CyberArk Defender - EPM

CyberArk EPM-DEF

Version Demo

Total Demo Questions: 10

Total Premium Questions: 60

QUESTION NO: 1

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

A. Windows Workstations

B. Windows Servers

C. MacOS

D. Linux

ANSWER: A B

QUESTION NO: 2

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

ANSWER: C

QUESTION NO: 3

What are valid policy options for JIT and elevation policies?

A. Grant temporary access for all users, Policy name, Restart administrative processes in admin approval mode, Collect audit information

B. Grant temporary access for, Policy name, Terminate administrative processes when the policy expires, Collect audit information

C. Grant administrative access, Policy name, Log off to apply policy, Collect policy violation information

D. Terminate administrative services, Grant policy access for, Policy name, Collect audit reports

ANSWER: C

QUESTION NO: 4

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

ANSWER: A C

QUESTION NO: 5

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?

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

QUESTION NO: 6

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

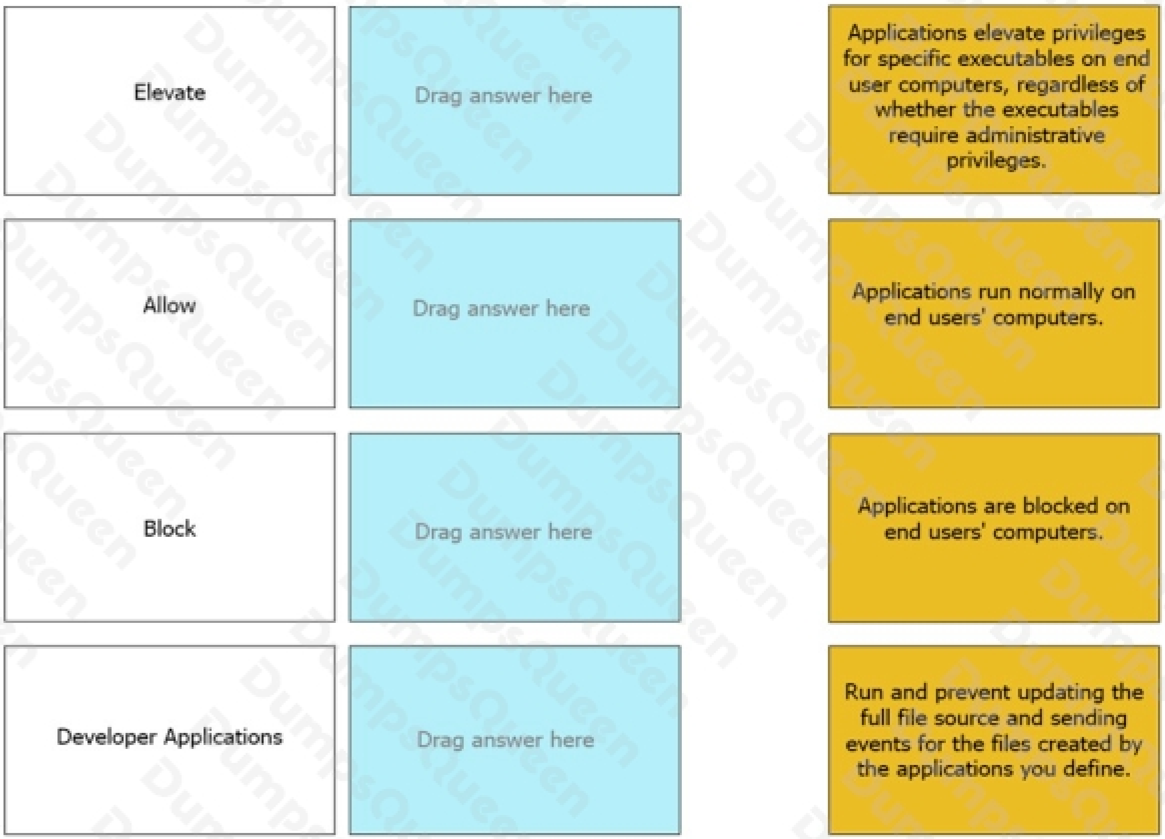
C. Threat Protection policies requires an additional agent to be installed.

