

KillTest

Higher Quality, Better Service!



Q&A

<http://www.killtest.com>

We offer free update service for one year.

Exam : **ST0-093**

Title : Symantec Data Loss
Prevention 10.5 (STS)

Version : Demo

1.Which information is recommended to be included in an Exact Data Matching (EDM) data source?

- A. date fields
- B. numeric fields with fewer than five digits
- C. column names in the first row
- D. country, state, or province names

Answer: C

2.What must a policy manager do when working with Exact Data Matching (EDM) indexes?

- A. re-index large data sources on a daily or weekly basis
- B. index the original data source on the detection server
- C. deploy the index only to specific detection servers
- D. create a new data profile if data source schema changes

Answer: D

3.Which two protocols are available by default and recognized by Network Monitor by their individual signatures? (Select two.)

- A. FTP
- B. HTTPS
- C. IM: AIM
- D. SNMP
- E. TFTP

Answer: A,C

4.What does Network Monitor use to identify network traffic going to a nonstandard port?

- A. string matching
- B. port range
- C. either UDP or TCP
- D. protocol signature

Answer: D

5.Which detection server can block file transfer protocol (FTP) requests?

- A. Network Monitor Server
- B. FTP Prevent Server
- C. Web Prevent Server
- D. Endpoint Prevent Server

Answer: C

6.Which server encrypts the message when using a Modify SMTP Message response rule?

- A. Encryption Gateway
- B. SMTP Prevent Server
- C. MTA Server
- D. Enforce Server

Answer: A

7.What must a Data Loss Prevention administrator recycle for Network Monitor filter configuration changes to take effect?

- A. VontuMonitorController
- B. PacketCapture
- C. FileReader
- D. Network Monitor

Answer: D

8.What are two available options when accessing the Configure Server page to configure protocol filters? (Select two.)

- A. HTTPS
- B. FTP
- C. SMTP
- D. ICMP
- E. UDP

Answer: B,C

9.What should be used to exclude email going to any email address in the partner.com domain?

- A. IP filter
- B. L7 filter
- C. Content filter
- D. Sender/User Matches pattern

Answer: B

10.Which products run on the same detection server?

- A. Network Protect and Network Discover
- B. Endpoint Discover and Network Discover
- C. Network Monitor and Network Prevent
- D. Network Discover and Network Monitor

Answer: A

11.What is the primary function of Endpoint Prevent?

- A. encrypts confidential data being sent over the network or copied to removable media
- B. finds confidential data and quarantines the data to a central repository
- C. disables end-user devices that are unauthorized by a company's data security policies
- D. stops confidential data from being sent over the network or copied to removable media

Answer: A

12.What is a function of the Enforce Server?

- A. policy creation
- B. detection of incidents
- C. inspection of network communication
- D. identification of confidential data in repositories

Answer: A

13.Which two actions are associated with FlexResponse? (Select two.)

- A. manually quarantine files
- B. automatically quarantine files on file shares
- C. modify a response within a policy
- D. automatically quarantine files on endpoints
- E. apply digital rights to content

Answer: A,E

14.Where does an incident responder find the exact matches that triggered an incident?

- A. Incident Dashboard
- B. Incident Snapshot
- C. Incident List
- D. Incident Summary Report

Answer: B

15.Which feature is a key benefit of on-screen notification?

- A. uses on-screen notification in different languages
- B. educates the user about the violation that has occurred
- C. stops the movement of data that violates policies
- D. notifies the user that the Endpoint Agent is active

Answer: D

16.Which product lets an incident responder see who has access to confidential files on a public file share?

- A. Network Protect
- B. Endpoint Discover
- C. Endpoint Prevent
- D. Network Discover

Answer: D

17.The user interface (UI) will be used to upgrade to Symantec Data Loss Prevention 10.5. A Data Loss Prevention administrator will be logging in to the Enforce Server from a desktop to perform the upgrade. The Vontu\Protect\config\Manager.properties file is set to default settings. Which port must be open to connect to the upgrader application?

- A. 8080
- B. 8090
- C. 8100
- D. 8300

Answer: D

18.To which file system folder does PacketCapture write reconstructed SMTP messages?

- A. drop
- B. drop_pcap

C. drop_discover

D. drop_smtp

Answer: B

19.What is the sequence of message processing for Network Monitor?

A. Packet Capture -> File Reader -> Detection -> Incident Writer

B. Monitor Controller -> Detection -> File Reader -> Incident Writer

C. File Reader -> IncidentPersister -> Manager -> Notifier

D. Request Processor -> Packet Capture -> File Reader -> Detection

Answer: A

20.Which component has an obfuscated (hidden) log?

A. Endpoint Agent

B. Enforce Server

C. Network Monitor

D. Network Discover

Answer: D