

IT 认证电子书



质 量 更 高 服 务 更 好

半年免费升级服务

<http://www.itrenzheng.com>

Exam: **250-510**

Title : Administration of
Symantec™ Data Loss
Prevention 10.5 - BETA

Version : DEMO

1. Which two products can be run on virtual servers? (Select two.)

- A.Endpoint Discover
- B.Endpoint Prevent
- C.Network Monitor
- D.Enforce
- E.Network Prevent

Answer: DE

2. How is the incident count for a new system managed in order to avoid overwhelming the incident response team?

- A.Match count thresholds are set.
- B.More than one policy is enabled.
- C.Many incident responders are allowed access to the system.
- D.Incidents are auto-filtered to hide false positives.

Answer: A

3. Which response rule action will be ignored when using an Exact Data Matching (EDM) policy?

- A.Endpoint: Notify
- B.Network: Block HTTP/HTTPS
- C.Protect: Quarantine File
- D.Network: Remove HTTP/HTTPS Content

Answer: A

4. Which two recommendations should an organization follow when deploying Endpoint Prevent? (Select two.)

- A.test the agent on a variety of end-user images
- B.initially enable monitoring of the local file system
- C.enable monitoring of many destinations and protocols simultaneously
- D.configure, test, and tune filters
- E.configure blocking as soon as the agents are deployed

Answer: AD

5. Which plug-in can connect to Microsoft Active Directory (AD)?

- A.CSV Lookup
- B.Live LDAP Lookup
- C.Active Directory Integration Lookup
- D.Directory Server Lookup

Answer: B

6. 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

7. What are two valid reasons for adding notes to incidents? (Select two.)

- A.to provide incident detail to policy violators
- B.to allow the next responder to more quickly prioritize incidents for review
- C.to allow the next responder to more quickly understand the incident history
- D.to provide detail when closing an incident
- E.to provide incident detail for report filtering

Answer: CD

8. What must be running on a Linux Enforce server to enable the Symantec Data Loss Prevention user interface?

- A.selinux
- B.iptables
- C.xwindows
- D.ssh

Answer: B

9. Which file on the endpoint machine stores messages that are temporarily cached when using two-tier policies such as IDM or EDM?

- A.is.ead
- B.ttds.ead
- C.ks.ead
- D.cg.ead

Answer: B

10. Which detection server setting enables detecting text within markup language tags?

- A.ContentExtraction.MarkupAsText
- B.ContentExtraction.EnableMetaData
- C.Detection.EncodingGuessingEnabled
- D.Lexer.Validate

Answer: A

11. What are two benefits that data loss prevention solutions provide? (Select two.)

- A.provides accurate measurement of encrypted outgoing email
- B.gives insight into capacity planning for sensitive data
- C.identifies who has access to sensitive data
- D.indicates where sensitive data is being sent
- E.measures encryption strength for sensitive data

Answer: CD

12. What are two examples of confidential data? (Select two.)

- A.manufacturing plant locations
- B.published press releases
- C.stock performance history
- D.CAD drawings

E.employee health information

Answer: DE

13. Which two statements describe an effective data loss prevention (DLP) program? (Select two.)

A.DLP is best implemented as a departmental initiative.

B.DLP is primarily driven by the network team.

C.An incident response team is rarely required.

D.Employee education is important.

E.Business stakeholders are held accountable for risk reduction.

Answer: DE

14. Which two products are required for quarantining confidential files residing inappropriately on a public file share? (Select two.)

A.Network Discover

B.Endpoint Discover

C.Network Monitor

D.Network Prevent

E.Network Protect

Answer: AE

15. Which product can replace a confidential document residing on a share with a marker file explaining why the document was removed?

A.Network Discover

B.Network Protect

C.Endpoint Prevent

D.Endpoint Discover

Answer: B

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. 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

18. 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

19. 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

20. 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: AE