyberattacks that exploit privileged access points, the need for a comprehensive PAM solution like CyberArk becomes urgent. CyberArk plays a key role in enforcing the principle of least privilege, ensuring that users can only access the systems they truly need.

Additionally, this report delves into how CyberArk is deployed, configured, and integrated into existing security frameworks, as well as how it aligns with zero-trust security models. Ultimately, the study demonstrates how organizations can leverage CyberArk to create a secure, resilient, and compliance-ready digital environment.[1]

1.2 Problem Statement

As modern enterprises continue to expand their digital footprint, securing sensitive systems and data has become increasingly complex. The widespread adoption of cloud platforms, hybrid work environments, and diverse IT infrastructures has led to a dramatic rise in the number of privileged accounts across organizations. These accounts, often used by system administrators, software services, or automated scripts, have elevated permissions that can bypass standard security restrictions. If these accounts are exploited, the attacker gains near-complete control over the organization's critical assets.

Many businesses continue to manage these privileged accounts manually, often relying on spreadsheets or static credentials shared among teams. This lack of centralized control and accountability significantly increases the risk of unauthorized access. Additionally, it becomes difficult to monitor activities tied to these accounts, making it harder to respond to incidents or prove compliance with regulatory standards such as HIPAA, GDPR, and PCI-DSS.

Cyber attackers have grown more sophisticated, frequently targeting privileged credentials in the initial stages of an attack to move laterally within networks, deploy malware, or exfiltrate data. Traditional cybersecurity solutions—like antivirus software or firewalls— are not designed to handle the complexities of privileged access threats. Without a dedicated solution to secure, monitor, and manage privileged accounts, organizations leave themselves exposed to internal misuse and external threats.

This project addresses the urgent need for a Privileged Access Management (PAM) strategy by exploring CyberArk's capabilities. It identifies key challenges that organizations face, including:

- Lack of automated control over privileged credentials.
- Inability to track and audit privileged activities in real time.
- Increased risk of insider threats and compromised credentials.
- Difficulty in enforcing the principle of least privilege.
- Gaps in compliance and reporting due to insufficient access control mechanisms.

By implementing CyberArk, organizations can centralize credential storage, automate password rotation, restrict access to critical resources, and actively monitor privileged sessions. This project will study how CyberArk fills the security gaps that exist in conventional identity and access management (IAM) systems, helping companies prevent privilege abuse, reduce the attack surface, and achieve regulatory compliance.

1.3 Objectives

The central goal of this project is to explore CyberArk as a leading solution in the field of Privileged Access Management (PAM) and evaluate its role in strengthening an organization's cybersecurity framework. The specific objectives include:

1. **To identify the security challenges posed by privileged accounts** in diverse IT environments and the risks associated with their mismanagement.
2. **To understand the architecture of CyberArk**, including its core components such as the Digital Vault, PVWA (Password Vault Web Access), CPM (Central Policy Manager), PSM (Privileged Session Manager), and PTA (Privileged Threat Analytics).

3. **To demonstrate how CyberArk securely stores, rotates, and manages passwords** and credentials used by privileged accounts, applications, and services.
4. **To evaluate how session monitoring and access auditing** features help detect suspicious behavior and enforce accountability.
5. **To assess CyberArk's compliance capabilities**, especially its alignment with global data protection laws and industry regulations.
6. **To simulate deployment and integration of CyberArk** within an enterprise IT environment and highlight best practices for configuration.
7. **To study the role of CyberArk in a Zero Trust Security model** and how it supports broader security strategies through integration with SIEMs and IAM systems.

By fulfilling these objectives, the project will offer a practical understanding of how organizations can use CyberArk to mitigate identity-related threats, reduce the risk of insider attacks, and create a secure digital infrastructure.

Chapter 2
Literature Survey/ Background

In recent years, the increase in cyber threats has significantly impacted how organizations manage access to their IT resources. Studies and industry reports consistently highlight that **privileged accounts** are one of the most exploited vectors in successful cyberattacks. These accounts—used by system administrators, services, and applications—grant elevated access to critical systems, making them prime targets for attackers. According to research from Verizon's Data Breach Investigations Report, a large portion of data breaches involve the misuse of privileged credentials.

The concept of **Privileged Access Management (PAM)** has evolved in response to these risks. Initially, organizations relied on basic password vaulting solutions to store and share credentials. However, as threats became more sophisticated, the need for more advanced systems that could offer real-time monitoring, automatic credential rotation, and access control became clear. This is where PAM platforms like CyberArk gained prominence.

CyberArk stands out as a dedicated PAM solution developed to secure privileged accounts across on-premises, cloud, and hybrid environments. Literature in cybersecurity journals, white papers, and industry evaluations consistently recognize CyberArk's effectiveness in reducing internal threats and preventing external breaches. Researchers have emphasized its ability to automate password management, track privileged user activity, and integrate with other security systems to provide a multi-layered defence.

Additionally, various case studies published by enterprises that have implemented CyberArk highlight significant improvements in audit readiness, reduced incidents of credential abuse, and streamlined compliance with frameworks such as GDPR, HIPAA, and SOX. Academic research also supports the integration of PAM into a **Zero Trust Architecture**, where no entity—whether inside or outside the network—is automatically trusted.

In conclusion, the literature confirms that managing privileged access is a fundamental requirement for securing modern IT infrastructures. CyberArk's contributions in this domain are widely acknowledged, making it a key technology in the broader field of identity and access management. This background provides the foundation for exploring CyberArk's real-world application in organizational security strategies.

In addition to securing traditional IT environments, modern PAM solutions like CyberArk are being increasingly utilized in DevOps and cloud-native ecosystems, where rapid deployment and automation are essential. Literature from cloud security experts points out that unmanaged secrets—such as API keys, SSH keys, and cloud credentials—often pose a major threat in CI/CD pipelines. CyberArk's **Secrets Manager** component is designed to manage and rotate these credentials securely, thereby minimizing the attack surface and maintaining security without hindering developer productivity.

Furthermore, research highlights the **growing threat landscape involving insider threats and advanced persistent threats (APTs)**. Unlike external attackers, insiders already possess a level of trust and access, making their actions harder to detect. CyberArk helps in addressing this challenge through its **continuous session recording, access analytics, and real-time alerting** features, which together enhance visibility and control over all privileged activities. Academic publications and industry evaluations continue to recommend CyberArk as a key part of a layered defence strategy, ensuring both proactive threat prevention and rapid response in case of a breach.[2]

Chapter 3

Software Used

In the domain of cybersecurity, safeguarding privileged access is a fundamental requirement for ensuring secure IT operations. Organizations depend heavily on specialized software platforms to manage, monitor, and secure their most sensitive user accounts and administrative credentials. One of the leading solutions in this area is CyberArk, a robust software suite designed specifically for Privileged Access Management (PAM). This software is widely recognized for its effectiveness in securing, controlling, and auditing privileged access to critical systems and infrastructure.

CyberArk is not a single application, but rather a comprehensive software ecosystem that includes multiple interconnected components. Each module is designed to serve a specific function while contributing to the overall objective of minimizing the risks associated with privileged accounts. In this project, CyberArk was used and studied in-depth to understand its structure, deployment, and real-world application within enterprise environments.

3.1 Overview of CyberArk

CyberArk is an enterprise-grade software platform that addresses the growing concern of privileged account abuse, which is often a primary vector in major data breaches. These accounts, which typically include system administrators, database administrators, service accounts, and application accounts, have elevated access privileges that can bypass many traditional security controls. If compromised, they can provide attackers with unrestricted access to sensitive data and systems.

The CyberArk software helps prevent such attacks by implementing a multi-layered security model. It allows organizations to store credentials securely, automate password rotation, control access based on user roles, and monitor all privileged session activity. This comprehensive approach not only helps to reduce internal and external security risks but also ensures compliance with industry regulations like HIPAA, GDPR, SOX, and ISO 27001.

