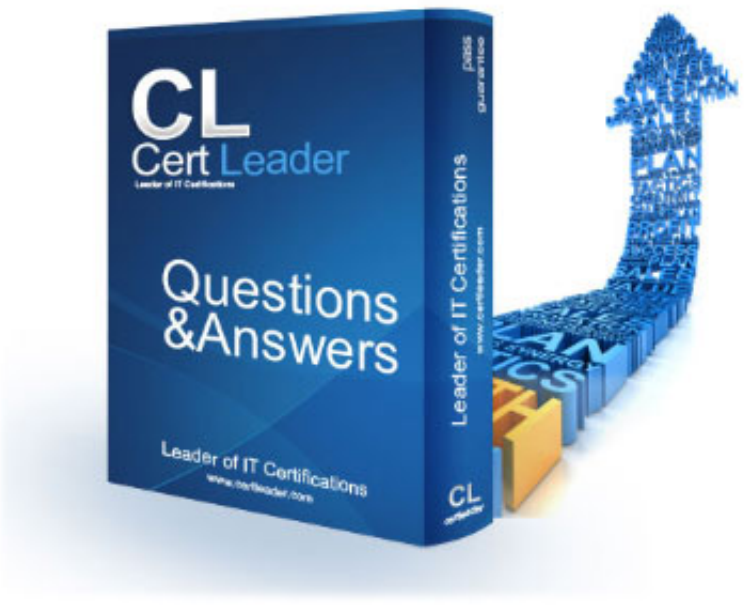
250-438 Dumps

Administration of Symantec Data Loss Prevention 15

https://www.certleader.com/250-438-dumps.html



NEW QUESTION 1
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 2
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 3
Which detection method depends on “training sets”?

A. Form Recognition
B. Vector Machine Learning (VML)
C. Index Document Matching (IDM)
D. Exact Data Matching (EDM)

Answer: B

Explanation:
Reference: http://eval.symantec.com/mktginfo/enterprise/white_papers/b-dlp_machine_learning.WP_en-us.pdf

NEW QUESTION 4
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 5
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 6
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 7
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.

Answer: B

Explanation:
Reference: https://support.symantec.com/content/unifiedweb/en_US/article.TECH220250.html

NEW QUESTION 8
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 9
An administrator is unable to log in to the Enforce management console as “sysadmin”. Symantec DLP is configured to use Active Directory authentication. The administrator is a member of two roles: “sysadmin” and “remediator.” How should the administrator log in to the Enforce console with the “sysadmin” role?

A. sysadmin\username
B. sysadmin\username@domain
C. domain\username
D. username\sysadmin

Answer: C

NEW QUESTION 10
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 10
Which option is an accurate use case for Information Centric Encryption (ICE)?

A. The ICE utility encrypts files matching DLP policy being copied from network share through use of encryption keys.
B. The ICE utility encrypts files matching DLP policy being copied to removable storage through use of encryption keys.
C. The ICE utility encrypts files matching DLP policy being copied to removable storage on an endpoint use of certificates.
D. The ICE utility encrypts files matching DLP policy being copied from network share through use of certificates

Answer: B

Explanation:
Reference: https://help.symantec.com/cs/ICE1.0/ICE/v126756321_v120576779/Using-ICE-with-Symantec-Data-Loss-Preventionabout_dlp?locale=EN_US

NEW QUESTION 14
DRAG DROP
The Symantec Data Loss risk reduction approach has six stages.
Drag and drop the six correct risk reduction stages in the proper order of Occurrence column.
Select and Place:

