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.pass2lead.com/250-438.html

100% Passing Guarantee
100% Money Back Assurance

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

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

What should an incident responder select in the Enforce management console to remediate multiple incidents simultaneously?

A. Smart Response on the Incident page

B. Automated Response on the Incident Snapshot page

C. Smart Response on an Incident List report

D. Automated Response on an Incident List report

Correct Answer: B

QUESTION 2

How should a DLP administrator change a policy so that it retains the original file when an endpoint incident has detected a "copy to USB device" operation?

A. Add a "Limit Incident Data Retention" response rule with "Retain Original Message" option selected.

B. Modify the agent config.db to include the file

C. Modify the "Endpoint_Retain_Files.int" setting in the Endpoint server configuration

D. Modify the agent configuration and select the option "Retain Original Files"

Correct Answer: A

QUESTION 3

Which two Infrastructure-as-a-Service providers are supported for hosting Cloud Prevent for Office 365? (Choose two.)

A. Any customer-hosted private cloud

B. Amazon Web Services

C. ATandT

D. Verizon

E. Rackspace

Correct Answer: BE

Reference: https://symwisedownload.symantec.com//resources/sites/SYMWISE/content/live/DOCUMENTATION/8000/DOC8244/en_US/Symantec_DLP_15.0_Cloud_Prevent_O365.pdf?__gda__=1554430310_584ffada3918e15ced8b6483a2bfb6fb (14)

QUESTION 4

Which two detection technology options run on the DLP agent? (Choose two.)

A. Optical Character Recognition (OCR)

B. Described Content Matching (DCM)

C. Directory Group Matching (DGM)

D. Form Recognition

E. Indexed Document Matching (IDM)

Correct Answer: BE

QUESTION 5

An organization wants to restrict employees to copy files only a specific set of USB thumb drives owned by the organization. Which detection method should the organization use to meet this requirement?

A. Exact Data Matching (EDM)

B. Indexed Document Matching (IDM)

C. Described Content Matching (DCM)

D. Vector Machine Learning (VML)

Correct Answer: D

QUESTION 6

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 7

Which server target uses the "Automated Incident Remediation Tracking" feature in Symantec DLP?

A. Exchange

B. File System

C. Lotus Notes

D. SharePoint

Correct Answer: B

Reference: https://help.symantec.com/cs/DLP15.0/DLP/v83981880_v120691346/Troubleshooting-automated-incident-remediation-tracking?locale=EN_US

QUESTION 8

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

Correct Answer: CD

Reference: https://www.symantec.com/connect/articles/network-prevent

QUESTION 9

Which action is available for use in both Smart Response and Automated Response rules?

A. Log to a Syslog Server

B. Limit incident data retention

C. Modify SMTP message

D. Block email message

Correct Answer: D

QUESTION 10

What detection technology supports partial row matching?

A. Vector Machine Learning (VML)

B. Indexed Document Matching (IDM)

C. Described Content Matching (DCM)

D. Exact Data Matching (EDM)

Correct Answer: D

Reference: https://www.slideshare.net/iftikhariqbal/technology-overview-symantec-data-loss-prevention-dlp

QUESTION 11

Which statement accurately describes where Optical Character Recognition (OCR) components must be installed?

A. The OCR engine must be installed on detection server other than the Enforce server.

B. The OCR server software must be installed on one or more dedicated (non-detection) Linux servers.

C. The OCR engine must be directly on the Enforce server.

D. The OCR server software must be installed on one or more dedicated (non-detection) Windows servers.

Correct Answer: C

Reference: https://help.symantec.com/cs/dlp15.0/DLP/v122760174_v120691346/Setting-up-OCR-Servers?locale=EN_US

QUESTION 12

Which tool must a DLP administrator run to certify the database prior to upgrading DLP?

A. Lob_Tablespace Reclamation Tool

B. Upgrade Readiness Tool

C. SymDiag

D. EnforceMigrationUtility

Correct Answer: B

Reference: https://support.symantec.com/en_US/article.DOC10667.html

QUESTION 13

A customer needs to integrate information from DLP incidents into external Governance, Risk and Compliance dashboards.

Which feature should a third party component integrate with to provide dynamic reporting, create custom incident remediation processes, or support business processes?

A. Export incidents using the CSV format

B. Incident Reporting and Update API

C. Incident Data Views

D. A Web incident extraction report

Correct Answer: B

QUESTION 14

How do Cloud Detection Service and the Enforce server communicate with each other?

A. Enforce initiates communication with Cloud Detection Service, which is expecting connections on port 8100.

B. Cloud Detection Service initiates communication with Enforce, which is expecting connections on port 443.

C. Cloud Detection Service initiates communication with Enforce, which is expecting connections on port 1443.

D. Enforce initiates communication with Cloud Detection Service, which is expecting connections on port 443.

Correct Answer: D

QUESTION 15

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