Total Question: 70 QAs

Question: 1

A DLP administrator is preparing to install Symantec DLP and has been asked to use an Oracle database provided by the Database Administration team.

Which SQL *Plus command should the administrator utilize to determine if the database is using a supported version of Oracle?

A. select database version from <database name>;

B. select * from db$version;

C. select * from v$version;

D. select db$ver from <database name>;

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 attributed.

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

Answer: D

Question: 3

Which two Network Discover/Cloud Storage targets apply Information Centric Encryption as policy response rules?

A. Microsoft Exchange

B. Windows File System

C. SQL Databases

D. Microsoft SharePoint

E. Network File System (NFS)

Answer: A,D

Question: 4

A company needs to implement Data Owner Exception so that incidents when employees send or receive their own personal information.

What detection method should the company use?

A. Indexed Document Matching (IDM)

B. Vector Machine Learning (VML)

C. Exact data matching (EDM)

D. Described Content matching (DCM)

Answer: C

Question: 5
What detection method utilizes Data Identifiers?
A. Indexed Document matching (IDM)
B. Described Content Matching (DCM)
C. Directory Group Matching (DGM)
D. Exact Data Matching (EDM)
Answer: D

Question: 6
What detection server is used for Network Discover, Network Protect, and Cloud Storage?
A. Network Protect Storage Discover
B. Network Discover/Cloud Storage Discover
C. Network Prevent/Cloud Detection Service
D. Network Protect/Cloud Detection Service
Answer: B

Question: 7
A DLP administrator is testing Network Prevent for Web functionality. When the administrator posts a small test file to a cloud storage website, no new incidents are reported.
What should the administrator do to allow incidents to be generated against this file?
A. Change the “Ignore requests Smaller Than” value to 1
B. Add the filename to the Inspect Content Type field
C. Change the “PacketCapture.DISCARD_HTTP_GET” value to “false”
D. Uncheck trial mode under the ICAP tab
Answer: A

Question: 8
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
Answer: A,E

Question: 9
Which two technologies should an organization utilize for integration with the Network Prevent products? (choose two.)
A. Network Tap
B. Network Firewall
C. Proxy Server

D. Mail Transfer Agent
E. Encryption Appliance
Answer: C,D

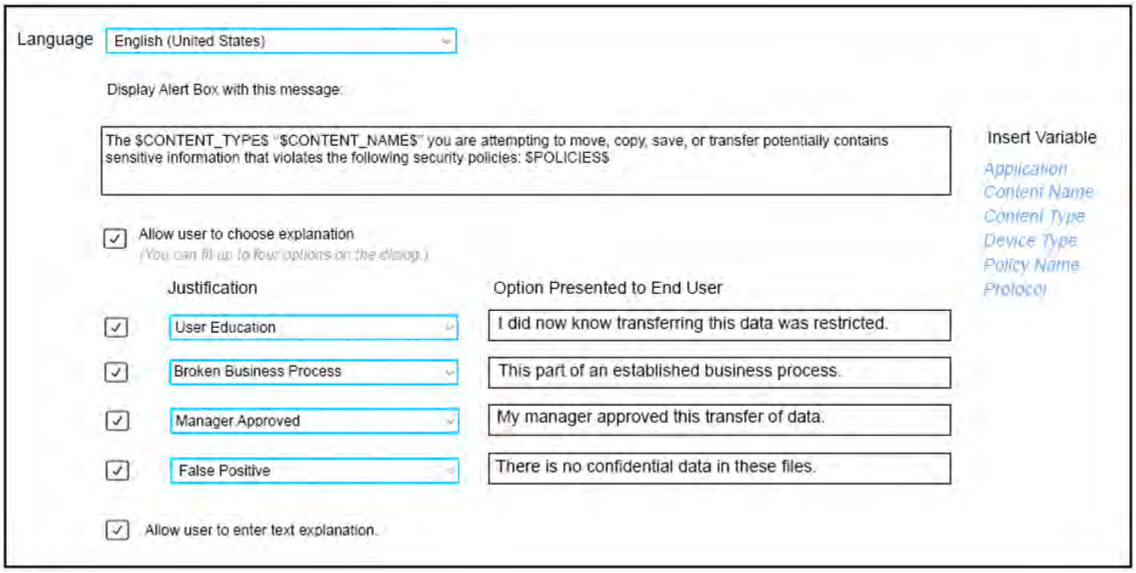
Question: 10
Which detection server is available from Symantec as a hardware appliance?
A. Network Prevent for Email
B. Network Discover
C. Network Monitor
D. Network Prevent for Web
Answer: D