3.2 Key Components of CyberArk Software

Each component of the CyberArk platform performs a unique function, contributing to the platform's holistic security framework. Below is a breakdown of the major modules used within the CyberArk software suite:

1. Digital Vault

At the core of CyberArk lies the Digital Vault, a highly secure repository for storing privileged credentials, SSH keys, certificates, and sensitive documents. It uses strong encryption algorithms to protect the data and is designed to operate in an isolated environment, minimizing the risk of external threats. Access to the vault is strictly regulated, with comprehensive logging of every user activity.

2. Password Vault Web Access (PVWA)

PVWA is a user-facing web interface that allows authorized users and administrators to access the platform. Through this portal, users can view stored credentials, initiate password requests, and manage access workflows. PVWA is also used for session launching, policy enforcement, and role-based access control, making it a central access point for the entire software suite.

3. Central Policy Manager (CPM)

The CPM component automates the process of password rotation and policy enforcement. It communicates with the systems where the privileged accounts reside and ensures that passwords are changed regularly based on organizational policies. This automation minimizes the risk of password reuse and exposure and ensures compliance with password best practices.

4. Privileged Session Manager (PSM)

The PSM enables secure, monitored access to critical systems without revealing actual passwords to users. It acts as a proxy between the user and the target system, recording each session in real-time. These recordings are stored securely and can be reviewed later to investigate suspicious activities or ensure compliance with internal policies.

5. Privileged Threat Analytics (PTA)

PTA is an analytics engine that monitors privileged activities for signs of anomalous behavior. It uses machine learning and behavioral analysis techniques to identify threats such as unauthorized access attempts, privilege escalation, or unusual command

executions. When suspicious activity is detected, it triggers real-time alerts and recommends remediation actions.

6. Application Access Manager (AAM)

In modern IT environments, applications and scripts often require access to secure resources. AAM eliminates the risk of hard-coded credentials by providing APIs that applications can use to retrieve passwords securely at runtime. This is particularly beneficial in DevOps and cloud environments where automation is heavily used.[3]
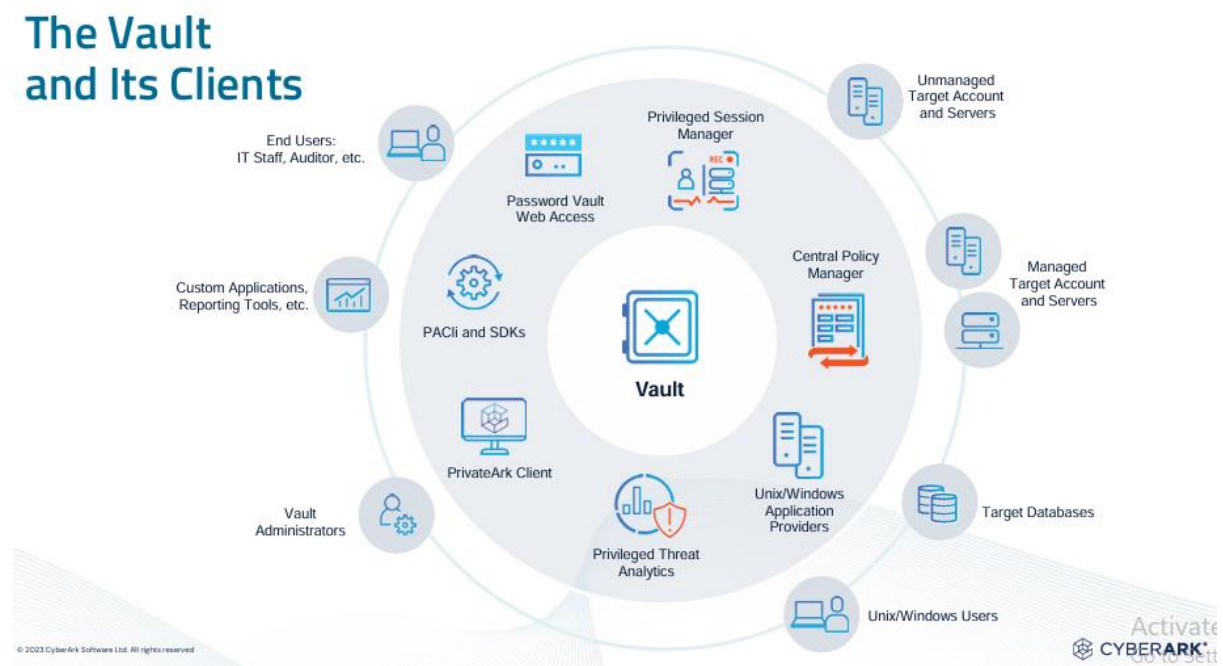

Fig. 3.1 Components of CyberArk

3.3 Features and Benefits of CyberArk Software

CyberArk is widely used across industries due to its wide array of powerful features:

- End-to-End Credential Protection: From storage to access and rotation, CyberArk ensures that credentials are protected at every stage.

- Complete Audit Trail: Every action taken within the platform is logged and time-stamped, helping meet compliance and audit requirements.

- Session Isolation and Recording: Prevents users from directly interacting with target systems while recording all session activity.

- Granular Access Control: Users are granted only the access they need, aligned with the principle of the least privilege.
- Threat Detection and Response: Real-time monitoring and anomaly detection help reduce response times and limit damage from potential breaches.

3.4 CyberArk's Role in the Project

During this project, CyberArk was explored both theoretically and practically to understand its role in modern cybersecurity frameworks. Emphasis was placed on its deployment structure, component interactions, and integration with other enterprise tools such as Active Directory and SIEM systems.

Hands-on experience with the CyberArk environment allowed a deeper appreciation of how each module works in unison to enforce security policies and safeguard high-privilege accounts. The system's seamless automation, intuitive interface, and deep analytical capabilities demonstrate why it is a preferred choice among organizations seeking to strengthen their identity security posture.[4]
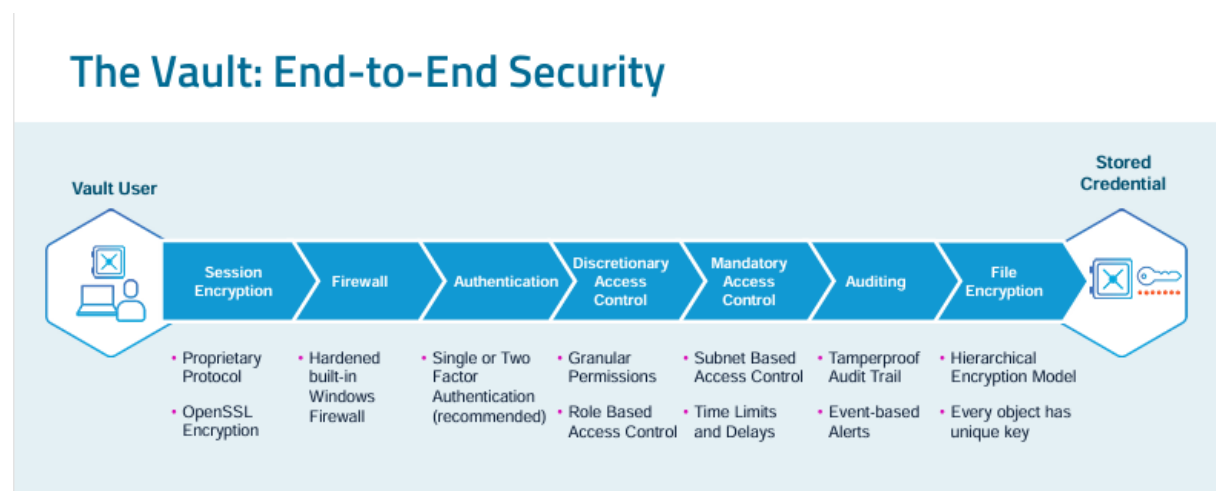

