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.leads4pass.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

A company needs to secure the content of all Mergers and Acquisitions Agreements However, the standard text included in all company literature needs to be excluded. How should the company ensure that this standard text is excluded from detection?

A. Create a Whitelisted.txt file after creating the Vector Machine Learning (VML) profile.

B. Create a Whitelisted.txt file after creating the Exact Data Matching (EDM) profile

C. Create a Whitelisted.txt file before creating the Indexed Document Matching (IDM) profile

D. Create a Whitelisted.txt file before creating the Exact Data Matching (EDM) profile

Correct Answer: C

Reference: https://help.symantec.com/cs/dlp15.0/DLP/v27161240_v120691346/White-listing-file-contents-to-exclude-from-partial-matching?locale=EN_US

QUESTION 2

Which service encrypts the message when using a Modify SMTP Message response rule?

A. Network Monitor server

B. SMTP Prevent

C. Enforce server

D. Encryption Gateway

Correct Answer: D

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

QUESTION 3

Which two DLP products support the new Optical Character Recognition (OCR) engine in Symantec DLP 15.0? (Choose two.)

A. Endpoint Prevent

B. Cloud Service for Email

C. Network Prevent for Email

D. Network Discover

E. Cloud Detection Service

Correct Answer: BC

QUESTION 4

What is the correct order for data in motion when a customer has integrated their CloudSOC and DLP solutions?

A. User > CloudSOC Gatelet > DLP Cloud Detection Service > Application

B. User > Enforce > Application

C. User > Enforce > CloudSOC > Application

D. User > CloudSOC Gatelet > Enforce > Application

Correct Answer: C

QUESTION 5

What detection technology supports partial contents matching?

A. Indexed Document Matching (IDM)

B. Described Content Matching (DCM)

C. Exact Data Matching (EDM)

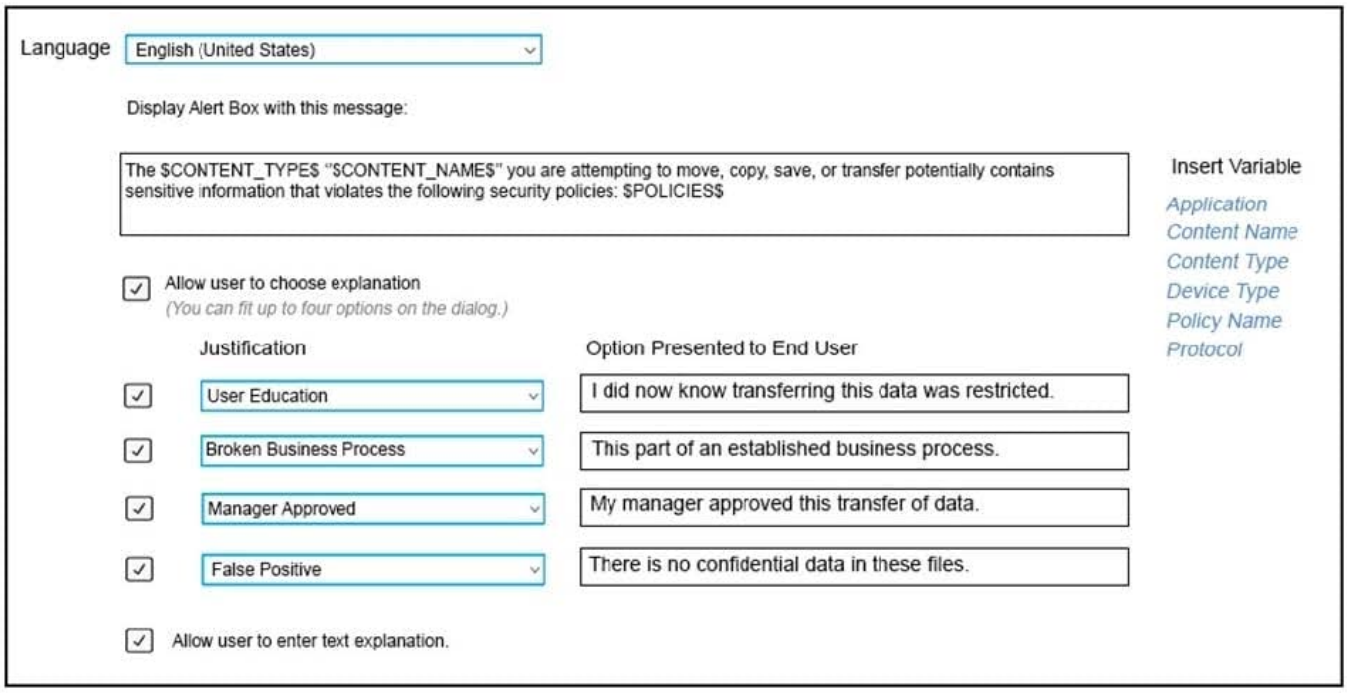
D. Optical Character Recognition (OCR)

Correct Answer: A

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

QUESTION 6

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



A. Endpoint Prevent: User Notification

B. Endpoint Prevent: Block

C. Endpoint Prevent: Notify

D. Endpoint Prevent: User Cancel

Correct Answer: B

Reference: https://help.symantec.com/cs/dlp15.0/DLP/v27595430_v120691346/Configuring-the-Endpoint-Prevent:-Block-action?locale=EN_US

QUESTION 7

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)

Correct Answer: D

Reference: https://help.symantec.com/cs/DLP15.0/DLP/v100774847_v120691346/Scheduling-remote-indexing?locale=EN_US

QUESTION 8

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 9

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

Correct Answer: D

Reference: https://help.symantec.com/cs/dlp15.0/DLP/v122938258_v120691346/Setting-up-the-DLP-S500-Appliance?locale=EN_US

QUESTION 10

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 11

What is the Symantec recommended order for stopping Symantec DLP services on a Windows Enforce server?

A. Vontu Notifier, Vontu Incident Persister, Vontu Update, Vontu Manager, Vontu Monitor Controller

B. Vontu Update, Vontu Notifier, Vontu Manager, Vontu Incident Persister, Vontu Monitor Controller

C. Vontu Incident Persister, Vontu Update, Vontu Notifier, Vontu Monitor Controller, Vontu Manager.

D. Vontu Monitor Controller, Vontu Incident Persister, Vontu Manager, Vontu Notifier, Vontu Update.

Correct Answer: D

Reference: https://help.symantec.com/cs/dlp15.1/DLP/v23042736_v125428396/Stopping-an-Enforce-Server-on-Windows?locale=EN_US

QUESTION 12

What are two reasons an administrator should utilize a manual configuration to determine the endpoint location? (Choose two.)

A. To specify Wi-Fi SSID names

B. To specify an IP address or range

C. To specify the endpoint server

D. To specify domain names

E. To specify network card status (ON/OFF)

Correct Answer: BD

Reference: https://help.symantec.com/cs/dlp15.1/DLP/v18349332_v125428396/Setting-the-endpoint-location?locale=EN_US

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

Where should an administrator set the debug levels for an Endpoint Agent?

A. Setting the log level within the Agent List

B. Advanced configuration within the Agent settings

C. Setting the log level within the Agent Overview

D. Advanced server settings within the Endpoint server

Correct Answer: C

Reference: https://support.symantec.com/en_US/article.TECH248581.html

QUESTION 15

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)

Correct Answer: AD