CyberArk Defender-PAM Certification

Study Guide

How to use this study guide

We recommend that you thoroughly review each topic listed within the Exam Content section of this study guide. Make sure you understand each topic using the suggested resources or by searching the CyberArk online documentation and the Technical Community. Hands-on experience with the CyberArk solution will be very helpful.

Exam Objectives

The CyberArk Defender-PAM Certification tests for the practical knowledge and technical skills to maintain day-to-day operations and to support the ongoing maintenance of the CyberArk Privileged Access Management solution. It is intended to certify a candidate's competence to fill one of the following roles within a Privileged Account Management Program.

Application Support

The Application Support Engineer provides first-level support of the CyberArk PAM applications within the customer organization.

CyberArk Administrator

The Vault Administrator is responsible for application administration and maintaining an operable PAM environment.

Content Administrator

The Data Administrator is responsible for provisioning safes and platforms, and for onboarding accounts

Preparing for the Exam

Recommended Experience

- 3-6 Months of Experience Administering the CyberArk PAM Solution
- Microsoft MCSE Certification or equivalent experience
- Network+ Certification or equivalent experience
- Security+ Certification or equivalent experience

Training (Recommended)

- Privilege Cloud (CPC) Administration
    - OR
- Privileged Access Management (PAM) Administration
- Find additional Free Learning: CyberArk University, YouTube

Documentation

- Privileged Access Manager - Self-Hosted
    - OR
- Privilege Cloud

Exam Topics

The CyberArk Defender Certification tests examinee's ability to perform the following tasks in seven knowledge domains. All tasks are universal to both PAM – Self Hosted and CyberArk Privilege Cloud unless otherwise noted.

Onboard Accounts

- Prioritize onboarding projects
- Perform a bulk upload of accounts
- Create an onboarding rule
- Onboard an account from the pending accounts list
- Setup a UNIX discovery
- Setup a Windows discovery
- Manually onboard an account

Manage the Application

- Identify and describe tools used to monitor CyberArk application health
- Describe how each component communicates with other devices at a high level
- Identify the purpose of RestAPI

Perform ongoing maintenance and troubleshooting

- Describe how to ensure each component is operational
- Understand which types of activities are break/fix vs. services engagement

Configure and Manage Passwords

- Configure a request/approval process
- Configure workflow processes to ensure non-repudiation
- Configure logon and reconcile accounts
- Configure and link a service account platform to a target account platform
- Configure workflow processes to reduce the risk of credential theft
- Configure Safe Data Retention, Time of Use Restrictions, and CPM assignment
- Identify cases where Loosely Connected Devices would be appropriate

- Manage the password of a supported usage
- Describe the process to provision a safe
- Identify and describe safe naming conventions
- Duplicate a platform
- Add a User/Group to a safe in accordance with access control policies
- Use an Out-of-the-Box platform to manage a device
- Import a custom platform from the Marketplace
- Setup automatic verification, change, and reconciliation of passwords or SSH keys
- Describe the security value of managing credentials

Manage Security and Audit Functions

- Generate reports
- Identify and describe reports within the PVWA
- Describe the use of safe permissions to limit the scope of reports for specific users
- Describe the purpose of the CyberArk Telemetry Tool
- Search for a recording
- Review a recording
- Describe the CyberArk Blueprint
- Understand how to find out more about the CyberArk Blueprint

Configure Session Management

- Configure a split workflow
- Configure the Master Policy to enable the PSM
- Configure the Master Policy to create PSM recordings
- Configure the Master Policy to enable the connect button
- Configure the PSM to use the HTML5 Gateway
- Identify and describe connection components and their functions
- Configure a recording safe
- Describe how to grant access to view recordings or monitor sessions live
- Describe the security value of session isolation and session audit

Configure User Management

- Administer and Operate Remote Access Service (VPAM)