CYBERARK

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 Account Security Solution. It is intended to certify an examinee's competence to fill one of the following roles within a Privileged Account Security 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 PAS 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 form the following tasks in seven knowledge domains. Only functions of the Core PAS Solution are included.

Account Onboarding

- Perform a bulk upload of accounts using Password Upload Utility or REST
- Create an Onboarding Rule
- Onboard an account from the pending accounts list
- Setup a Unix Discovery
- Setup a Windows Discovery
- Manually onboard an account
- Onboard SSH Keys with Account Uploader

Application Management

- Describe tools that could be used to monitor CyberArk Application Health
- Use PrivateArk with Proficiency
- Describe how each component communicates with others or devices on network at a high level
- Maintain an appropriate chain of custody for Encryption Keys

Ongoing Maintenance

- Restore DR to normal operation after a failover
- Backup 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)
- Ensure each component is operational
- Open a support case with appropriate description and severity
- Create or Upvote an ER
- Restore an object to the vault from a PAReplicate Backup

Password Management Configuration

- Configure a request/approval process
- Configure workflow processes to ensure non-repudiation
- Setup automatic verification, management, and reconciliation of passwords or SSH Keys
- Explain the differences between a logon versus a reconcile account
- Configure a logon account
- Configure a reconcile account
- Properly configure the “SearchForUsages” Platform parameter
- Configure workflow processes to reduce the risk of credential theft
- Configure workflow processes to comply with audit/regulatory policies
- Import a Custom Platform from the Marketplace
- Duplicate a Platform
- Manage the password of a supported usage
- Provision a Safe
- Follow a safe naming convention
- Configure Safe Retention
- Configure Management of Workstation Passwords using Loosely Connected Devices
- Add a User/Group to a safe in accordance with access control policies
- Use an OOB Platform to manage a device

Security and Audit

- Configure a Response to Unmanaged Credentials
- Describe the various PTA detections
- Configure Automatic Session Termination
- Configure a Response to Credential Theft
- Search for a recording
- Utilize safe permissions to limit the scope of reports for specific users

- Understand the purpose of EVD
- Grant appropriate permission to allow users to run reports
- Describe all reports and what information they give a user
- Review a recording
- Configure email alerts in PTA

Session Management Configuration

- Configure the Master Policy to enable the PSM
- Grant Access to view recordings
- Configure a recording safe
- Make a PSM for SSH Connection using an SSH Client
- Make a PSM Connection using the Connect Button
- Make a PSM Connection using an RDP Client
- Setup text based or video based recordings on PSM
- Configure the PSM to utilize the HTML5 Gateway
- Configure the Master Policy to enable the connect button
- Configure the Master Policy to create PSM recordings
- Configure a split workflow
- Describe connection components and what they do

User Management Configuration

- Be able to describe the difference between safe and vault level permissions without the GUI (web or PA client)
- Add an LDAP User/Group to a Local Group
- Configure additional LDAP hosts
- Validate Proper Function of Pre-Configured Directory Mappings
- Verify an LDAP Configuration is using SSL
- Add a User to a Vault Group
- Configure Safe Level Permissions on a User or Group
- Configure Vault Level Permissions on a User
- Describe the purpose of each Built-In Vault User
- Login as the Master user
- Provision an internally authenticated user in the vault
- Set/Reset a Vault User's Password

Study Resources

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

Instructor Led Courses

CyberArk Privileged Account Security Administration

Free eLearning

Core PAS Troubleshooting
Customizing Privileged Account Requests
Limiting Lateral Movement with CyberArk
Linked Accounts
Working with CyberArk Support

Documentation

CyberArk Privileged Access Solution Administration Guide