Fig. 3.2 Vault Security

Chapter 4

Requirements and Methodology

4.1 Requirements

4.1.1 Software Requirements

For the successful execution of this project, specific software tools and platforms were required. These components were selected to meet the needs of the CyberArk implementation within the cybersecurity domain. The software components include:

- **CyberArk**: The central component of this project, CyberArk, is a trusted Privileged Access Management (PAM) solution. It plays a crucial role in securing and managing privileged accounts and sensitive system access.
  - *Version*: CyberArk Vault 12.6 (or the version you're working with).
  - *Capabilities*: Includes password vaulting, session control, and activity auditing.
- **Operating Systems**:
  - **Windows Server 2019** (or any supported version) to host CyberArk components and handle administrative tasks.
  - **Linux (Ubuntu)** for integrating other cybersecurity tools and performing additional security tasks.
- **Programming Languages**:
  - **Python**: Employed for automation tasks such as interacting with CyberArk's APIs and handling system security.
  - **PowerShell**: Utilized for automating tasks specific to Windows-based systems.
- **Database**:
  - **Microsoft SQL Server**: Used to store configuration details, logs, and user session data.
  - **MySQL**: Potentially integrated for any additional tools or systems.
- **Security Tools**:
  - **Nessus** or **OpenVAS**: Deployed for conducting vulnerability assessments on the environment.
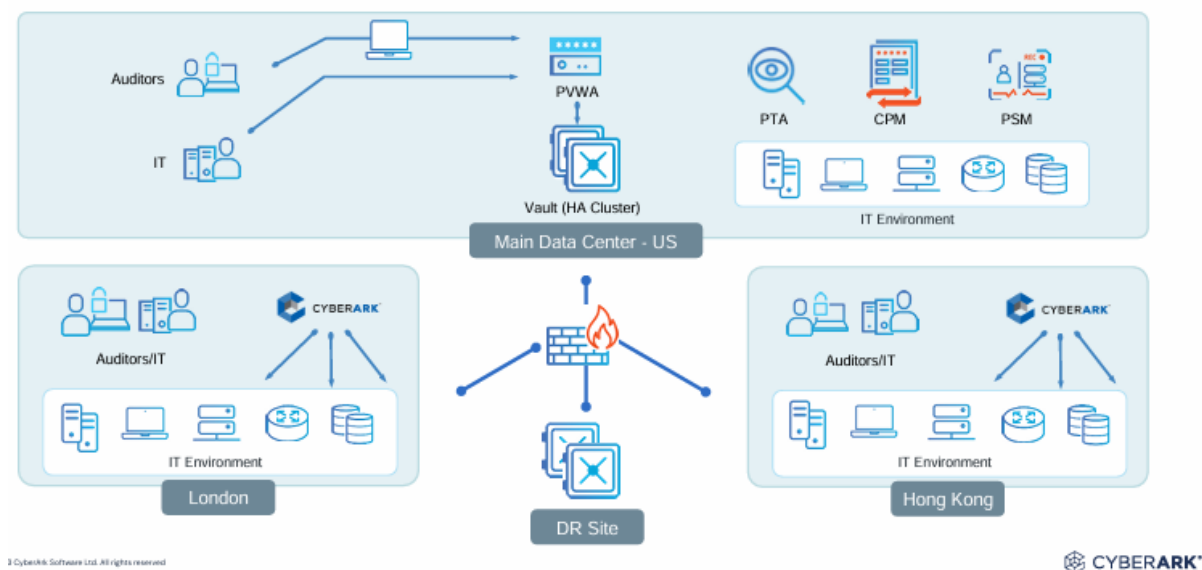 - **Wireshark**: Used for network traffic analysis to verify secure communication.

Fig. 4.1 CyberArk architecture

4.1.2 Hardware Requirements

To ensure the effective operation of the system, the following hardware was deemed necessary:

- **Server Configuration**:
  - **Processor**: Intel Xeon E5 or an equivalent high-performance CPU.
  - **RAM**: A minimum of 16 GB to handle the management of privileged accounts and user sessions efficiently.
  - **Storage**: SSDs with a capacity of at least 500 GB for storing logs, configuration data, and other system-related files.

- **Client Configuration**:
  - **Processor**: Intel Core i5 or higher.
  - **RAM**: 8 GB minimum to ensure the management consoles run smoothly.
  - **Storage**: A minimum of 256 GB SSD for managing files and logs locally.

4.1.3 System Requirements

For optimal performance, the following system requirements must be met:

- **CyberArk Vault** needs to be installed and configured per CyberArk's official documentation and security best practices.
- **Security Measures**: All systems must be securely configured, following standard cybersecurity protocols (e.g., firewall settings, access control, etc.).

- **Networking**: Secure and reliable network connections between all systems in the environment are necessary, with proper network segmentation to protect critical resources.

4.1.4 User Requirements

Key users of the system include:

- **System Administrators**: They will be responsible for configuring and maintaining the CyberArk environment, ensuring that privileged accounts and access policies are securely managed.

- **Security Auditors**: These users will oversee the system's security, performing audits to ensure compliance with regulatory standards.

- **End Users**: Individuals requiring secure access to sensitive systems, whose access will be managed through CyberArk's PAM solutions.[5]

4.2 Methodology

4.2.1 Research & Literature Review

The project began with a thorough review of existing research related to Privileged Access Management (PAM) and its role in modern cybersecurity. This review provided insights into:

- The potential risks associated with inadequate management of privileged accounts.

- The effectiveness of CyberArk as a leading PAM solution.

- How PAM solutions like CyberArk protect organizations from security breaches, focusing on features such as credential vaulting, session monitoring, and access control.

This initial research phase established a comprehensive understanding of CyberArk's importance in the cybersecurity field.

4.2.2 System Design

The system design for the project was developed with a focus on ensuring both security and scalability. The architecture involves multiple layers to secure privileged accounts:

- **CyberArk Vault**: Acts as the core of the system, storing credentials in an encrypted format.

- **PVWA (Privileged Vault Web Access)**: Serves as the interface for managing and accessing privileged accounts.

- **Central Policy Manager (CPM)**: Responsible for enforcing password policies and automating password changes based on security needs.

Key security principles were followed in the design, including:

- **Multi-Factor Authentication (MFA)**: Required for all users accessing privileged accounts to prevent unauthorized access.
- **Session Monitoring**: All user sessions are tracked, recorded, and stored for audit and review.
- **Access Control**: Implemented role-based access control (RBAC) to restrict access based on the user's job function.

4.2.3 Implementation Process

The implementation phase was broken down into distinct steps to ensure a structured deployment of the CyberArk solution:

1. **CyberArk Vault Installation and Setup**:
   o CyberArk Vault was installed on a secure server and configured based on best practices for privileged account management.

2. **System Integration**:
   o Various systems, including network devices and servers, were integrated into CyberArk for centralized management of privileged credentials.
   o Integration with CyberArk APIs allowed for seamless communication between systems and automated management of privileged accounts.

3. **Automation**:
   o **Python scripts** were developed to automate routine administrative tasks like password management and account provisioning.
   o **PowerShell scripts** were utilized to automate Windows-specific tasks, such as managing user accounts.

4. **User Access Configuration**:
   o Role-based access control was enforced, ensuring that only authorized users could access specific systems.
   o MFA was configured to ensure that all privileged access is verified through multiple authentication factors.

