



**Free Questions for [EPM-DEF](#) by [go4braindumps](#)**

**Shared by [Schultz](#) on [20-03-2023](#)**

**For More Free Questions and Preparation Resources**

**[Check the Links on Last Page](#)**

## Question 1

---

**Question Type:** MultipleChoice

---

What is the CyberArk recommended practice when deploying the EPM agent to non-persistent VDIs?

### Options:

---

- A- A separate set
- B- a VDI advanced policy
- C- a separate license
- D- A separate computer group

### Answer:

---

D

## Question 2

---

**Question Type:** MultipleChoice

---

How does CyberArk EPM's Ransomware Protection feature monitor for Ransomware Attacks?

**Options:**

---

- A-** It compares known ransomware signatures retrieved from virus databases.
- B-** It sandboxes the suspected ransomware and applies heuristics.
- C-** It monitors for any unauthorized access to specified files.
- D-** It performs a lookup of file signatures against VirusTotal's database.

**Answer:**

---

B

## Question 3

---

**Question Type: MultipleChoice**

---

If Privilege Management is not working on an endpoint, what is the most likely cause that can be verified in the EPM Agent Log Files?

**Options:**

---

- A- Behavior of the elevation prompt for administrators in Admin Approval Mode is set to "Prompt for Consent for non-Windows binaries".
- B- Agent version is incompatible.
- C- UAC policy Admin Approval for the Built-in Administrator Account is set to "Disabled".
- D- UAC policy Run all administrators in Admin Approval Mode is set to "Enabled".

**Answer:**

---

D

## Question 4

---

**Question Type: MultipleChoice**

---

When adding the EPM agent to a pre-existing security stack on workstation, what two steps are CyberArk recommendations. (Choose two.)

**Options:**

---

- A- Add any pre-existing security application to the Files to Be Ignored Always.

- B-** Add EPM agent to the other security tools exclusions.
- C-** EPM agent should never be run with any other security tools.
- D-** Create new advanced policies for each security tool.

**Answer:**

---

A, B

## Question 5

---

**Question Type:** MultipleChoice

---

For the CyberArk EPM Threat Deception Credential Lure feature, what is the recommendation regarding the username creation?

**Options:**

---

- A-** The username should match to an existing account.
- B-** The username should have a strong password associated.
- C-** The username should not match to an existing account.
- D-** The username should match the built-in local Administrator.

**Answer:**

---

C

## Question 6

---

**Question Type: MultipleChoice**

---

An EPM Administrator needs to create a policy to allow the MacOS developers elevation to an application. What type of policy should be used?

**Options:**

---

- A- Elevate Application Group
- B- Developer Applications Application Group
- C- Elevate Trusted Applications If Necessary Advanced Policy
- D- Elevate MacOS Policy

**Answer:**

---

C

## Question 7

---

**Question Type:** MultipleChoice

---

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?

### Options:

---

- 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

### Answer:

---

D

## Question 8

---

**Question Type:** MultipleChoice

---

Where can you view CyberArk EPM Credential Lures events?

**Options:**

---

- A- Application Catalog
- B- Threat Protection Inbox
- C- Events Management
- D- Policy Audit

**Answer:**

---

B

## Question 9

---

**Question Type: MultipleChoice**

---

When blocking applications, what is the recommended practice regarding the end-user UI?



**Options:**

---

- A- Show a block prompt for blocked applications.
- B- Show no prompts for blocked applications.
- C- Hide the CyberArk EPM Agent icon in the system tray.
- D- Enable the Default Deny policy.

**Answer:**

---

A

## Question 10

---

**Question Type: MultipleChoice**

---

A company is looking to manage their Windows Servers and Desktops with CyberArk EPM. Management would like to define different default policies between the Windows Servers and Windows Desktops.

What should the EPM Administrator do?

**Options:**

---

- A- In the Default Policies, exclude either the Windows Servers or the Windows Desktops.
- B- Create Advanced Policies to apply different policies between Windows Servers and Windows Desktops.
- C- CyberArk does not recommend installing EPM Agents on Windows Servers.
- D- Create a separate Set for Windows Servers and Windows Desktops.

**Answer:**

---

B

**To Get Premium Files for EPM-DEF Visit**

<https://www.p2pexams.com/products/epm-def>

**For More Free Questions Visit**

<https://www.p2pexams.com/cyberark/pdf/epm-def>

