250-438 Q&As

Administration of Symantec Data Loss Prevention 15

Pass Symantec 250-438 Exam with 100% Guarantee

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

https://www.certbus.com/250-438.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

When managing an Endpoint Discover scan, a DLP administrator notices some endpoint computers are NOT completing their scans. When does the DLP agent stop scanning?

A. When the agent sends a report within the "Scan Idle Timeout" period

B. When the endpoint computer is rebooted and the agent is started

C. When the agent is unable to send a status report within the "Scan Idle Timeout" period

D. When the agent sends a report immediately after the "Scan Idle Timeout" period

Correct Answer: C

QUESTION 2

A DLP administrator has enabled and successfully tested custom attribute lookups for incident data based on the Active Directory LDAP plugin. The Chief Information Security Officer (CISO) has attempted to generate a User Risk Summary report, but the report is empty. The DLP administrator confirms the Cisco\\'s role has the "User Reporting" privilege enabled, but User Risk reporting is still not working.

What is the probable reason that the User Risk Summary report is blank?

A. Only DLP administrators are permitted to access and view data for high risk users.

B. The Enforce server has insufficient permissions for importing user attributes.

C. User attribute data must be configured separately from incident data attributes.

D. User attributes have been incorrectly mapped to Active Directory accounts.

Correct Answer: D

QUESTION 3

What is the correct configuration for "BoxMonitor.Channels" that will allow the server to start as a Network Monitor server?

A. Packet Capture, Span Port

B. Packet Capture, Network Tap

C. Packet Capture, Copy Rule

D. Packet capture, Network Monitor

Correct Answer: C

Reference: https://support.symantec.com/en_US/article.TECH218980.html

QUESTION 4

What detection technology supports partial contents matching?

A. Indexed Document Matching (IDM)

B. Described Content Matching (DCM)

C. Exact Data Matching (EDM)

D. Optical Character Recognition (OCR)

Correct Answer: A

Reference: https://help.symantec.com/cs/dlp15.1/DLP/v115965297_v125428396/Mac-agent-detection-technologies?locale=EN_US

QUESTION 5

A DLP administrator has added several approved endpoint devices as exceptions to an Endpoint Prevent policy that blocks the transfer of sensitive data. However, data transfers to these devices are still being blocked. What is the first action an administrator should take to enable data transfers to the approved endpoint devices?