4.2.4 Security Analysis

A comprehensive security evaluation was conducted to validate the effectiveness of the implemented CyberArk solution. The steps included:

- **Penetration Testing**: Tools like **Metasploit** were used to simulate attacks on the system and identify potential vulnerabilities.
- **Network Security Audits**: **Wireshark** was employed to capture network traffic and ensure that all sensitive data was encrypted during transmission.
- **Access Control Review**: All user roles and permissions were audited to verify that users only had access to the systems necessary for their roles.

4.2.5 Testing & Evaluation

Once the system was implemented, thorough testing was conducted to ensure that the system met both functional and security requirements:

- **Functional Testing**: This ensured that all features of CyberArk, such as password vaulting, session management, and credential rotation, were functioning properly.
- **Security Testing**: Penetration tests and vulnerability scans were performed to identify weaknesses in the system.
- **User Acceptance Testing (UAT)**: A group of end users tested the system to ensure that it was user-friendly and met their needs.

Chapter 5

Configuration and Implementation Details

5.1 System Setup and Vault Deployment

The CyberArk environment typically begins with the deployment of the **Digital Vault**, the core secure repository where all privileged credentials and configuration data are stored. This Vault is installed on a hardened Windows server with strict firewall rules and system hardening to prevent unauthorized access. The Vault acts as the central node for the PAM solution.
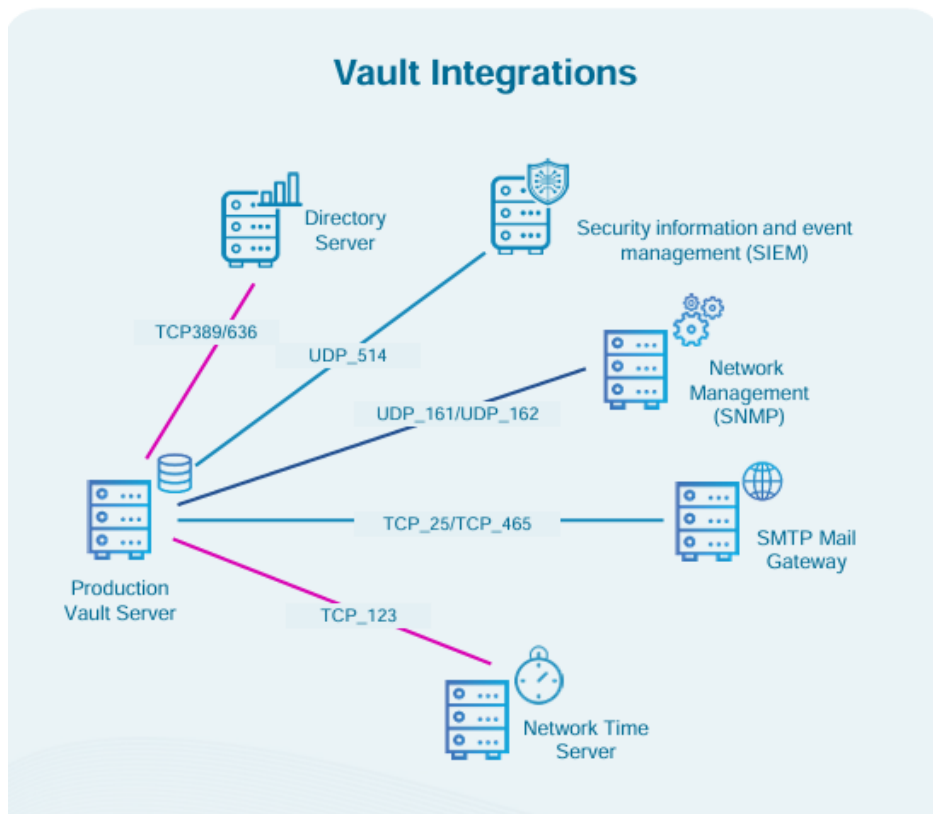

Fig. 5.1 Vault Integrations

5.2 User and Safe Configuration

Once the core components are installed, administrators begin by configuring **Users** and **Safes**. A *Safe* is a logical container in CyberArk where credentials and secrets are securely stored. Users or groups are assigned specific permissions on these Safes—such as Retrieve, List, or Manage—to ensure **role-based access control** (RBAC).

LDAP or Active Directory integration is often used to map existing users into CyberArk, allowing for easier authentication and role assignment.

Example Configuration Tasks:

- Create new safes for departments (e.g., IT, Finance).
- Define access permissions for each role.
- Map LDAP groups to CyberArk roles.
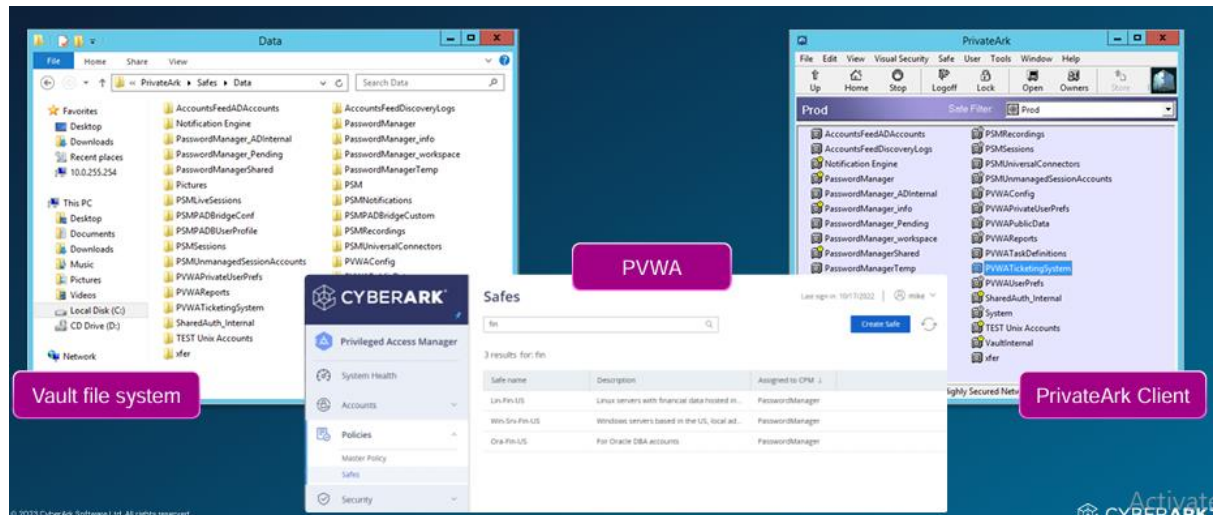
Fig. 5.2 Safe Configuration

5.3 Account Onboarding and Discovery

CyberArk offers automated **account discovery** features. This allows the system to scan the network and detect privileged accounts across Windows, UNIX, databases, and applications. These accounts are then reviewed and onboarded into the Vault.