A. Mastered
B. Not Mastered

Answer: A

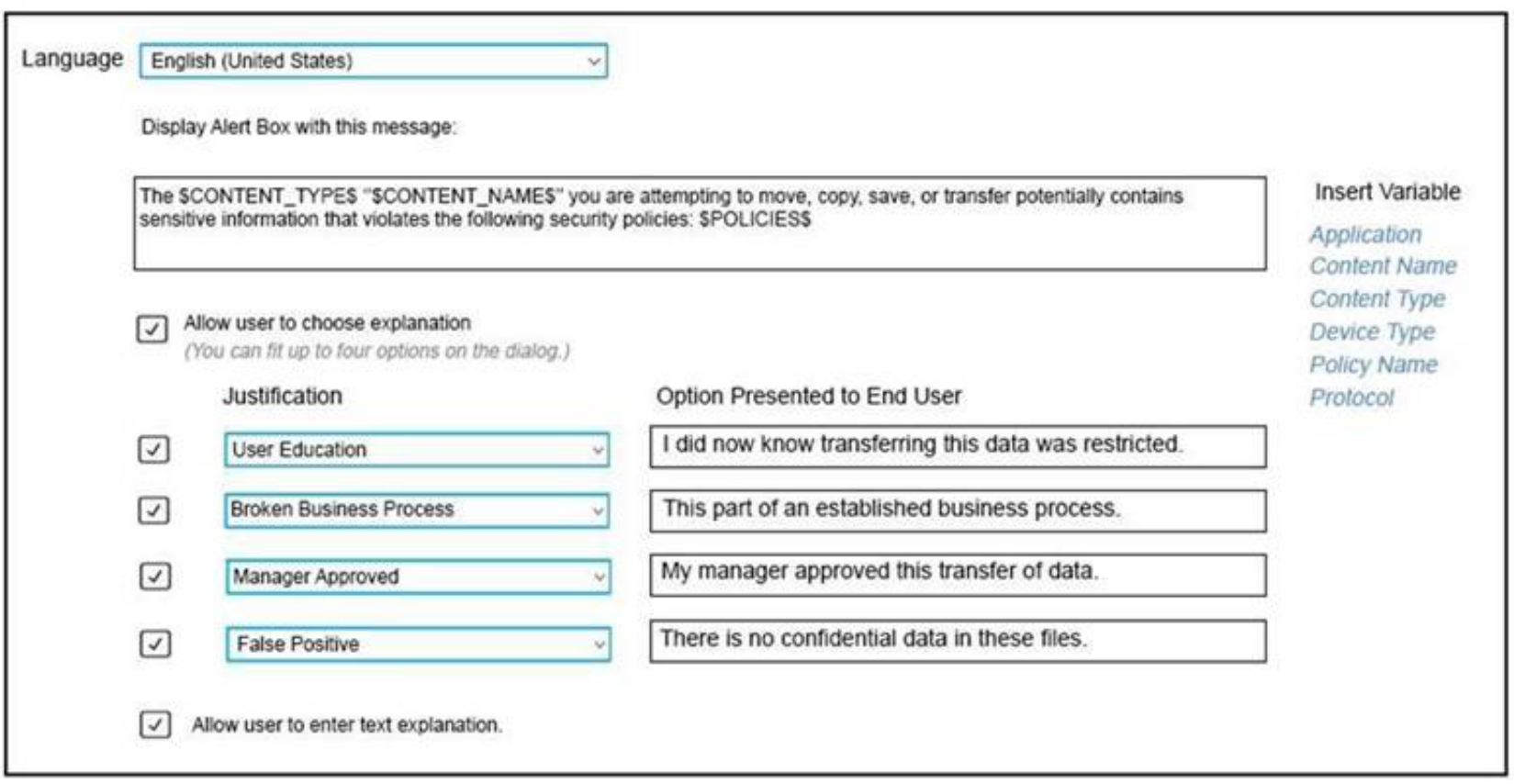
Explanation:
Reference: https://www.slideshare.net/iftikhariqbal/symantec-data-loss-prevention-technical-proposal-general

NEW QUESTION 19
What detection server type requires a minimum of two physical network interface cards?

A. Network Prevent for Web
B. Network Prevent for Email
C. Network Monitor
D. Cloud Detection Service (CDS)

Answer: A

NEW QUESTION 23
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

Answer: B

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

NEW QUESTION 24
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

Answer: CD

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

NEW QUESTION 28
.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your 250-438 Exam with Our Prep Materials Via below:

https://www.certleader.com/250-438-dumps.html