CyberArk Defender Access Certification

Study Guide

Exam Objectives

The CyberArk Defender - Access 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 Access solution.

Exam Content

The CyberArk Access Certification tests examanees ability to perform the following tasks in six knowledge domains.

Manage Users

- Describe key functionality available in the CyberArk Identity Admin Portal.
- Identify, describe and assign users to roles.
- Describe how to add and manage users.
- Identify and describe dashboards.
- Identify and manage reports.
- Perform CyberArk Identity Connector tasks.
- Identify information available in the User Portal and how to access it.
- Identify basic user management problems and how to resolve them.

Configure application for SSO

- Describe the use of the App Gateway.
- Deploy applications.
- Add applications for SSO from the app catalog, such as Office 365, Salesforce
- Add custom applications.
- Add a custom application using standard protocols such as SAML, WS-Fed and OIDC
- Compare and contrast IDP versus SP initiated logins
- Identify basic SSO issues and how to resolve them.

Configure policies

- Manage user security policies.
- Manage end point policies.
- Manage authentication policies.
- Block IP addresses from accessing Identity
- Manage application policies

- Identify policy configuration issues and how to resolve them.

Configure Adaptive Multi-Factor Authentication (MFA)

- Identify and describe the fundamentals of securing access with adaptive MFA.
- Describe various configurations to minimize MFA prompts.
- Identify and describe MFA filter options.
- Identify and describe MFA use cases.
- Identify and describe steps to install CyberArk Authenticator desktop app.
- Describe what to do if you forget your CyberArk Authenticator pin.
- Identify supported MFA types.
- Describe how to enroll a mobile device.
- Temporarily suspend MFA.
- Identify and configure UBA (User Behavior Analytics).
- Generate risk analysis reports.
- Investigate and report user-risk.
- Identify adaptive MFA issues and how to resolve them.

Manage Endpoints

- Manage certificates and credentials.
- Describe how to enroll CyberArk Identity Windows Device Trust.
- Identify and resolve end point enrollment issues.

Identify and configure LCM (Life Cycle Management) use cases

- Create and delete users in provisioning enabled web applications (outbound provisioning).
- Import user identity data from supported external systems, such as Human Capital Management System (inbound provisioning).
- Identify and describe how LCM works.
- Identify connectors and describe their use.
- Identify and resolve LCM provisioning issues.

Study Resources

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

Instructor Led Courses

Introduction to CyberArk Identity Administration

Free eLearning

https://training.cyberark.com/category/idaptive-elearning

Official YouTube Videos

Documentation

https://docs.cyberark.com/Product-Doc/OnlineHelp/Idaptive/Latest/en/Content/Resources/_TopNav/cc_Home.htm