EPM-DEF^{Q&As}

CyberArk Defender - EPM

Pass CyberArk EPM-DEF Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.certbus.com/epm-def.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by CyberArk
Official Exam Center

⚙ **Instant Download** After Purchase

⚙ **100% Money Back** Guarantee

⚙ **365 Days** Free Update

⚙ **800,000+** Satisfied Customers

QUESTION 1

On the Default Policies page, what are the names of policies that can be set as soon as EPM is deployed?

A. Privilege Escalation, Privilege Management, Application Management

B. Privilege Management, Application Control, Threat analysis

C. Privilege Management, Threat Protection, Application Escalation Control

D. Privilege Management, Privilege Threat Protection, Local Privileged Accounts Management

Correct Answer: D

QUESTION 2

An EPM Administrator would like to notify end users whenever the Elevate policy is granting users elevation for their applications. Where should the EPM Administrator go to enable the end-user dialog?

A. End-user UI in the left panel of the console

B. Advanced, Agent Configurations

C. Default Policies

D. End-User UI within the policy

Correct Answer: D

QUESTION 3

What feature is designed to exclude applications from CyberArk EPM\\'s Ransomware Protection, without whitelisting the application launch?

A. Trusted Sources

B. Authorized Applications (Ransomware Protection)

C. Threat Intelligence

D. Policy Recommendations

Correct Answer: B

QUESTION 4

Which setting in the agent configuration controls how often the agent sends events to the EPM Server?

A. Event Queue Flush Period

B. Heartbeat Timeout

C. Condition Timeout

D. Policy Update Rate

Correct Answer: A

QUESTION 5

When working with credential rotation/loosely connected devices, what additional CyberArk components are required?

A. PTA

B. OPM

C. PVWA

D. DAP

Correct Answer: C

QUESTION 6

Which of the following application options can be used when defining trusted sources?

A. Publisher, Product, Size, URL

B. Publisher, Name, Size, URI

C. Product, URL, Machine, Package

D. Product, Publisher, User/Group, Installation Package

Correct Answer: D

QUESTION 7

What are Trusted sources for Windows endpoints used for?

A. Creating policies that contain trusted sources of applications.

B. Defining applications that can be used by the developers.

C. Listing all the approved application to the end users.

D. Managing groups added by recommendation.

Correct Answer: C

QUESTION 8

A particular user in company ABC requires the ability to run any application with administrative privileges every day that they log in to their systems for a total duration of 5 working days.

What is the correct solution that an EPM admin can implement?

A. An EPM admin can generate a JIT access and elevation policy with temporary access timeframe set to 120 hours

B. An EPM admin can generate a JIT access and elevation policy with temporary access timeframe set to 120 hours and Terminate administrative processes when the policy expires option unchecked

C. An EPM admin can create an authorization token for each application needed by running: EPMOPAGtool.exe -command gentoken -targetUser -filehash -timeLimit 120 -action run

D. An EPM admin can create a secure token for the end user\\'s computer and instruct the end user to open an administrative command prompt and run the command vfagent.exe - UseToken

Correct Answer: B

QUESTION 9

What can you manage by using User Policies?

A. Just-In-Time endpoint access and elevation, access to removable drives, and Services access.

B. Access to Windows Services only.

C. Filesystem and registry access, access to removable drives, and Services access.

D. Just-In-Time endpoint access and elevation, access to removable drives, filesystem and registry access, Services access, and User account control monitoring.

Correct Answer: D

QUESTION 10

CyberArk EPM\\'s Ransomware Protection comes with file types to be protected out of the box. If an EPM Administrator would like to remove a file type from Ransomware Protection, where can this be done?

A. Policy Scope within Protect Against Ransomware

B. Authorized Applications (Ransomware Protection) within Application Groups

C. Set Security Permissions within Advanced Policies

D. Protected Files within Agent Configurations

Correct Answer: D