A. Disable and re-enable the Endpoint Prevent policy to activate the changes

B. Double-check that the correct device ID or class has been entered for each device

C. Verify Application File Access Control (AFAC) is configured to monitor the specific application

D. Edit the exception rule to ensure that the "Match On" option is set to "Attachments"

Correct Answer: D

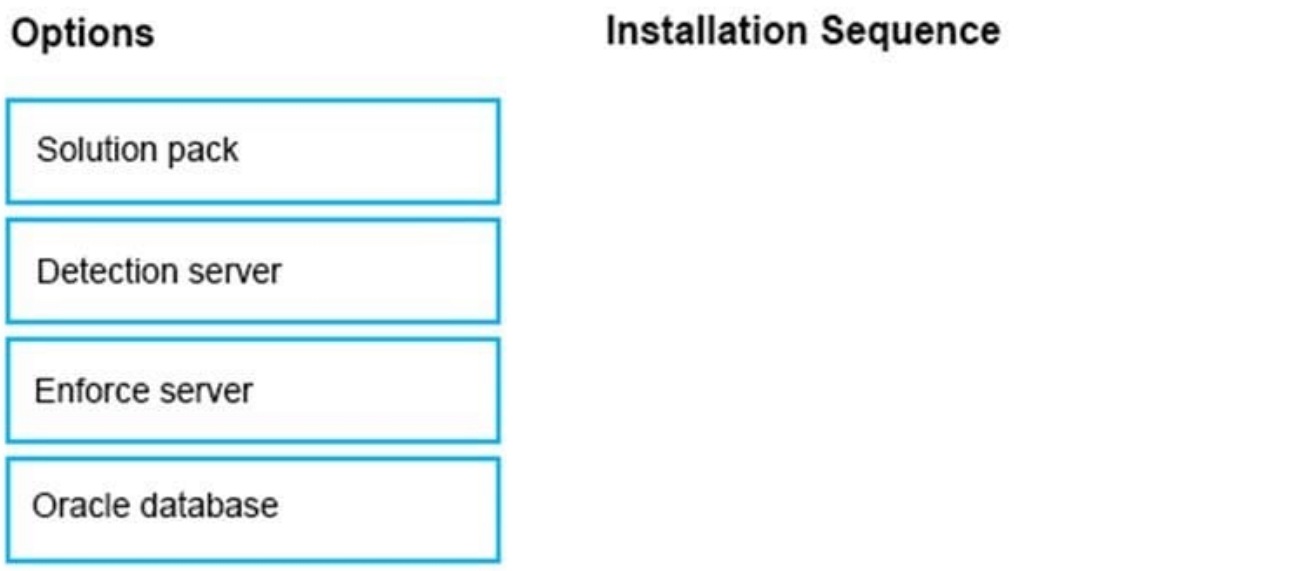
QUESTION 6

DRAG DROP

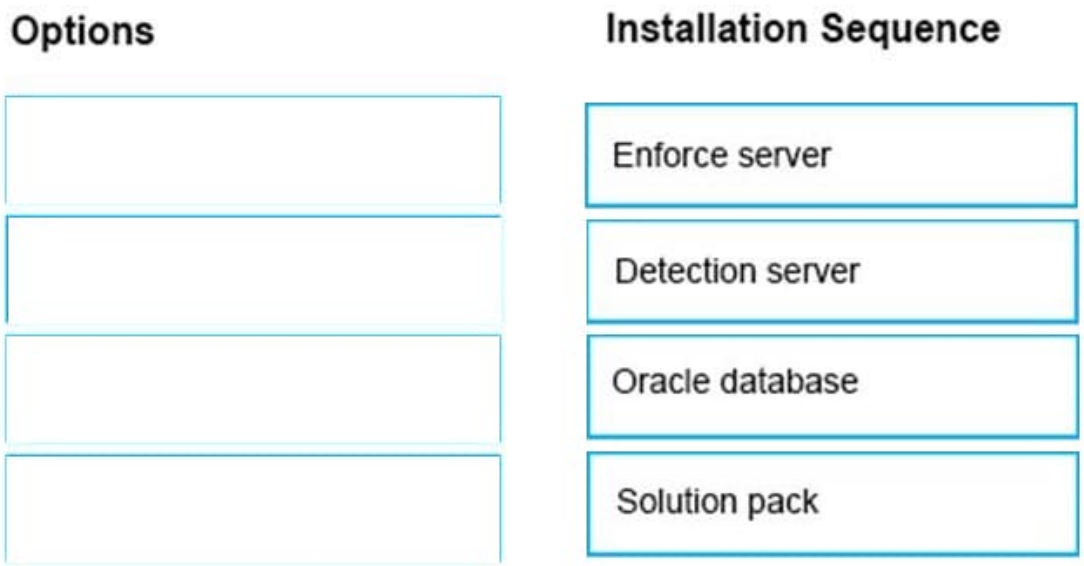
What is the correct installation sequence for the components shown here, according to the Symantec Installation Guide?

Place the options in the correct installation sequence.

Select and Place:



Correct Answer:



QUESTION 7

Which two actions are available for a "Network Prevent: Remove HTTP/HTTPS content" response rule when the content is unable to be removed? (Choose two.)

A. Allow the content to be posted

B. Remove the content through FlexResponse

C. Block the content before posting

D. Encrypt the content before posting

E. Redirect the content to an alternative destination

Correct Answer: AE

QUESTION 8

A DLP administrator has performed a test deployment of the DLP 15.0 Endpoint agent and now wants to uninstall the agent. However, the administrator no longer remembers the uninstall password. What should the administrator do to work around the password problem?

A. Apply a new global agent uninstall password in the Enforce management console.

B. Manually delete all the Endpoint agent files from the test computer and install a new agent package.

C. Replace the PGPsdk.dll file on the agent\\'s assigned Endpoint server with a copy from a different Endpoint server

D. Use the UninstallPwdGenerator to create an UninstallPasswordKey.

Correct Answer: D

QUESTION 9

A DLP administrator determines that the \SymantecDLP\Protect\Incidents folder on the Enforce server contains. BAD files dated today, while other. IDC files are flowing in and out of the \Incidents directory. Only .IDC files larger than 1MB are

turning to .BAD files.

What could be causing only incident data smaller than 1MB to persist while incidents larger than 1MB change to .BAD files?

