Actual exam question from CyberArk's EPM-DEF

Question #: 1

Topic #: 1

[All EPM-DEF Questions]

A Helpdesk technician needs to provide remote assistance to a user whose laptop cannot connect to the Internet to pull EPM policies. What CyberArk EPM feature should the Helpdesk technician use to allow the user elevation capabilities?

A. Offline Policy Authorization Generator

B. Elevate Trusted Application If Necessary

C. Just In Time Access and Elevation

D. Loosely Connected Devices Credential Management

Show Suggested Answer

Actual exam question from CyberArk's EPM-DEF

Question #: 2

Topic #: 1

[All EPM-DEF Questions]

Which user or group will not be removed as part of CyberArk EPM's Remove Local Administrators feature?

A. Built-in Local Administrator

B. Domain Users

C. Admin Users

D. Power Users

Show Suggested Answer

Actual exam question from CyberArk's EPM-DEF
Question #: 3
Topic #: 1
[All EPM-DEF Questions]

An end user is reporting that an application that needs administrative rights is crashing when selecting a certain option menu item. The Application is part of an advanced elevate policy and is working correctly except when using that menu item.
What could be the EPM cause of the error?

A. The Users defined in the advanced policy do not include the end user running the application.

B. The Advanced: Time options are not set correctly to include the time that the user is running the application at.

C. The Elevate Child Processes option is not enabled.

D. The Specify permissions to be set for selected Services on End-user Computers is set to Allow Start/Stop

Show Suggested Answer

Actual exam question from CyberArk's EPM-DEF

Question #: 4

Topic #: 1

[All EPM-DEF Questions]

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

Show Suggested Answer

Actual exam question from CyberArk's EPM-DEF

Question #: 5

Topic #: 1

[All EPM-DEF Questions]

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

Show Suggested Answer

Actual exam question from CyberArk's EPM-DEF

Question #: 6

Topic #: 1

[All EPM-DEF Questions]

What EPM component is responsible for communicating password changes in credential rotation?

A. EPM Agent

B. EPM Server

C. EPM API

D. EPM Discovery

Show Suggested Answer

Actual exam question from CyberArk's EPM-DEF

Question #: 7

Topic #: 1

[All EPM-DEF Questions]

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

Show Suggested Answer

Actual exam question from CyberArk's EPM-DEF

Question #: 8

Topic #: 1

[All EPM-DEF Questions]

Which of the following is CyberArk's Recommended FIRST roll out strategy?

A. Implement Application Control

B. Implement Privilege Management

C. Implement Threat Detection

D. Implement Ransomware Protection

Show Suggested Answer

Actual exam question from CyberArk's EPM-DEF

Question #: 9

Topic #: 1

[All EPM-DEF Questions]

An EPM Administrator would like to include a particular file extension to be monitored and protected under Ransomware Protection. What setting should the EPM Administrator configure to add the extension?

A. Authorized Applications (Ransomware Protection)

B. Files to be Ignored Always

C. Anti-tampering Protection

D. Default Policies

Show Suggested Answer

Actual exam question from CyberArk's EPM-DEF

Question #: 10

Topic #: 1

[All EPM-DEF Questions]

When deploying EPM and in the Privilege Management phase what is the purpose of Discovery?

A. To identify all non-administrative events

B. To identify all administrative level events

C. To identify both administrative and non-administrative level events

D. To identify non-administrative threats

Show Suggested Answer

Actual exam question from CyberArk's EPM-DEF

Question #: 11

Topic #: 1

[All EPM-DEF Questions]

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.

Show Suggested Answer

Actual exam question from CyberArk's EPM-DEF

Question #: 12

Topic #: 1

[All EPM-DEF Questions]

CyberArk's Privilege Threat Protection policies are available for which Operating Systems? (Choose two.)

A. Windows Workstations

B. Windows Servers

C. MacOS

D. Linux

Show Suggested Answer

Actual exam question from CyberArk's EPM-DEF

Question #: 13

Topic #: 1

[All EPM-DEF Questions]

Which threat intelligence source requires the suspect file to be sent externally?

A. NSRL

B. Palo Alto Wildfire

C. VirusTotal

D. CyberArk Application Risk Analysis Service (ARA)

Show Suggested Answer

Actual exam question from CyberArk's EPM-DEF

Question #: 14

Topic #: 1

[All EPM-DEF Questions]

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

Show Suggested Answer

Actual exam question from CyberArk's EPM-DEF

Question #: 15

Topic #: 1

[All EPM-DEF Questions]

An EPM Administrator would like to exclude an application from all Threat Protection modules. Where should the EPM Administrator make this change?

