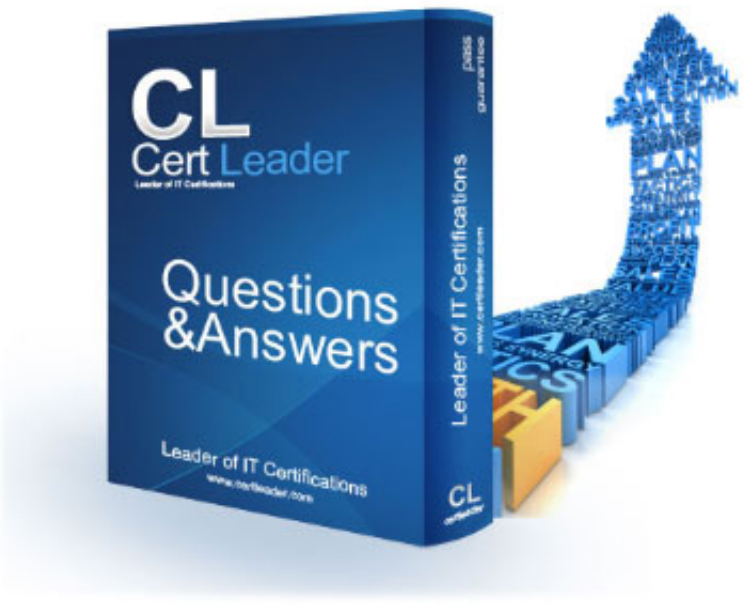
250-438 Dumps

Administration of Symantec Data Loss Prevention 15

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



NEW QUESTION 1
What is the correct configuration for “BoxMonitor.Channels” that will allow the server to start as a Network Monitor server?

A. Packet Capture, Span Port
B. Packet Capture, Network Tap
C. Packet Capture, Copy Rule
D. Packet capture, Network Monitor

Answer: C

Explanation:
Reference: https://support.symantec.com/en_US/article.TECH218980.html

NEW QUESTION 2
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 3
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 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)

Answer: BE

NEW QUESTION 5
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 6
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 7
Which two components can perform a file system scan of a workstation? (Choose two.)

A. Endpoint Server
B. DLP Agent
C. Network Prevent for Web Server
D. Discover Server
E. Enforce Server

Answer: BD

NEW QUESTION 8
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 9
When managing an Endpoint Discover scan, a DLP administrator notices some endpoint computers are NOT completing their scans. When does the DLP agent stop scanning?

A. When the agent sends a report within the “Scan Idle Timeout” period
B. When the endpoint computer is rebooted and the agent is started
C. When the agent is unable to send a status report within the “Scan Idle Timeout” period
D. When the agent sends a report immediately after the “Scan Idle Timeout” period

Answer: C

NEW QUESTION 10
Which two detection servers are available as virtual appliances? (Choose two.)

A. Network Monitor
B. Network Prevent for Web
C. Network Discover
D. Network Prevent for Email
E. Optical Character Recognition (OCR)

Answer: BD

Explanation:
Reference: https://help.symantec.com/cs/dlp15.0/DLP/v123002905_v120691346/About-DLP-Appliances?locale=EN_US

NEW QUESTION 10
Which server target uses the “Automated Incident Remediation Tracking” feature in Symantec DLP?

A. Exchange
B. File System
C. Lotus Notes
D. SharePoint

Answer: B

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

NEW QUESTION 14
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 17
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

Answer: C

NEW QUESTION 18
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

Answer: BC

NEW QUESTION 21
A compliance officer needs to understand how the company is complying with its data security policies over time. Which report should be compliance officer generate to obtain the compliance information?

