CyberArk

Exam EPM-DEF

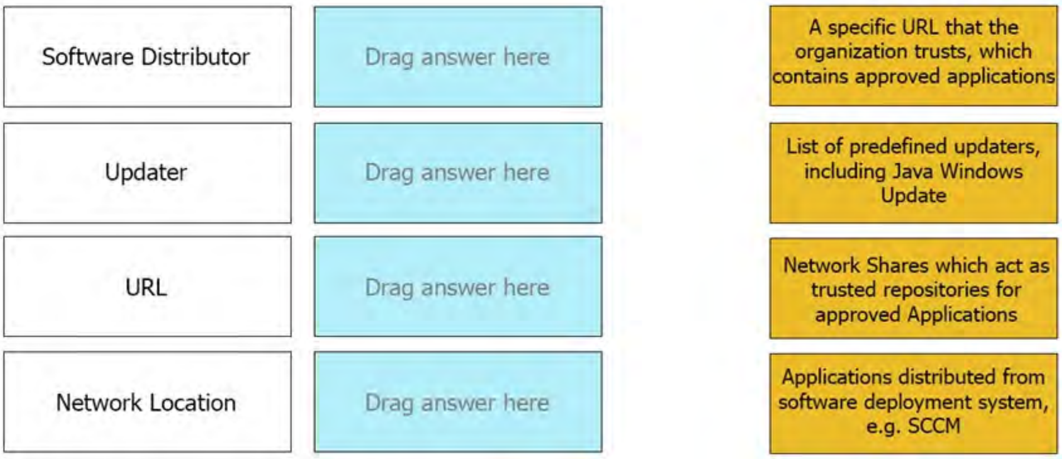
CyberArk Defender - EPM

Version: 3.0

[Total Questions: 60]

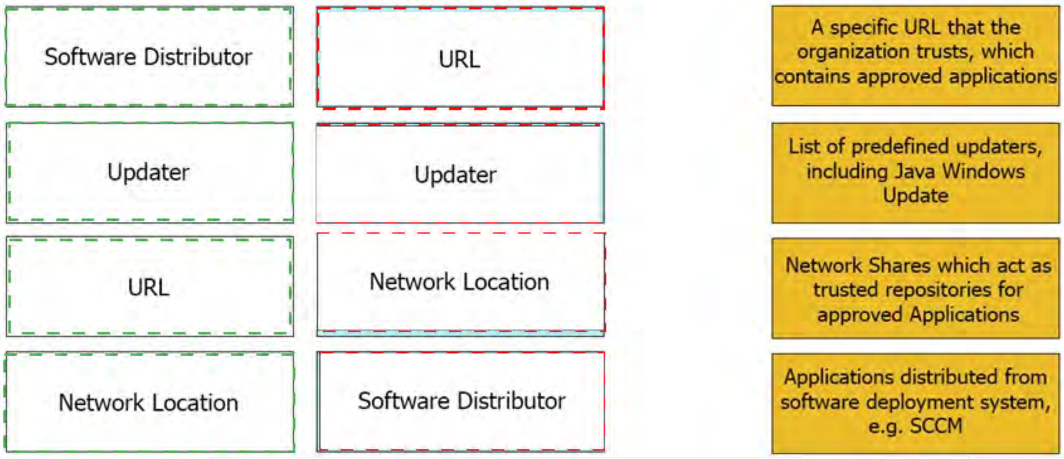
Question No : 1 DRAG DROP

Match the Trusted Source to its correct definition:



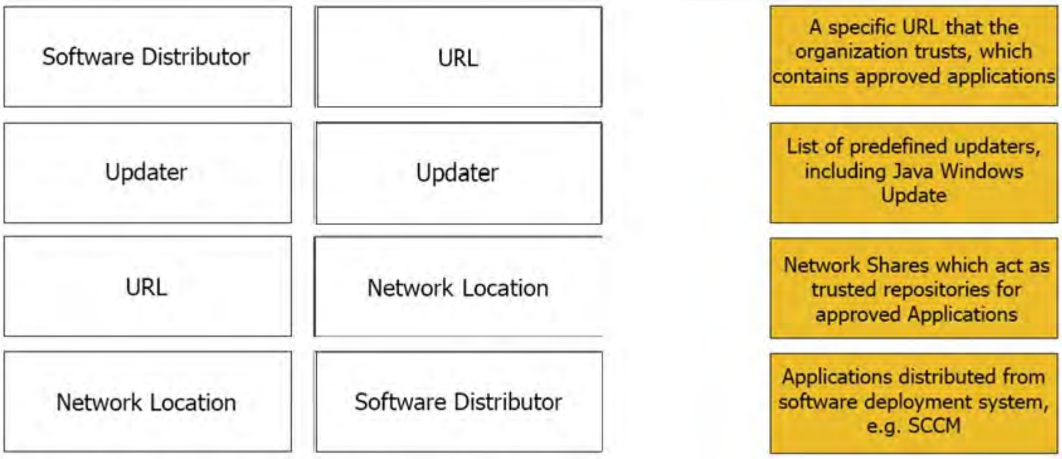
Software Distributor	Drag answer here	A specific URL that the organization trusts, which contains approved applications
Updater	Drag answer here	List of predefined updaters, including Java Windows Update
URL	Drag answer here	Network Shares which act as trusted repositories for approved Applications
Network Location	Drag answer here	Applications distributed from software deployment system, e.g. SCCM

Answer:



Software Distributor	URL	A specific URL that the organization trusts, which contains approved applications
Updater	Updater	List of predefined updaters, including Java Windows Update
URL	Network Location	Network Shares which act as trusted repositories for approved Applications
Network Location	Software Distributor	Applications distributed from software deployment system, e.g. SCCM

Explanation:



Software Distributor	URL	A specific URL that the organization trusts, which contains approved applications
Updater	Updater	List of predefined updaters, including Java Windows Update
URL	Network Location	Network Shares which act as trusted repositories for approved Applications
Network Location	Software Distributor	Applications distributed from software deployment system, e.g. SCCM

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

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

Answer: B

Question No : 4

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

Answer: D

Question No : 5

An EPM Administrator is looking to enable the Threat Deception feature, under what section should the EPM Administrator go to enable this feature?

A. Threat Protection Inbox

B. Policies
C. Threat Intelligence
D. Policy Audit

Answer: B

Question No : 6

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.

Answer: C

Question No : 7

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.

Answer: D

Question No : 8

After a clean installation of the EPM agent, the local administrator password is not being changed on macOS and the old password can still be used to log in.

What is a possible cause?

A. Secure Token on macOS endpoint is not enabled.
B. EPM agent is not able to connect to the EPM server.
C. After installation, Full Disk Access for the macOS agent to support EPM policies was not approved.
D. Endpoint password policy is too restrictive.

Answer: A

Question No : 9

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

Answer: D

Question No : 10

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 : 11

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.

Answer: C

Question No : 12

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

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

Answer: D

Question No : 13

If you want to diagnose agent EPM agent connectivity issues, what is the agent executable that can be used from the command line?

A. vf_agent.exe
B. epm_agent.exe
C. vault_agent.exe
D. db_agent.exe

Answer: B

Question No : 14

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

Answer: D

Question No : 15

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

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 No : 16

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

Answer: D

Question No : 17

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

Answer: D

Reference: https://docs.cyberark.com/Product-Doc/OnlineHelp/EPM/Latest/en/Content/EndUser/EndUserDialogs.htm

Question No : 18

Can the EPM Set Administrator configure Audit Dialog Pop-ups for the Record Audit Video option?

A. Yes, when Audit Video recording started, when Audit Video recording stopped, and when Audit Recording video reached size limit.
B. Yes, when Audit Video recording started, when not enough disk space to start the video recording, and when video recording is initializing.
C. Yes, when Audit Video recording started, when Audit Video recording is uploaded to the EPM server, and when audit recording cannot be initialized.
D. No, Audit Video is only available without the possibility of having End-User dialog pop-ups.

Answer: D

Question No : 19

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.

Answer: B

Question No : 20

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.