A. Privilege Threat Protection under Policies.

B. Authorized Applications under Application Groups.

C. Protect Against Ransomware under Default Policies.

D. Threat Protection under Agent Configurations.

Show Suggested Answer

Actual exam question from CyberArk's EPM-DEF

Question #: 16

Topic #: 1

[All EPM-DEF Questions]

Which EPM reporting tool provides a comprehensive view of threat detection activity?

A. Threat Detection Dashboard

B. Detected Threats

C. Threat Detection Events

D. McAfee ePO Reports

Show Suggested Answer

Actual exam question from CyberArk's EPM-DEF

Question #: 17

Topic #: 1

[All EPM-DEF Questions]

What type of user can be created from the Threat Deception LSASS Credential Lures feature?

A. It does not create any users

B. A standard user

C. A local administrator user

D. A domain admin user

Show Suggested Answer

Actual exam question from CyberArk's EPM-DEF

Question #: 18

Topic #: 1

[All EPM-DEF Questions]

What is a valid step to investigate an EPM agent that is unable to connect to the EPM server?

A. On the end point, open a browser session to the URL of the EPM server.

B. Ping the endpoint from the EPM server.

C. Ping the server from the endpoint.

D. Restart the end point

Show Suggested Answer

Actual exam question from CyberArk's EPM-DEF

Question #: 19

Topic #: 1

[All EPM-DEF Questions]

Which programming interface enables you to perform activities on EPM objects via a REST Web Service?

A. EPM Web Services SDK

B. Application Password SDK

C. Mac Credential Provider SDK

D. Java password SDK

Show Suggested Answer

Actual exam question from CyberArk's EPM-DEF

Question #: 20

Topic #: 1

[All EPM-DEF Questions]

What are the policy targeting options available for a policy upon creation?

A. AD Users and Groups, Computers in AD Security Groups, Servers

B. Computers in this set, Computers in AD Security Groups, Users and Groups

C. OS Computers, EPM Sets, AD Users

D. EPM Sets, Computers in AD Security Groups, AD Users and AD Security Groups

Show Suggested Answer

Actual exam question from CyberArk's EPM-DEF

Question #: 21

Topic #: 1

[All EPM-DEF Questions]

When enabling Threat Protection policies, what should an EPM Administrator consider? (Choose two.)

A. Some Threat Protection policies are applicable only for Windows Servers as opposed to Workstations.

B. Certain Threat Protection policies apply for specific applications not found on all machines.

C. Threat Protection policies requires an additional agent to be installed.

D. Threat Protection features are not available in all regions.

Show Suggested Answer

Actual exam question from CyberArk's EPM-DEF

Question #: 22

Topic #: 1

[All EPM-DEF Questions]

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

A. PTA

B. OPM

C. PVWA

D. DAP

Show Suggested Answer

Actual exam question from CyberArk's EPM-DEF

Question #: 23

Topic #: 1

[All EPM-DEF Questions]

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.

Show Suggested Answer

Actual exam question from CyberArk's EPM-DEF
Question #: 24
Topic #: 1
[All EPM-DEF Questions]

An end user is experiencing performance issues on their device after the EPM Agent had been installed on their machine. What should the EPM Administrator do first to help resolve the issue?

A. Verify any 3rd party security solutions have been added to EPM's Files To Be Ignored Always configuration and CyberArk EPM has also been excluded from the 3rd party security solutions.

B. Enable the Default Policy's Privilege Management Control, Unhandled Privileged Applications in Elevate mode.

C. Rerun the agent installation on the user's machine to repair the installation.

D. Uninstall or disable any anti-virus software prohibiting the EPM Agent functionalities.

Show Suggested Answer

Actual exam question from CyberArk's EPM-DEF

Question #: 26

Topic #: 1

[All EPM-DEF Questions]

Before enabling Ransomware Protection, what should the EPM Administrator do first?

A. Enable the Privilege Management Inbox in Elevate mode.

B. Enable the Control Applications Downloaded From The Internet feature in Restrict mode.

C. Review the Authorized Applications (Ransomware Protection) group and update if necessary.

D. Enable Threat Protection and Threat Intelligence modules.

Show Suggested Answer

Actual exam question from CyberArk's EPM-DEF

Question #: 27

Topic #: 1

[All EPM-DEF Questions]

How does EPM help streamline security compliance and reporting?

A. Use of automated distribution of reports to the security team

B. Provides reports in standard formats such as PDF, Word and Excel

C. Print reports

D. Create custom reports

Show Suggested Answer

Actual exam question from CyberArk's EPM-DEF

Question #: 28

Topic #: 1

[All EPM-DEF Questions]

Select the default threat intelligence source that requires additional licensing.