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

ANSWER: A B

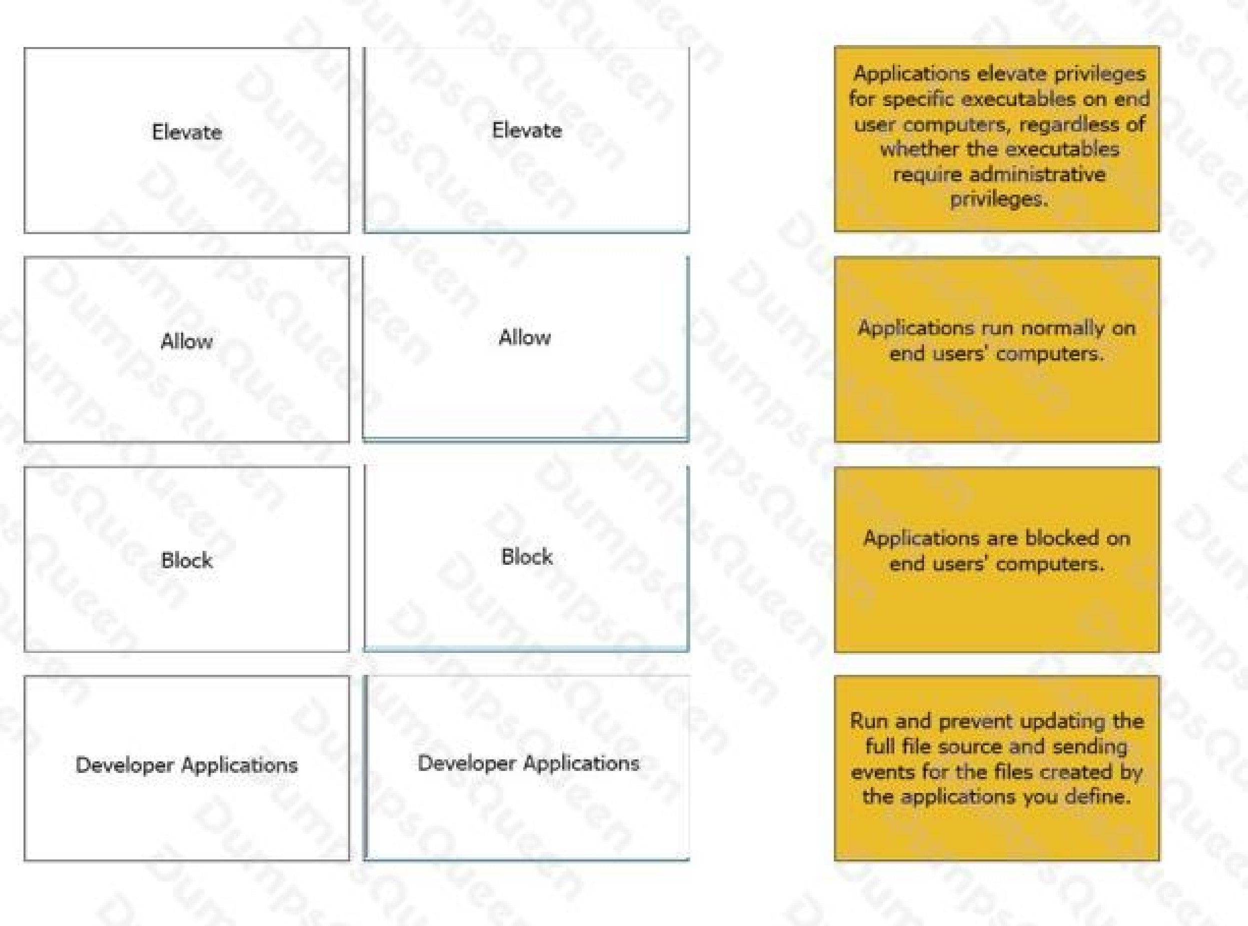
QUESTION NO: 7 - (DRAG DROP)

Match the Application Groups policy to their correct description.



