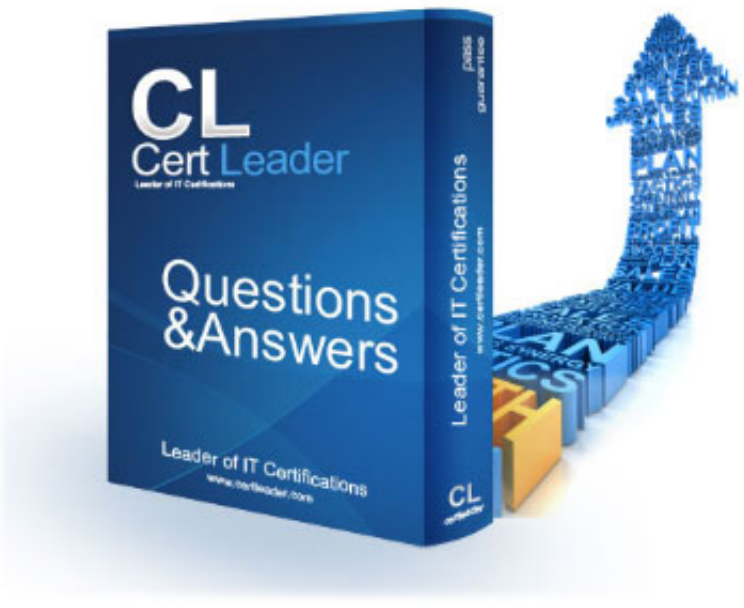
250-438 Dumps

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
How should a DLP administrator exclude a custom endpoint application named “custom_app.exe” from being monitoring by Application File Access Control?

A. Add “custom_app.exe” to the “Application Whitelist” on all Endpoint servers.
B. Add “custom_app.exe” Application Monitoring Configuration and de-select all its channel options.
C. Add “custom_app_.exe” as a filename exception to the Endpoint Prevent policy.
D. Add “custom_app.exe” to the “Program Exclusion List” in the agent configuration settings.

Answer: A

Explanation:
Reference: https://docs.mcafee.com/bundle/data-loss-prevention-11.0.400-product-guide-epolicy-orchestrator/page/GUID-0F81A895-0A46-4FF8-A869-0365D6620185.html

NEW QUESTION 3
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)

Answer: BD

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

NEW QUESTION 4
Which two locations can Symantec DLP scan and perform Information Centric Encryption (ICE) actions on? (Choose two.)

A. Exchange
B. Jiveon
C. File store
D. SharePoint
E. Confluence

Answer: CD

Explanation:
Reference: https://www.symantec.com/content/dam/symantec/docs/data-sheets/information-centric-encryption-en.pdf

NEW QUESTION 5
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 6
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 7
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 8
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 9
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

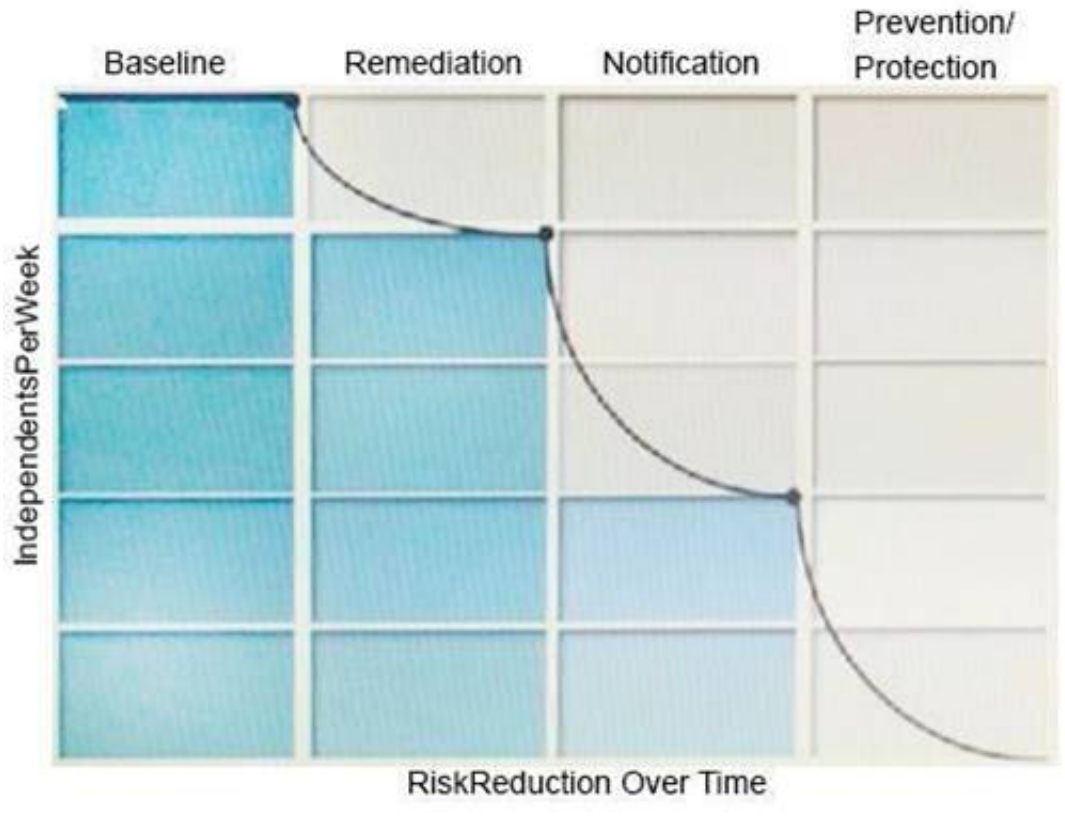
Explanation:
Reference: https://help.symantec.com/cs/DLP15.0/DLP/v83981880_v120691346/Troubleshooting-automated-incident-remediation-tracking?locale=EN_US

NEW QUESTION 10
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 11
Refer to the exhibit.



What activity should occur during the baseline phase, according to the risk reduction model?

A. Define and build the incident response team
B. Monitor incidents and tune the policy to reduce false positives
C. Establish business metrics and begin sending reports to business unit stakeholders
D. Test policies to ensure that blocking actions minimize business process disruptions

Answer: C

NEW QUESTION 14
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 17
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 20
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 22
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 26
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)

Answer: D

NEW QUESTION 27
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 29
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 31
Which two detection technology options ONLY run on a detection server? (Choose two.)

A. Form Recognition
B. Indexed Document Matching (IDM)
C. Described Content Matching (DCM)
D. Exact Data Matching (EDM)
E. Vector Machine Learning (VML)

Answer: BD

Explanation:
Reference: https://support.symantec.com/en_US/article.INFO5070.html

NEW QUESTION 32
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 36
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 39
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 43
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 48
Which two automated response rules will be active in policies that include Exact Data Matching (EDM) detection rule? (Choose two.)

A. Endpoint Discover: Quarantine File
B. All: Send Email Notification
C. Endpoint Prevent: User Cancel
D. Endpoint Prevent: Block
E. Network Protect: Quarantine File

Answer: AD

NEW QUESTION 51
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 53
.....

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