A. Policy report, filtered on date and summarized by policy
B. Policy Trend report, summarized by policy, then quarter
C. Policy report, filtered on quarter and summarized by policy
D. Policy Trend report, summarized by policy, then severity

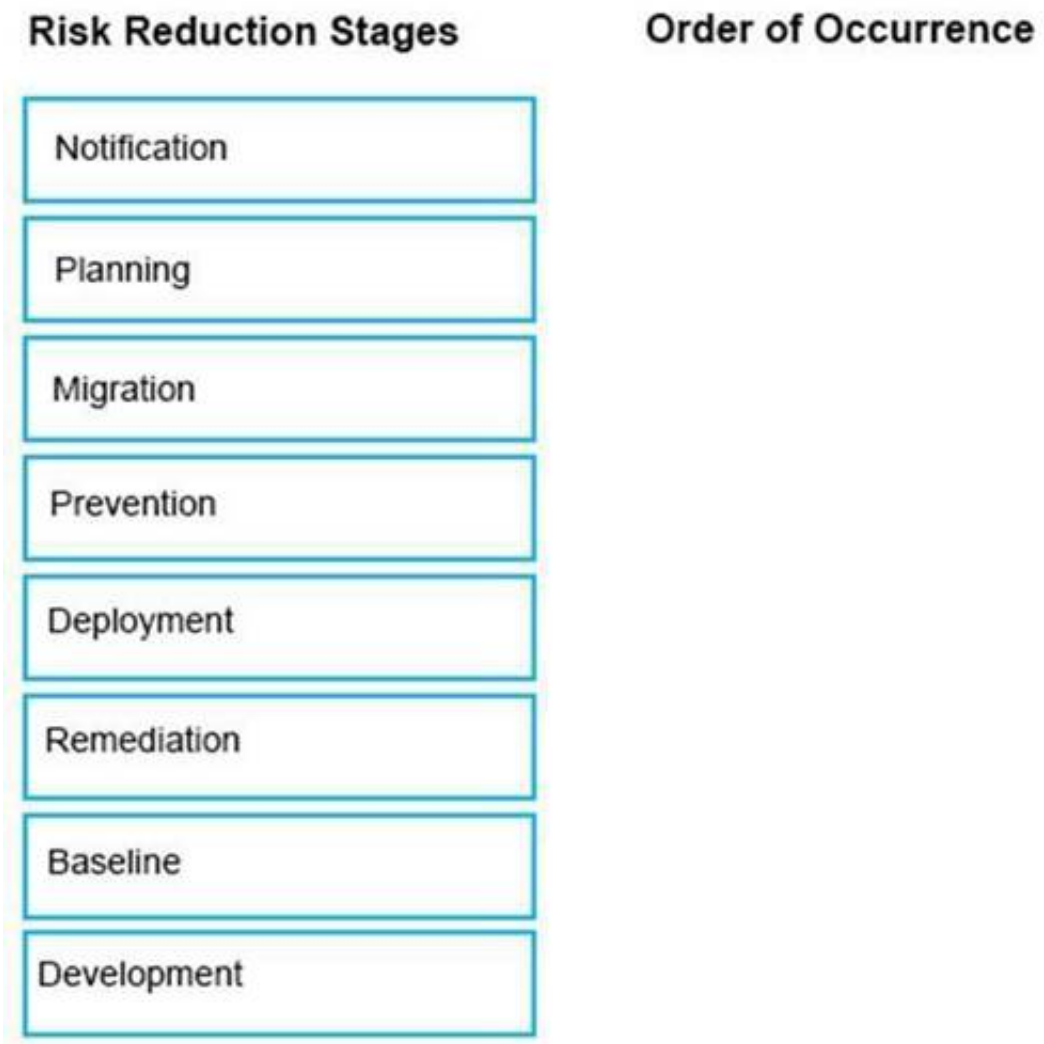
Answer: A

NEW QUESTION 23
A DLP administrator has performed a test deployment of the DLP 15.0 Endpoint agent and now wants to uninstall the agent. However, the administrator no longer remembers the uninstall password. What should the administrator do to work around the password problem?

A. Apply a new global agent uninstall password in the Enforce management console.
B. Manually delete all the Endpoint agent files from the test computer and install a new agent package.
C. Replace the PGPsdk.dll file on the agent's assigned Endpoint server with a copy from a different Endpoint server
D. Use the UninstallPwdGenerator to create an UninstallPasswordKey.