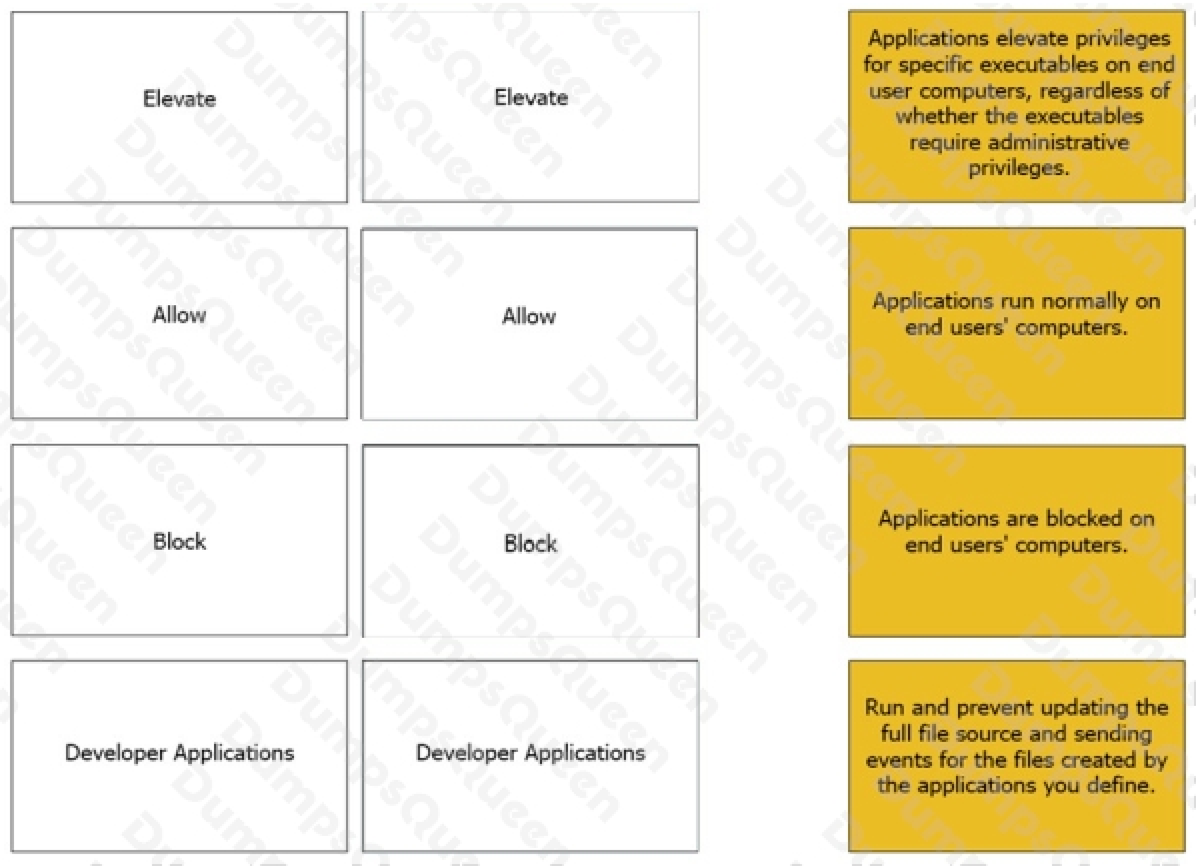
Elevate	Drag answer here	Applications elevate privileges for specific executables on end user computers, regardless of whether the executables require administrative privileges.
Allow	Drag answer here	Applications run normally on end users' computers.
Block	Drag answer here	Applications are blocked on end users' computers.
Developer Applications	Drag answer here	Run and prevent updating the full file source and sending events for the files created by the applications you define.

ANSWER:



Elevate	Elevate	Applications elevate privileges for specific executables on end user computers, regardless of whether the executables require administrative privileges.
Allow	Allow	Applications run normally on end users' computers.
Block	Block	Applications are blocked on end users' computers.
Developer Applications	Developer Applications	Run and prevent updating the full file source and sending events for the files created by the applications you define.

Explanation:



Elevate	Elevate	Applications elevate privileges for specific executables on end user computers, regardless of whether the executables require administrative privileges.
Allow	Allow	Applications run normally on end users' computers.
Block	Block	Applications are blocked on end users' computers.
Developer Applications	Developer Applications	Run and prevent updating the full file source and sending events for the files created by the applications you define.

QUESTION NO: 8

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

ANSWER: A

Explanation:

Reference: https://docs.cyberark.com/Product-Doc/OnlineHelp/EPM/Latest/en/Content/EPM/Server%20User%20Guide/PrivMgmnt-Ransomware-NewUI.htm

QUESTION NO: 9

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

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 NO: 10

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

A. EPM Agent

B. EPM Server

C. EPM API

D. EPM Discovery

ANSWER: B

Explanation:

Reference: https://docs.cyberark.com/Product-Doc/OnlineHelp/EPM/Latest/en/Content/Policies/CredentialsRotation-NewUI.htm