A. VirusTotal

B. Palo Alto WildFire

C. CyberArk Application Risk Analysis Service

D. NSRL

Show Suggested Answer

Actual exam question from CyberArk's EPM-DEF

Question #: 29

Topic #: 1

[All EPM-DEF Questions]

When deploying Ransomware Protection, what tasks should be considered before enabling this functionality? (Choose two.)

A. Add trusted software to the Authorized Applications (Ransomware protection) Application Group

B. Add trusted software to the Allow Application Group

C. Add additional files, folders, and/or file extensions to be included to Ransomware Protection

D. Enable Detect privileged unhandled applications under Default Policies

Show Suggested Answer

Actual exam question from CyberArk's EPM-DEF

Question #: 30

Topic #: 1

[All EPM-DEF Questions]

When working with credential rotation at the EPM level, what is the minimum time period that can be set between connections?

A. 1 hour

B. 5 hours

C. 24 hours

D. 72 hours

Show Suggested Answer

Actual exam question from CyberArk's EPM-DEF

Question #: 31

Topic #: 1

[All EPM-DEF Questions]

What unauthorized change can CyberArk EPM Ransomware Protection prevent?

A. Windows Registry Keys

B. Website Data

C. Local Administrator Passwords

D. Certificates in the Certificate Store

Show Suggested Answer

Actual exam question from CyberArk's EPM-DEF

Question #: 32

Topic #: 1

[All EPM-DEF Questions]

An EPM Administrator would like to enable CyberArk EPM's Ransomware Protection in Restrict mode. What should the EPM Administrator do?

A. Set Block unhandled applications to On.

B. Set Protect Against Ransomware to Restrict.

C. Set Protect Against Ransomware to Restrict and Set Block unhandled applications to On.

D. Set Control unhandled applications to Detect.

Show Suggested Answer

Actual exam question from CyberArk's EPM-DEF

Question #: 33

Topic #: 1

[All EPM-DEF Questions]

Where would an EPM admin configure an application policy that depends on a script returning true for an end user's machine being connected to an open (no password protection) Wi-Fi?

A. Advanced Policy - Application Control - Check Wi-Fi security

B. Advanced Policy - Options: Conditional enforcement - Apply Policy according to Script execution result

C. Default policies - Check if network access is secure

D. Advanced Policy - Access - Specify permissions to be set for Wi-Fi network security

Show Suggested Answer

Actual exam question from CyberArk's EPM-DEF

Question #: 34

Topic #: 1

[All EPM-DEF Questions]

An EPM Administrator would like to enable a Threat Protection policy, however, the policy protects an application that is not installed on all endpoints.

What should the EPM Administrator do?

A. Enable the Threat Protection policy and configure the Policy Targets.

B. Do not enable the Threat Protection policy.

C. Enable the Threat Protection policy only in Detect mode.

D. Split up the endpoints in to separate Sets and enable Threat Protection for only one of the Sets.

Show Suggested Answer

Actual exam question from CyberArk's EPM-DEF

Question #: 35

Topic #: 1

[All EPM-DEF Questions]

Which policy can be used to improve endpoint performance for applications commonly used for software development?

A. Developer Applications

B. Trusted Application

C. Trusted Source

D. Software Updater

Show Suggested Answer

Actual exam question from CyberArk's EPM-DEF

Question #: 36

Topic #: 1

[All EPM-DEF Questions]

What are the predefined application groups?

A. Developer group, Administrator group

B. Run as Administrator, Run as Developer, Block

C. Elevate, Allow, Block, Developer Applications

D. Block Only

Show Suggested Answer

Actual exam question from CyberArk's EPM-DEF

Question #: 37

Topic #: 1

[All EPM-DEF Questions]

In EPM, creation of which user type is required to use SAML?

A. Local CyberArk EPM User

B. AD User

C. SQL User

D. Azure AD User

Show Suggested Answer

Actual exam question from CyberArk's EPM-DEF

Question #: 38

Topic #: 1

[All EPM-DEF Questions]

For Advanced Policies, what can the target operating system users be set to?

A. Local or AD users and groups, Azure AD User, Azure AD Group

B. AD Groups, Azure AD Groups

C. Local or AD users and groups

D. Local or AD users, Azure AD Users

Show Suggested Answer

Actual exam question from CyberArk's EPM-DEF
Question #: 39
Topic #: 1
[All EPM-DEF Questions]

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 <username> -filehash <file hash> -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 <securetoken_value>

Show Suggested Answer