Exam Questions 250-438

Administration of Symantec Data Loss Prevention 15

https://www.2passeasy.com/dumps/250-438/

NEW QUESTION 1
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”

Answer: A

NEW QUESTION 2
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

NEW 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. AT&T
D. Verizon
E. Rackspace

Answer: BE

NEW QUESTION 4
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 attributes.
D. User attributes have been incorrectly mapped to Active Directory accounts.

Answer: D

NEW QUESTION 5
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

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

NEW QUESTION 6
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

Explanation:
Reference: https://help.symantec.com/cs/dlp15.1/DLP/v15600645_v125428396/Configuring-Network-Protect-for-file-shares?locale=EN_US

NEW QUESTION 7

Which action should a DLP administrator take to secure communications between an on-premises Enforce server and detection servers hosted in the Cloud?

A. Use the built-in Symantec DLP certificate for the Enforce Server, and use the “sslkeytool” utility to create certificates for the detection servers.
B. Use the built-in Symantec DLP certificate for both the Enforce server and the hosted detection servers.
C. Set up a Virtual Private Network (VPN) for the Enforce server and the hosted detection servers.
D. Use the “sslkeytool” utility to create certificates for the Enforce server and the hosted detection servers.

Answer: A

Explanation:
Reference: https://www.symantec.com/connect/articles/sslkeytool-utility-and-server-certificates

NEW QUESTION 8
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)

Answer: BE

NEW QUESTION 9
A DLP administrator has added several approved endpoint devices as exceptions to an Endpoint Prevent policy that blocks the transfer of sensitive data. However, data transfers to these devices are still being blocked. What is the first action an administrator should take to enable data transfers to the approved endpoint devices?

A. Disable and re-enable the Endpoint Prevent policy to activate the changes
B. Double-check that the correct device ID or class has been entered for each device
C. Verify Application File Access Control (AFAC) is configured to monitor the specific application
D. Edit the exception rule to ensure that the “Match On” option is set to “Attachments”

Answer: D

NEW QUESTION 10
What is the default fallback option for the Endpoint Prevent Encrypt response rule?

A. Block
B. User Cancel
C. Encrypt
D. Notify

Answer: D

NEW QUESTION 10
Which channel does Endpoint Prevent protect using Device Control?

A. Bluetooth
B. USB storage
C. CD/DVD
D. Network card

Answer: B

Explanation:
Reference: https://support.symantec.com/en_US/article.HOWTO80865.html#v36651044

NEW QUESTION 14
A divisional executive requests a report of all incidents generated by a particular region, summarized by department. What does the DLP administrator need to configure to generate this report?

A. Custom attributes
B. Status attributes
C. Sender attributes
D. User attributes

Answer: A

NEW QUESTION 19
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)

Answer: A

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

NEW QUESTION 23
What is Application Detection Configuration?

A. The Cloud Detection Service (CDS) process that tells Enforce a policy has been violated
B. The Data Loss Prevention (DLP) policy which has been pushed into Cloud Detection Service (CDC) for files in transit to or residing in Cloud apps
C. The terminology describing the Data Loss Prevention (DLP) process within the CloudSOC administration portal
D. The setting configured within the user interface (UI) that determines whether CloudSOC should send a file to Cloud Detection Service (CDS) for analysis.

Answer: A

Explanation:
Reference: https://help.symantec.com/cs/DLP15.0/DLP/v119805091_v120691346/About-Application-Detection%7CSymantec%EF%BF%BD-Data-Loss-Prevention-15.0?locale=EN_US

NEW QUESTION 28
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

Answer: C

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

NEW QUESTION 30
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: AE

NEW QUESTION 34
Which two factors are common sources of data leakage where the main actor is well-meaning insider? (Choose two.)

A. An absence of a trained incident response team
B. A disgruntled employee for a job with a competitor
C. Merger and Acquisition activities
D. Lack of training and awareness
E. Broken business processes

Answer: BD

NEW QUESTION 36
What is required on the Enforce server to communicate with the Symantec DLP database?

A. Port 8082 should be opened
B. CryptoMasterKey.properties file
C. Symbolic links to .dbf files
D. SQL*Plus Client

Answer: D

Explanation:
Reference: https://www.symantec.com/connect/articles/three-tier-installation-dlp-product

NEW QUESTION 38
A DLP administrator is attempting to add a new Network Discover detection server from the Enforce management console. However, the only available options are Network Monitor and Endpoint servers. What should the administrator do to make the Network Discover option available?

A. Restart the Symantec DLP Controller service
B. Apply a new software license file from the Enforce console
C. Install a new Network Discover detection server
D. Restart the Vontu Monitor Service

Answer: C

NEW QUESTION 40
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

Answer: B

NEW QUESTION 42
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

Answer: D

Explanation:
If you plan to use the grid scanning feature to distribute the scanning workload across multiple detection servers, retain the default value (1)

NEW QUESTION 43
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: AD

NEW QUESTION 46
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)

Answer: D

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

NEW QUESTION 47
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

Explanation:
Reference: https://www.symantec.com/connect/forums/new-install-oracle-returns-error

NEW QUESTION 52
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

Answer: D

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

NEW QUESTION 54
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

Answer: C

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

NEW QUESTION 59
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

Explanation:
Reference: https://www.symantec.com/connect/forums/dlp-pop-examining-content

NEW QUESTION 63
.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual 250-438 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the 250-438 Product From:

https://www.2passeasy.com/dumps/250-438/

Money Back Guarantee

250-438 Practice Exam Features:

* 250-438 Questions and Answers Updated Frequently

* 250-438 Practice Questions Verified by Expert Senior Certified Staff

* 250-438 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* 250-438 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year