Onboarding includes defining:

- Which platform does the account belong to (e.g., Windows, Oracle DB)
- Rotation policies (e.g., password must change every 30 days)
- Session recording or monitoring settings

Accounts can be onboarded manually or through bulk import tools. Once onboarded, these accounts are managed centrally under their assigned Safe.[6]
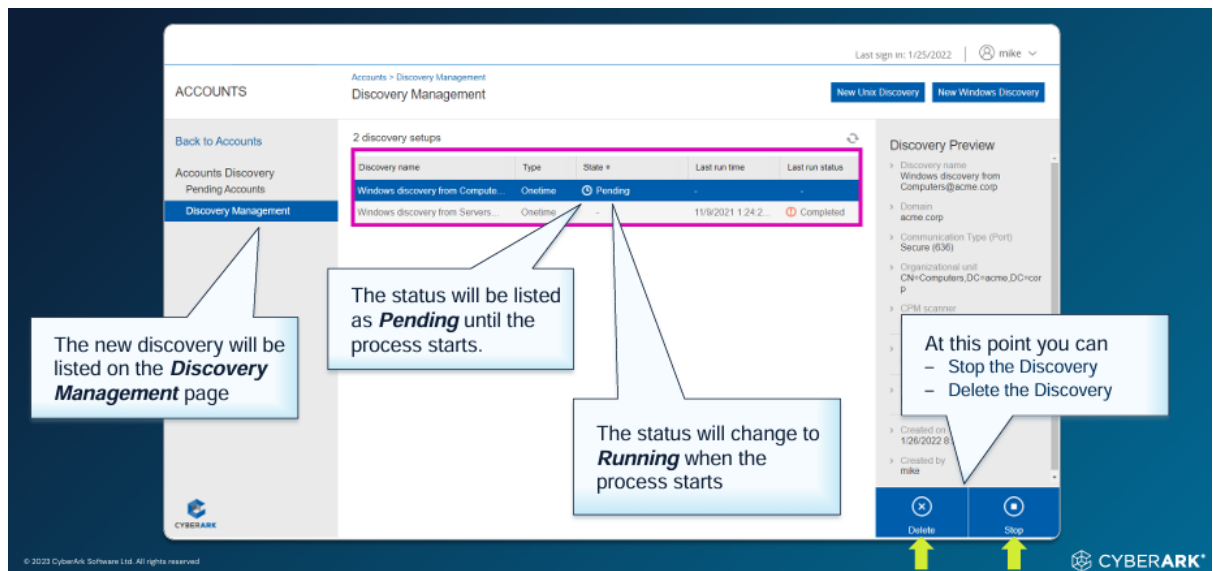
Fig. 5.3 Discovery and Onboarding Accounts

5.4 Session Management and Monitoring

To prevent misuse of privileged accounts, CyberArk employs **Privileged Session Manager (PSM)**. This module allows users to initiate remote sessions (RDP, SSH, etc.) without ever knowing the actual password. The session is launched directly from the PVWA.

Features of PSM:

- Full session recording for audit and compliance
- Real-time monitoring by security teams
- Session isolation to prevent malware spread

Sessions are stored as video-like files and logs can be filtered based on commands, time, and users. This enables forensic analysis in case of suspicious activity.
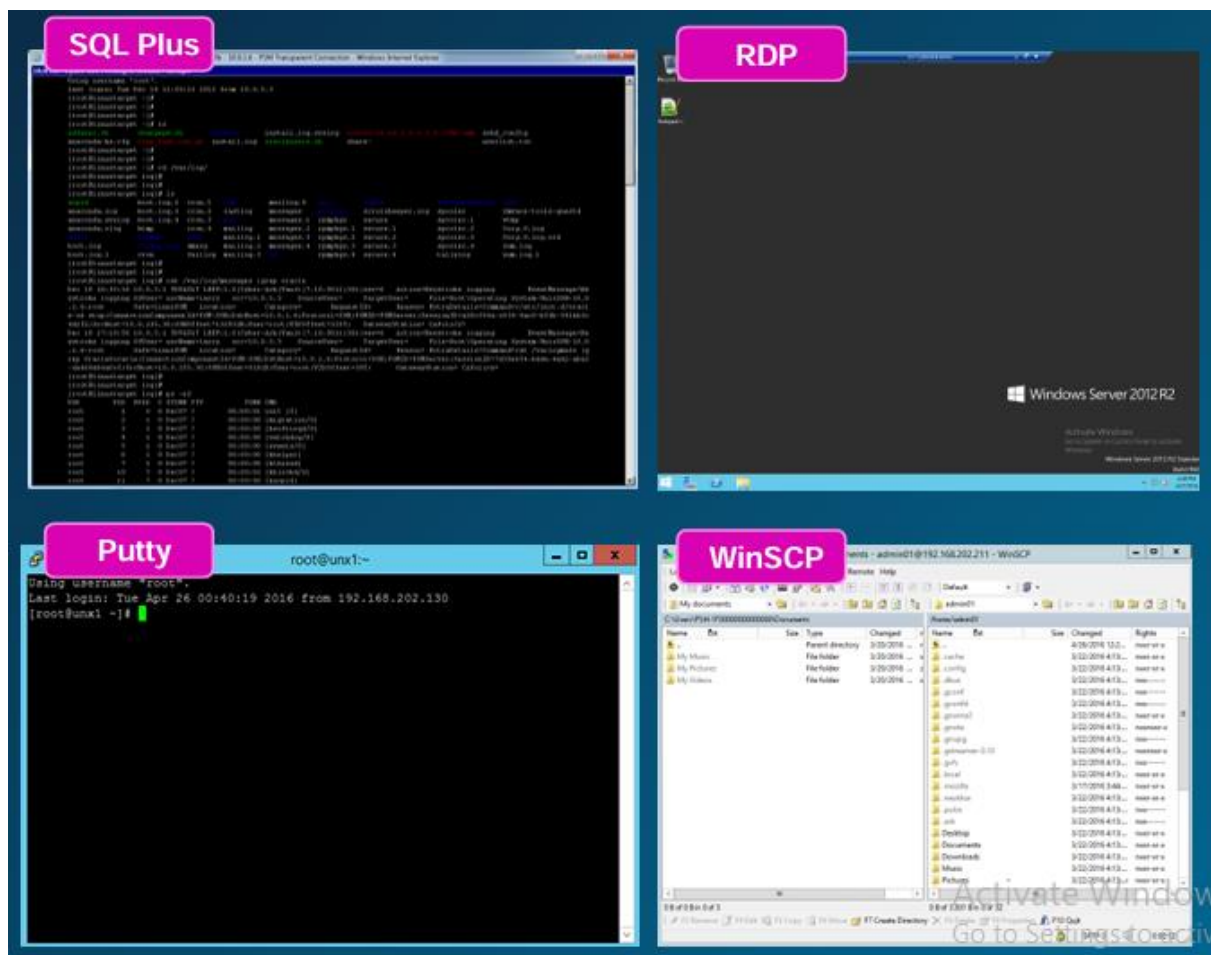
Fig. 5.4 PSM Sessions

5.5 Integration with External Systems

For large enterprises, CyberArk integrates with:

- SIEM tools (e.g., Splunk) for alerting and log forwarding
- Ticketing systems (e.g., ServiceNow) for workflow-based access
- MFA solutions for secure user login

This extensibility ensures CyberArk is part of the broader security ecosystem.

Chapter 6

Backup, Restore and Disaster Recovery

6.1 Importance of Backup and Disaster Recovery

CyberArk stores and manages sensitive data such as administrator credentials, service account passwords, SSH keys, and policy configurations. Any loss or corruption of this information can lead to serious security breaches or administrative disruptions. Therefore, a well-defined and regularly maintained backup and recovery plan is essential.

Some critical reasons for backup and DR planning in CyberArk include:

- Preventing data loss due to hardware failures, software corruption, or human error
- Restoring services quickly after a crash or system failure
- Ensuring business continuity during natural disasters or cyberattacks
- Meeting regulatory compliance and audit requirements for data protection and recovery

6.2 Backup Strategy in CyberArk

CyberArk follows a multi-layered backup strategy that focuses on both the **Vault database** and other application components like **PVWA**, **CPM**, and **PSM**. These backups are usually scheduled through automated scripts and must be tested periodically to ensure integrity.