A. A corrupted policy was deployed.

B. The Enforce server\\'s hard drive is out of space.

C. A detection server has excessive filereader restarts.

D. Tablespace is almost full.

Correct Answer: D

QUESTION 10

Why is it important for an administrator to utilize the grid scan feature?

A. To distribute the scan workload across multiple network discover servers

B. To distribute the scan workload across the cloud servers

C. To distribute the scan workload across multiple endpoint servers

D. To distribute the scan workload across multiple detection servers

Correct Answer: D

If you plan to use the grid scanning feature to distribute the scanning workload across multiple detection servers, retain the default value (1)

QUESTION 11

A DLP administrator needs to remove an agent its associated events from an Endpoint server.

Which Agent Task should the administrator perform to disable the agent\\'s visibility in the Enforce management console?

A. Delete action from the Agent Health dashboard

B. Delete action from the Agent List page

C. Disable action from Symantec Management Console

D. Change Endpoint Server action from the Agent Overview page

Correct Answer: C

QUESTION 12

Where in the Enforce management console can a DLP administrator change the "UI.NO_SCAN.int" setting to disable the "Inspecting data" pop-up?

A. Advanced Server Settings from the Endpoint Server Configuration

B. Advanced Monitoring from the Agent Configuration

C. Advanced Agent Settings from the Agent Configuration

D. Application Monitoring from the Agent Configuration

Correct Answer: C

Reference: https://www.symantec.com/connect/forums/dlp-pop-examining-content

QUESTION 13

A DLP administrator needs to stop the PacketCapture process on a detection server. Upon inspection of the Server Detail page, the administrator discovers that all processes are missing from the display. What are the processes missing from the Server Detail page display?

A. The Display Process Control setting on the Advanced Settings page is disabled.

B. The Advanced Process Control setting on the System Settings page is deselected.

C. The detection server Display Control Process option is disabled on the Server Detail page.

D. The detection server PacketCapture process is displayed on the Server Overview page.

Correct Answer: B

Reference: https://support.symantec.com/content/unifiedweb/en_US/article.TECH220250.html

