CyberArk EPM 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 EPM 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 Endpoint Privilege Manager solution.

Exam Format

Number questions: 60 Multiple-Choice items

Time allotted: 90 minutes

Exam Fee: 200 USD

Preparing for the Exam

We recommend a combination training, self-study, and on-the-job experience to get yourself ready to take this exam.

Training

The Endpoint Privilege Manager (EPM) Administration course can help you learn for this certification exam. While taking the training can be an important part of your preparation, it does not guarantee success on the exam. Self-study and on-the-job experience are also important determinants of success.

Study Resources

CyberArk provides the following additional resources to prepare for the EPM Exam

Sample Questions - **Defender - EPM Sample Items**

Online Documentation

CyberArk Endpoint Privilege Manager Documentation

Additional Free eLearning

EPM Rollout – Best Practices

Exam Content

The CyberArk Defender EPM Certification tests examinee's ability to perform the following tasks in six knowledge domains.

Identify and describe EPM basics and key security concepts.

- Define and describe Application Groups
- Define and describe Advanced Policies
- Understand policy actions, priority, and types
- Describe Least Privilege (LP) concepts at a high level
- Describe benefits and limiting permissions
- Compare and contrast normal and elevated programs
- Describe CyberArk's definition of Privileged Management
- Identify and describe the benefits of using Endpoint Privilege Manager (MAC and Windows)
- Identify and describe the event collection inboxes such as Privilege Management Inbox, Threat Protection Inbox, etc.
- Describe basic concepts around threat detection
- Describe Agent processes and communication to server, how the agent communicates to the server

Rollout, basic configurations, and CyberArk recommended practices.

- Identify and describe basic rollout strategies and how to apply them
- Identify and describe threat intelligence
- Describe how to configure SAML
- Identify the required settings to allow EPM to see elevated events (UAC controls and file manifests)
- Identify and describe various settings in agent configuration for specific business requirements
- Identify and describe the requirements for deploying EPM to a developer system
- Identify and describe Non-Persistent VDI set concerns
- Identify and describe Loosely Connected Devices at the EPM SaaS level
- Describe basic policies and naming conventions for CyberArk recommended practices
- Identify and describe the agent policy differences between windows desktop, Mac, and servers

- Identify and describe how some applications can be excluded and/or ignored always from EPM policies and application control
- Describe the "remove local admin" feature
- Identify how to create and customize end user dialogs.

Implement security measures for vertical movement. (PMI, ACI)

- Identify and describe each policy category type and how they are used to handle application control
- Identify and describe the process for handling elevation as local admin
- Identify and describe advanced policy access restriction options
- Identify and describe policy audit options
- Identify and describe Trusted Sources and the different options such as trusted publishers, updaters, etc.
- Describe policy targeting options (computers insets, ad computers, and user groups)
- Describe how to use Threat Intelligence
- Describe how to leverage internet downloaded applications policy
- Describe considerations concerning deny/allow listing folders

Implement security measures for lateral movement. (Ransomware TD,TP)

- Describe how to leverage Threat Deception and the integrations are required
- Describe how to exclude ransomware extensions and applications
- Describe threat protection exclusion options
- Describe options available with Threat Protection
- Identify the considerations with turning enforcement on Threat Protection
- Describe how EPM implements Ransomware protection
- Identify the considerations with turning enforcement on Ransomware

Reporting and audits

- Identify and describe report scheduling, formats, and limitations
- Identify common reports and their usage
- Describe how to customize reports
- Describe the types of reports available in EPM
- Describe the use cases that can be accomplished by RestAPI
- Describe how to display and configure the Threat Detection dashboard

- Describe audit policy usage and elevation requests

Support and troubleshooting

- Identify and describe EPM Agent installation and upgrade logs
- Identify and describe the methods, files, logs, and utilities to troubleshoot problems with EPM agents running on Windows endpoints
- Identify and describe the methods, files, logs, and utilities to troubleshoot problems while installing EPM agents on Windows endpoints
- Given a Windows Agent installation problem, describe how to resolve it
- Identify and describe the methods, files, logs, and utilities to troubleshoot problems with EPM agents running on macOS endpoints
- Identify and describe the steps to troubleshoot MacOS Agents Installation
- Given a MacOS Agent installation problem, describe how to resolve it
- Given a scenario, identify and describe the methods, files, logs, and utilities to troubleshoot problems with EPM Credential Rotation policies
- Given a scenario, explain the steps to troubleshoot End User Computer Performance issues where EPM Agent is installed (performance troubleshooting, conflict management, etc.)
- Given a scenario, explain the steps to troubleshoot and resolve EPM Agent not receiving policies
- Describe EPM agent diagnostic logs
- Understand supportability options for desktop teams (JIT, OPAG, Elevate on demand)