Answer: D

NEW QUESTION 28
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:

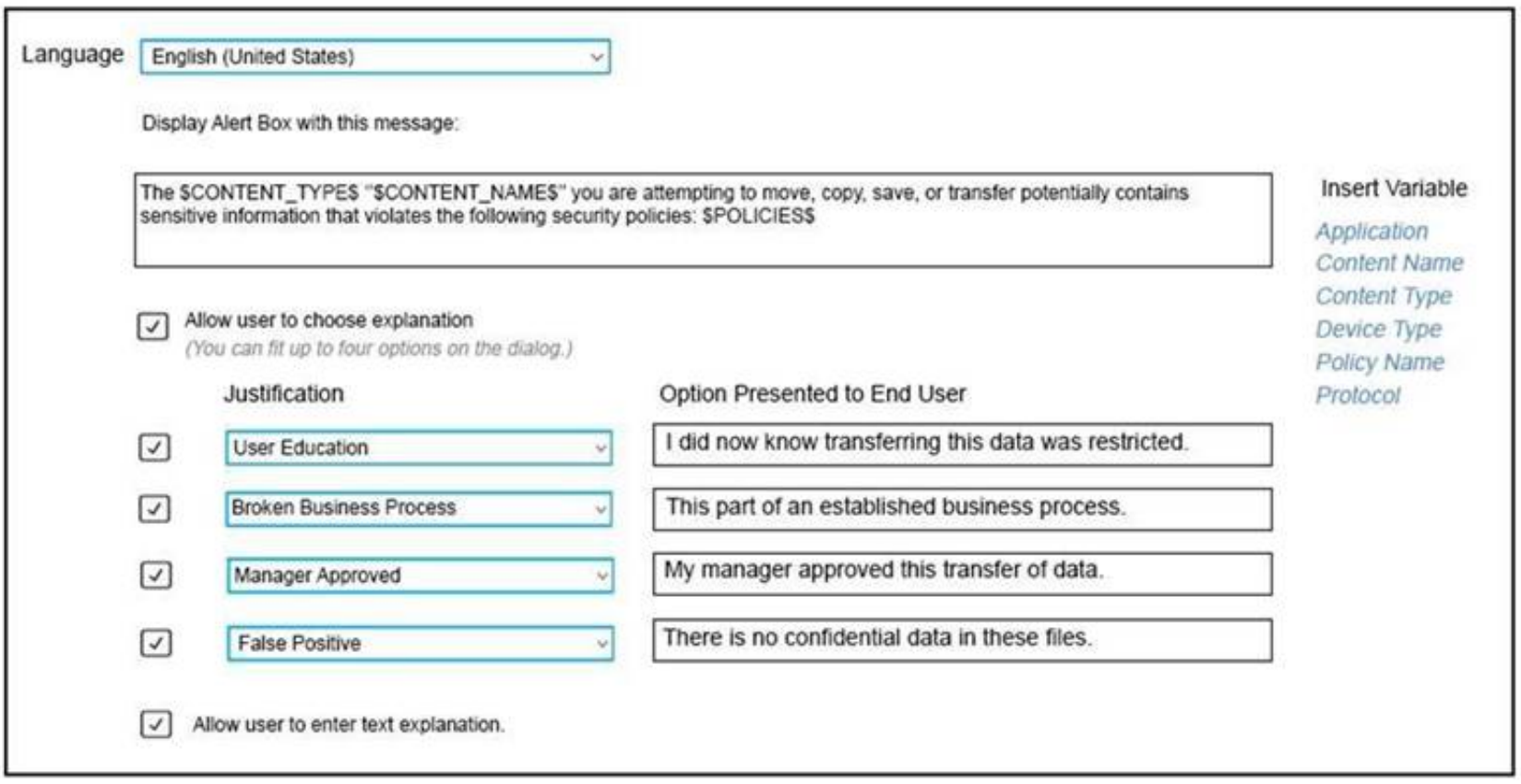


A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 29
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 31
Why would an administrator set the Similarity Threshold to zero when testing and tuning a Vector Machine Learning (VML) profile?

A. To capture the matches to the Positive set
B. To capture the matches to the Negative set
C. To see the false negatives only
D. To see the entire range of potential matches

Answer: D

Explanation:
Reference: https://help.symantec.com/cs/dlp15.0/DLP/v45067125_v120691346/Adjusting-the-Similarity-Threshold?locale=EN_US

NEW QUESTION 33
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 36
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

Answer: B

NEW QUESTION 37
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 39
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
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 48
.....

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