6.2.1 Vault Backup

The Digital Vault is the heart of CyberArk, and its backup is the most crucial. It involves:

- **PAReplicate Tool:** Used for replicating Vault data to the Disaster Recovery (DR) Vault
- **Manual or Automated File Backup:** Involves copying essential Vault files such as `Vault.ini`, `DBParm.ini`, and the `VaultData` directory
- **Key Files:** Backup of critical keys like `PAKey` is essential to decrypt stored credentials

- **Frequency:** Daily or hourly backups, depending on the organization's data sensitivity

6.2.2 Application Component Backup

For components like PVWA, CPM, and PSM, backup includes:

- **Configuration files:** Including web.config, password policies, and server settings
- **Log files:** For auditing and troubleshooting
- **Database files:** If configured with an external SQL database (e.g., for PVWA session logs).[7]
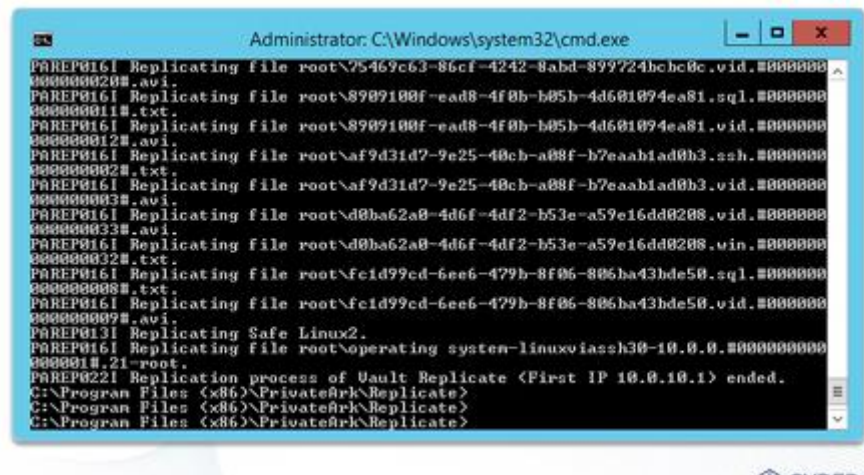

Fig. 6.1 Backup using exe file

6.3 Restoration Procedure

Restoring CyberArk involves retrieving backup files and bringing the system back to a known stable state. The restoration process depends on which component has failed — whether it's the Vault or an application server.

6.3.1 Vault Restoration

In case of Vault failure:

- The **Vault service** is reinstalled using the original installation package.
- The **backed-up VaultData folder and key files** are restored to their original location.

- Configuration files such as `Vault.ini` and `DBParm.ini` are re-applied.
- Vault services are restarted, and connectivity is validated with client tools (PVWA, CPM).

Care must be taken to ensure that the `PAKey` file used is exactly the one tied to the backup, otherwise decryption of data may fail.

6.3.2 Application Restoration

If application servers like PVWA or CPM fail:

- Reinstall the respective component (e.g., PVWA)
- Reconfigure using saved configuration files and policies
- Reconnect the application to the Vault for credential access
- Test logins and integrations to ensure functionality

Fig. 6.2 Restore using exe file

6.4 Disaster Recovery Vault

CyberArk supports a dedicated **Disaster Recovery (DR) Vault** to ensure high availability. The DR Vault is a replica of the production Vault and is kept in sync using **PAReplicate**, which performs real-time or scheduled replication.

6.4.1 How DR Vault Works

- It runs on a separate server, often in a geographically distant location.
- The DR Vault remains passive until activated (failover).
- During normal operation, it continuously receives updates from the primary Vault.
- In the event of a primary Vault failure, administrators can **manually promote the DR Vault** to take over operations.

This setup helps minimize downtime and maintain privileged access during large-scale outages or site disasters.

6.4.2 Failover and Recovery

Failover steps include:

- Shutting down or isolating the failed primary Vault
- Promoting the DR Vault via CyberArk tools
- Reconfiguring PVWA, CPM, and PSM to connect to the new active Vault
- Monitoring synchronization status and logs

After failover, once the original Vault is repaired, it can either be reinstated as primary or kept as a backup.
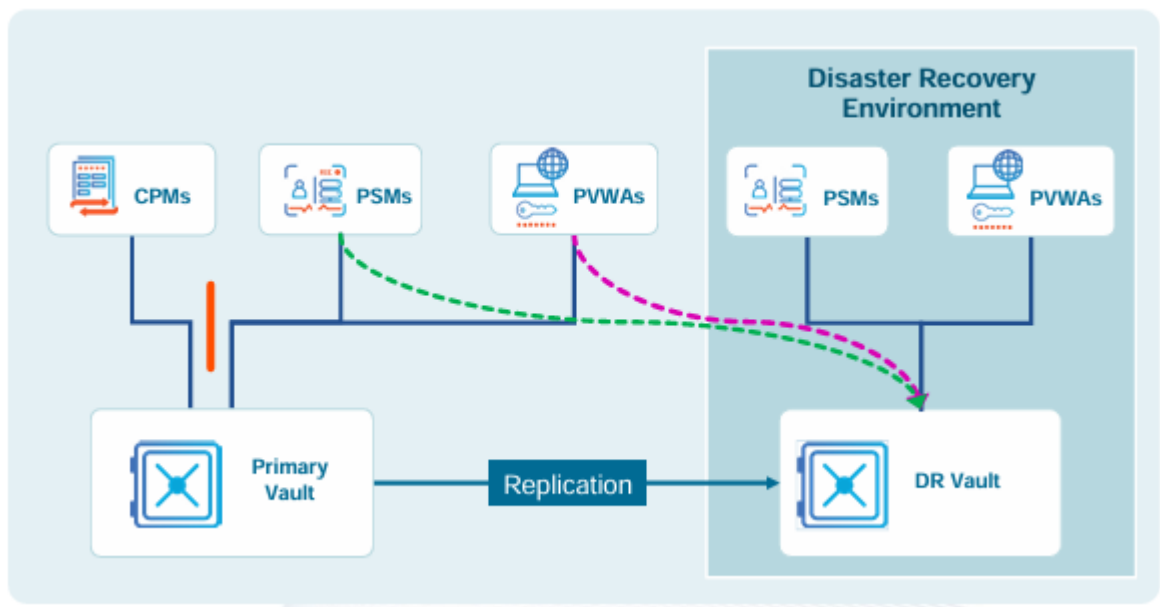

Fig. 6.3 Disaster Recovery Environment

6.5 Maintenance and Validation

Maintaining backup and DR readiness is a continuous process. Key practices include:

- Performing regular validation checks on backup files
- Testing full recovery and failover procedures quarterly or bi-annually
- Monitoring replication status and logs in the DR Vault
- Ensuring all keys, files, and credentials are protected with encryption and access control

It is also advisable to document the entire backup and recovery strategy, including contact points, server names, and recovery time objectives (RTOs) for quick reference.[8]

Chapter 7

Results and Discussions

This section reflects on the practical outcomes and insights gained from the configuration and understanding of the CyberArk Privileged Access Management platform. The focus was on setting up and analyzing the core modules such as Vault, PVWA, CPM, and PSM, along with their security controls, backup strategies, and disaster recovery readiness. These efforts were aimed at building a robust, secure, and scalable PAM solution.

7.1 Observations and Key Findings

- The **Vault** successfully served as the secure storage for privileged credentials, maintaining encryption and centralized access control.
- **PVWA (Password Vault Web Access)** provided a user-friendly interface to manage and monitor privileged account activities.
- **CPM (Central Policy Manager)** was configured to automate password changes and enforce credential policies, reducing human intervention and security risks.
- **PSM (Privileged Session Manager)** enabled secure session monitoring and recording for critical accounts, ensuring accountability and compliance.
- The **backup and DR** mechanisms ensured data integrity and availability during simulated failover conditions.