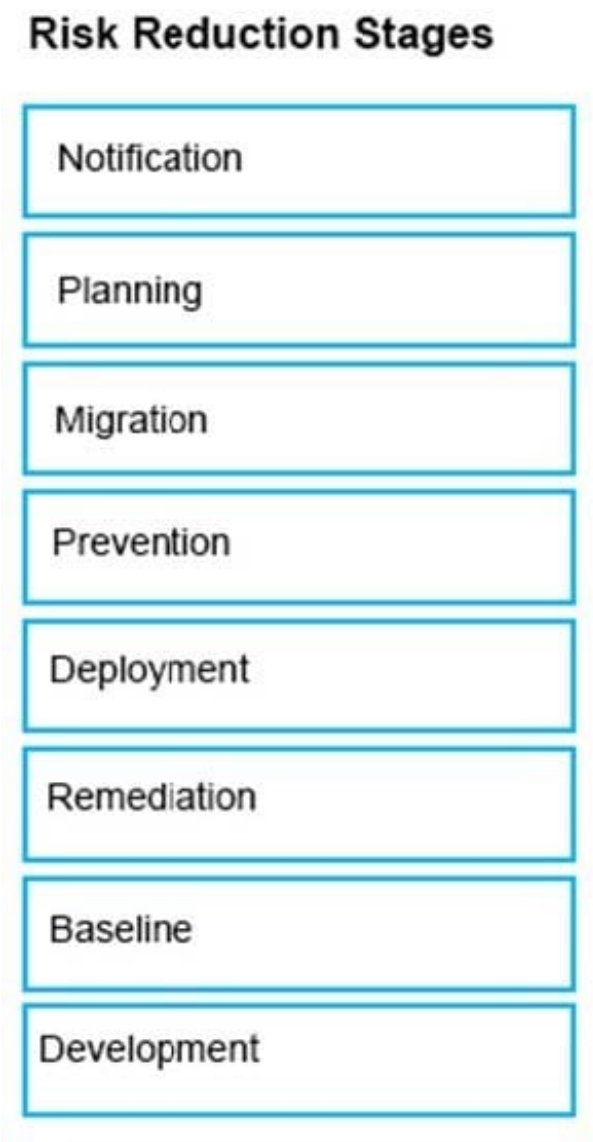
QUESTION 14

DRAG DROP

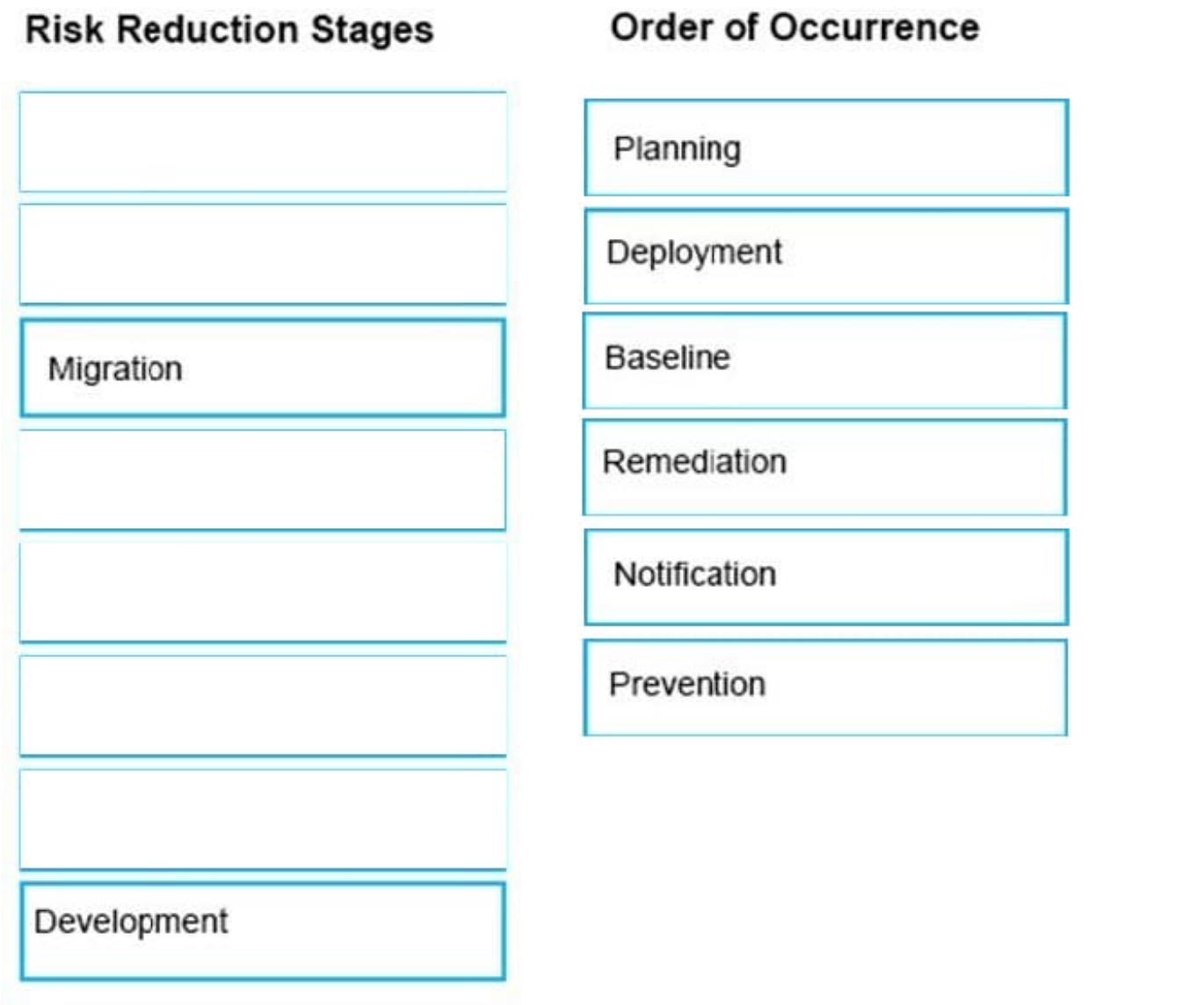
The Symantec Data Loss risk reduction approach has six stages.

Drag and drop the six correct risk reduction stages in the proper order of Occurrence column.

Select and Place:



Correct Answer:



Reference: https://www.slideshare.net/iftikhariqbal/symantec-data-loss-prevention-technical-proposal-general

QUESTION 15

Which channel does Endpoint Prevent protect using Device Control?

A. Bluetooth

B. USB storage

C. CD/DVD

D. Network card

Correct Answer: B

Reference: https://support.symantec.com/en_US/article.HOWTO80865.html#v36651044

250-438 VCE Dumps 250-438 Study Guide 250-438 Exam Questions