Question: 11
What detection technology supports partial contents matching?
A. Indexed Document Matching (IDM)
B. Described Content Matching (DCM)
C. Exact Data Matching (DCM)
D. Optical Character Recognition (OCR)
Answer: A

Question: 12
A software company wants to protect its source code, including new source code created between scheduled indexing runs.
Which detection method should the company use to meet this requirement?
A. Exact Data Matching (EDM)
B. Described Content Matching (DCM)
C. Vector Machine Learning (VML)
D. Indexed Document Matching (IDM)
Answer: D

Question: 13
Which product is able to replace a confidential document residing on a file share with a marker file explaining why the document was removed?
A. Network Discover
B. Cloud Service for Email
C. Endpoint Prevent
D. Network Protect
Answer: D

Question: 14
Refer to the exhibit. Which type of Endpoint response rule is shown?



Language: English (United States)

Display Alert Box with this message:

The $CONTENT_TYPES "$CONTENT_NAME$" you are attempting to move, copy, save, or transfer potentially contains sensitive information that violates the following security policies: $POLICIES$

☑ Allow user to choose explanation
(You can fill up to four options on the dialog.)

	Justification	Option Presented to End User
☑	User Education	I did now know transferring this data was restricted.
☑	Broken Business Process	This part of an established business process.
☑	Manager Approved	My manager approved this transfer of data.
☑	False Positive	There is no confidential data in these files.

☑ Allow user to enter text explanation.

A. Endpoint Prevent: User Notification
B. Endpoint Prevent: Block
C. Endpoint Prevent: Notify
D. Endpoint Prevent: User Cancel
Answer: B

Question: 15
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
Answer: C

Question: 16
A compliance officer needs to understand how the company is complying with its data security policies over time.
Which report should be compliance officer generate to obtain the compliance information?
A. Policy report, filtered on date and summarized by policy
B. Policy Trend report, summarized by policy, then quarter
C. Policy report, filtered on quarter and summarized by policy
D. Policy Trend report, summarized by policy, then severity
Answer: A

Question: 17
Under the "System Overview" in the Enforce management console, the status of a Network Monitor detection server is shown as "Running Selected." The Network Monitor server's event logs indicate that the packet capture and filereader processes are crashing.
What is a possible cause for the Network Monitor server being in this state?

A. There is insufficient disk space on the Network Monitor server.
B. The Network Monitor server's certificate is corrupt or missing.
C. The Network Monitor server's license file has expired.
D. The Enforce and Network Monitor servers are running different versions of DLP.
Answer: D

Question: 18
Which two detection technology options ONLY run on a detection server? (Choose two.)
A. Form Recognition
B. Indexed Document matching (IDM)
C. Described Content Matching (DCM)
D. Exact data matching (EDM)
E. vector Machine Learning (VML)
Answer: B,D

Question: 19
Which two components can perform a file system scan of a workstation? (Choose two.)
A. Endpoint Server
B. DLP Agent
C. Network Prevent for Web Server
D. Discover Server
E. Enforce Server
Answer: B,D

Question: 20
Which two locations can Symantec DLP scan and perform Information Centric Encryption (ICE) actions on? (Choose two.)
A. Exchange
B. Jiveon
C. File store
D. SharePoint
E. Confluence
Answer: C,D

Question: 21
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
Answer: C

Question: 22