7.2 Security Improvements and Impact

Implementing CyberArk results in the following improvements:

- **Minimized insider threats** by enforcing the least privilege access and password obfuscation.
- **Improved compliance posture** with session recordings, audit logs, and access tracking.
- **Automated credential rotation** eliminated password fatigue and manual management errors.
- **Disaster recovery capabilities** enhanced system resilience and ensured business continuity.
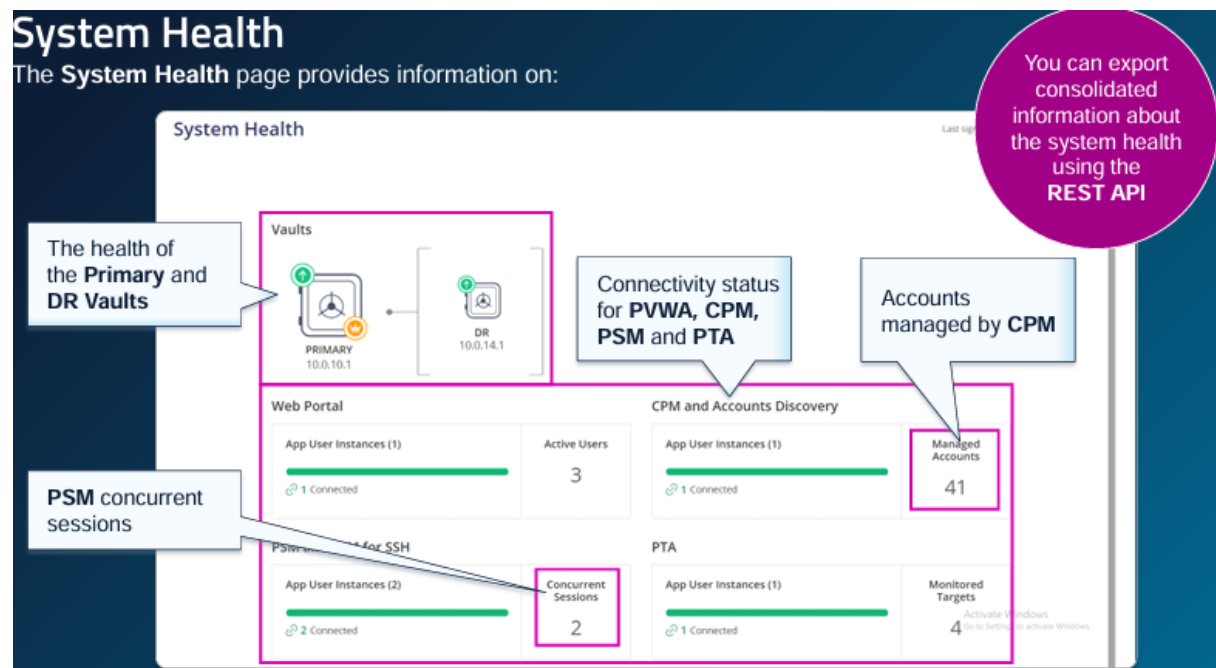
Fig. 7.1 System Health

7.3 Challenges Faced

While working with CyberArk, the following challenges were encountered:

- Initial setup of the Vault and secure key handling required detailed attention and familiarity with encryption methods.
- Configuring DR Vault replication needed careful timing and network optimization.
- Troubleshooting permission and access errors between modules like PVWA and CPM took significant time.
- Limited coding exposure made custom plugin development and automation more difficult, though not essential for base setup.[9]

7.4 Common Issues Encountered During Implementation

During the hands-on work, several challenges arose in various components of the CyberArk environment. These were documented in the Common Issues training and validated in practice.

7.4.1 Authentication and Access Failures

- Users attempting to log into the PVWA after recent password changes often encountered authentication errors.
- In several instances, users were suspended after repeated failed login attempts. This was resolved by either manually unsuspending them or adjusting the `UserLockoutPeriodInMinutes` parameter in the `dbparm.ini` configuration file.
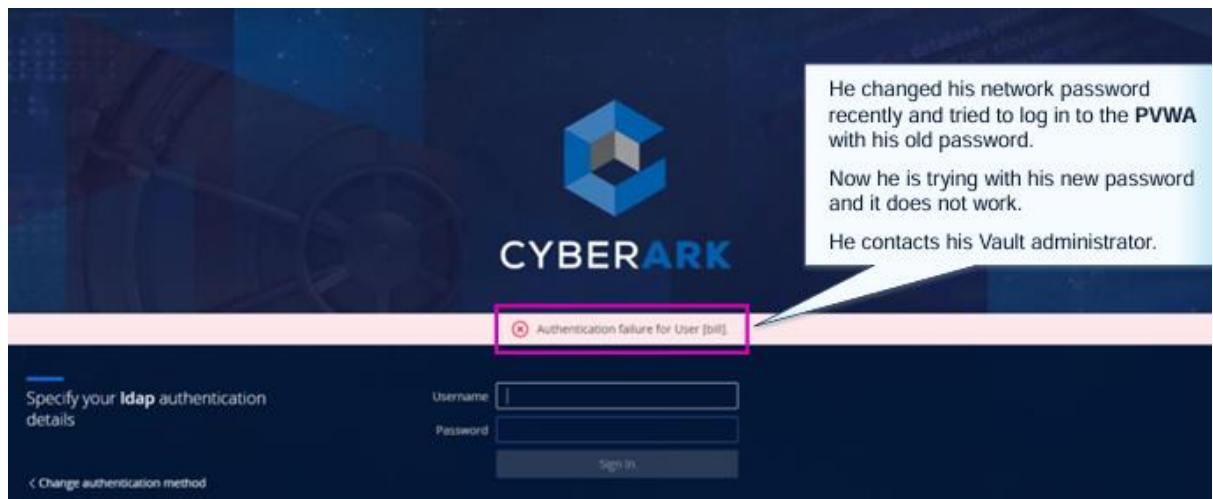- Logs such as `ITAlog.log` provided evidence of repeated failures and suspension triggers.

Fig. 7.2 Authentication Issue

7.4.2 CPM & PSM Connectivity Problems

- A key issue was the **CPM user becoming unsynchronized** with the Vault password. This required a reset of the credential file using the `CreateCredFile.exe` tool.
- Disconnected components were visible in the PVWA System Health dashboard, alerting administrators through email notifications.

- The PSM faced challenges in RDP session initialization. Disabling Network Level Authentication (NLA) and adjusting timeout parameters helped stabilize session launches.

7.5 Troubleshooting Practices and Case Studies

The Troubleshooting training outlined a structured approach for diagnosing issues in the CyberArk environment. This method was validated through test cases and practice scenarios.

7.5.1 Structured Troubleshooting Workflow

- Understand the environment (components, versions, load balancers, DR setup)
- Reproduce the issue and isolate the specific user or system component
- Analyse logs (ITAlog, Vault trace logs, PSM and CPM logs)
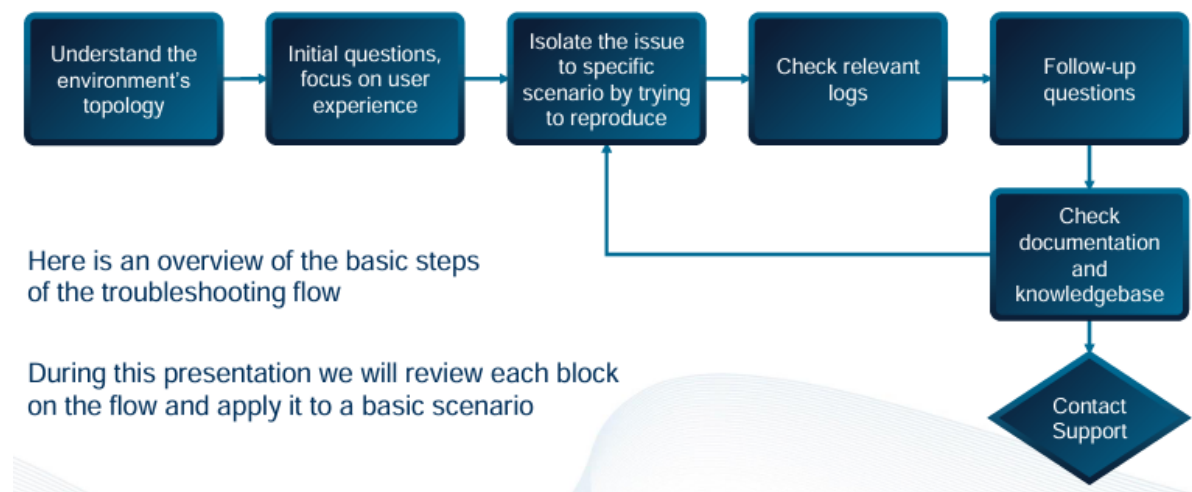- Refer to documentation and knowledgebase articles before escalating

Fig. 7.3 Troubleshooting Flowchart

7.5.2 Case Example – User Unable to Log In

- Problem: A user could not log into PrivateArk with admin credentials.
- Steps: Vault logs showed ITATS528E error. Searching documentation revealed this was due to a password sync issue. Resetting the user password resolved the problem.

