CyberArk Defender Certification

Study Guide

Exam Objectives

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

Application Support

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

Vault Administrator

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

Data Administrator

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

Exam Content

The CyberArk Defender Certification tests examanees ability to perform the following tasks in seven knowledge domains. Only functions of the Core PAM solution are included.

Application Managment

- Identify and describe tools used to monitor CyberArk application health
- Describe the use of PrivateArk
- Describe how each component communicates with others or devices at a high-level
- Describe the process to maintain an appropriate chain of custody for encryption keys

User Management

- Configure additional LDAP hosts
- Validate that pre-configured directory mappings are functioning correctly
- Verify an LDAP configuration is using SSL
- Add a user to a Vault group
- Add an LDAP User/Group to a Local Group
- Compare and contrast save and vault level permissions
- Configure Safe level permissions on a User group
- Configure Vault level permissions on a User
- Identify each Built-In Vault User or Group and their function
- Describe how to log in as the Master user

- Describe how to provision an internally authenticated user in the vault

Password Managment

- Configure a request/approval process
- Configure workflow processes to ensure non-repudiation
- Configure logon and reconcile accounts
- Compare and contrast reconcile and logon accounts
- Configure and link a service account platform to a target account platform
- Configure workflow processes to reduce the risk of credential theft
- Configure workflow processes to comply with audit/regulatory policies
- Configure Safe Data Retention, Time of Use Restrictions, and CPM assignment
- Configure management of workstation passwords using Loosely Connected Devices
- 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 OOB (out-of-box) platform to manage a device
- Import a custom platform from the Marketplace
- Setup automatic verification, management, and reconciliation of passwords or SSH keys

Account Lifecycle Managment

- Perform a bulk upload of accounts
- Create an onboarding rule
- Onboard an account from the pending accounts list
- Set up a UNIX discovery
- Set up a Windows discovery
- Manually onboard an account
- Onboard SSH Keys using Account Uploader

Session Management

- Configure a split workflow
- Configure the master policy to create PSM recordings
- Configure the master policy to enable the connect button
- Configure the master policy to enable the PSM
- Configure the PSM to use the HTML5 Gateway
- Identify and describe connection components and their functions
- Configure various PSM recording capabilities

- Configure CyberArk to allow PSM connections uisng an RDP client, the Connect button and an SSH client
- Configure a recording safe
- Describe how to grant access to view recordings or live monitor sessions

Security and Audit Functions

- Identify and describe all reports and the information they provide to a user
- Describe how to grant permission to users to allow them to run reports
- Describe the purpose of EVD
- Describe the use of safe permission to limit the scope of reports for specific users
- Search for a recording
- Review a recording
- Describe the various PTA detections
- Configure a response to credential theft
- Configure a response to unmanaged credentials
- Configure automatic session termination
- Configure email alerts in PTA

Maintenance and Troubleshooting

- Restore DR to normal operation after a failover
- Back up Vault data with PAReplicate
- Resync a credential file by running createcredfile manually on the command line
- Identify the log files for each component
- Identify and locate component configuration files
- Assemble necessary log files for submission to a case (X-RAY)
- Describe how to ensure each component is operational
- Restore an object to the vault from a PAReplicate backup
- Decrypt a PAReplicate backup using Recover.exe

Study Resources

CyberArk provides a number of resources to prepare for the Defender Exam

Instructor Led Courses

CyberArk Privileged Access Managment Administratration

Free eLearning

Core PAS Troubleshooting

Customizing Privileged Account Requests

Limiting Lateral Movement with CyberArk

Linked Accounts

Working with CyberArk Support

Documentation

CyberArk Privileged Access Security Administration Guide