This scenario highlighted the importance of precise error codes and detailed logs in troubleshooting.

7.5.3 Log Management and Debug Mode

Each component (Vault, PVWA, CPM, PSM) maintains its own logs. The debug level can be increased temporarily to gather deeper diagnostic information using config files or CyberArk Admin settings.

- The dbparm.ini file in the Vault was updated to change debug levels
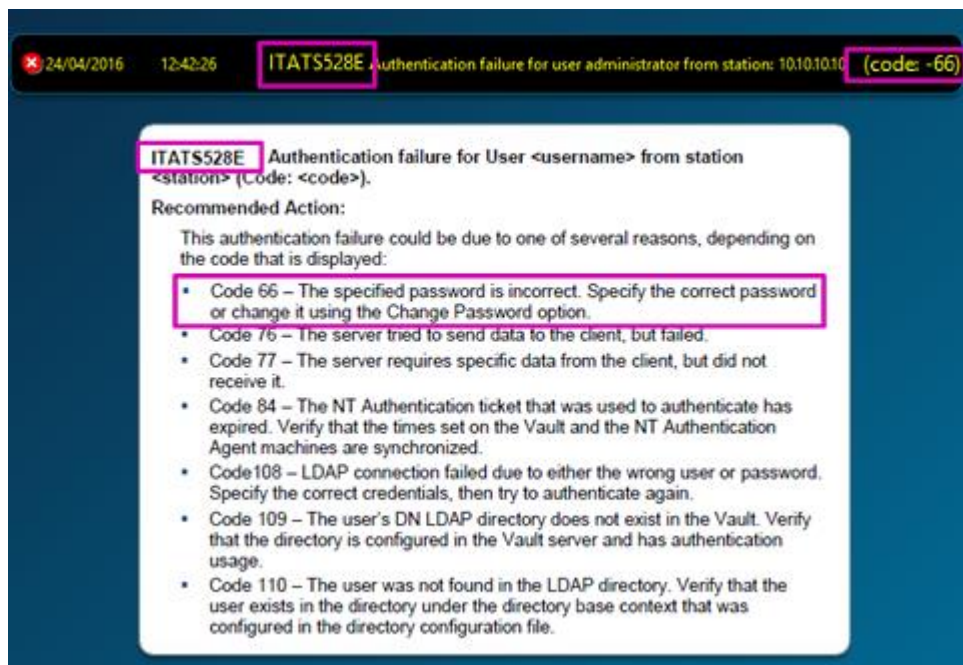- xRay utility was used to gather logs and securely share them with CyberArk support.[10]

Fig. 7.4 Check errors in log file

7.6 Performance, Reliability, and Security Insights

The platform demonstrated strong performance after resolving initial setup issues. Highlights include:

- **Password Rotation**: CPM successfully rotated credentials at scheduled intervals. Logs confirmed no policy failures after syncing reconciler accounts.
- **Session Stability**: PSM sessions maintained consistent connection quality after tuning NLA and timeout settings.

- **Audit Trail Integrity**: Logs and session recordings were complete and timestamped accurately, useful for forensic review and compliance audits.
- **Resilience**: Backup and DR replication notifications functioned correctly, ensuring system redundancy and failover readiness.

7.7 Key Takeaways

- **CyberArk's modular structure** allows precise control but requires careful configuration and regular health monitoring.
- **System health dashboards, log files, and REST APIs** offer transparency and ease of tracking status across the environment.
- **Real-time alerts and SIEM integration** help identify failures and respond quickly.
- **Structured troubleshooting flows**, especially with tools like xRay, simplify issue resolution and help maintain stability.
- **Security and compliance** are enforced through detailed policies, recording, and audit trails, which proved reliable under testing.

Chapter 8

Conclusion and Future Work

Conclusion

This project offered a comprehensive understanding of how CyberArk's Privileged Access Management (PAM) platform secures critical assets in enterprise environments. Through detailed exploration and configuration of key components like the Digital Vault, PVWA, CPM, and PSM, it became evident that CyberArk not only centralizes and automates credential management but also enforces strict access controls and full session visibility.

The configuration of automatic password rotation, privileged session recording, and role-based access demonstrated how the platform minimizes human error and protects against internal and external threats. Additionally, features like email alerts, SIEM integration, and remote monitoring further reinforced the security posture of the system. Despite facing challenges like authentication errors and connection issues during implementation, structured troubleshooting methods and logs enabled smooth resolution.

Future Work

As CyberArk continues to evolve, future enhancements in this field can focus on:

- **Integrating CyberArk with cloud-native platforms** (e.g., AWS, Azure) to manage cloud-based secrets and DevOps credentials.
- **Implementing CyberArk environment** to expand PAM to containerized and microservices environments.
- **Leveraging API and automation** for advanced onboarding workflows and faster response to access requests.
- **Enhancing threat detection** by combining CyberArk logs with machine learning models in SIEM tools.

Future work may also involve conducting penetration testing on the PAM deployment to identify vulnerabilities and further harden the system against sophisticated attacks.

References

[1] https://training.CyberArk.com/learn/course/external/view/classroom/25/privileged-access-management-pam-administration-4-credits

[2] https://community.CyberArk.com/s/article/Get-Started-with-CyberArk-Identity

[3] CyberArk Docs, "PVWA Pre-Installation Tasks," CyberArk, [Online]. Available: https://docs.CyberArk.com/pam-self-hosted/latest/en/content/pas%20inst/pvwa-install-preinstall-tasks.htm

[4] 51Sec, "CyberArk 12.1 Lab – PVWA Installation Guide," 51sec.org, [Online]. Available: https://www.51sec.org/2022/07/25/CyberArk-12-1-lab-3-pvwa-installation/

[5] Microsoft Docs, "Install IIS on Windows Server," Microsoft, [Online]. Available: https://learn.microsoft.com/en-us/iis/install/installing-iis-on-windows-server

[6] https://training.CyberArk.com/learn/course/external/view/elearning/342/CyberArk-pam-install-and-configure-for-customers-3-credits

[7] https://community.CyberArk.com/s/article/Monitoring-Your-CyberArk-PAM-Service-with-SIEM-Essential-Guide-to-SIEM-Analytics

[8] https://community.CyberArk.com/s/article/Running-a-Disaster-Recovery-Exercise-for-CyberArk-PAM-A-Comprehensive-Guide

[9] Doe, A., & Richards, K. (2021). *Enhancing Cybersecurity with Privileged Access Management: A Case Study of CyberArk*. Journal of Cybersecurity and Digital Risk, 8(3), 45-59.

[10] Wang, L., & Zhang, Q. (2022). *Challenges in Securing Privileged Access in Organizations: The Role of CyberArk*. Journal of Information Security, 11(2), 20-30.