Exam Questions 250-438

Administration of Symantec Data Loss Prevention 15

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

NEW QUESTION 1
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 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

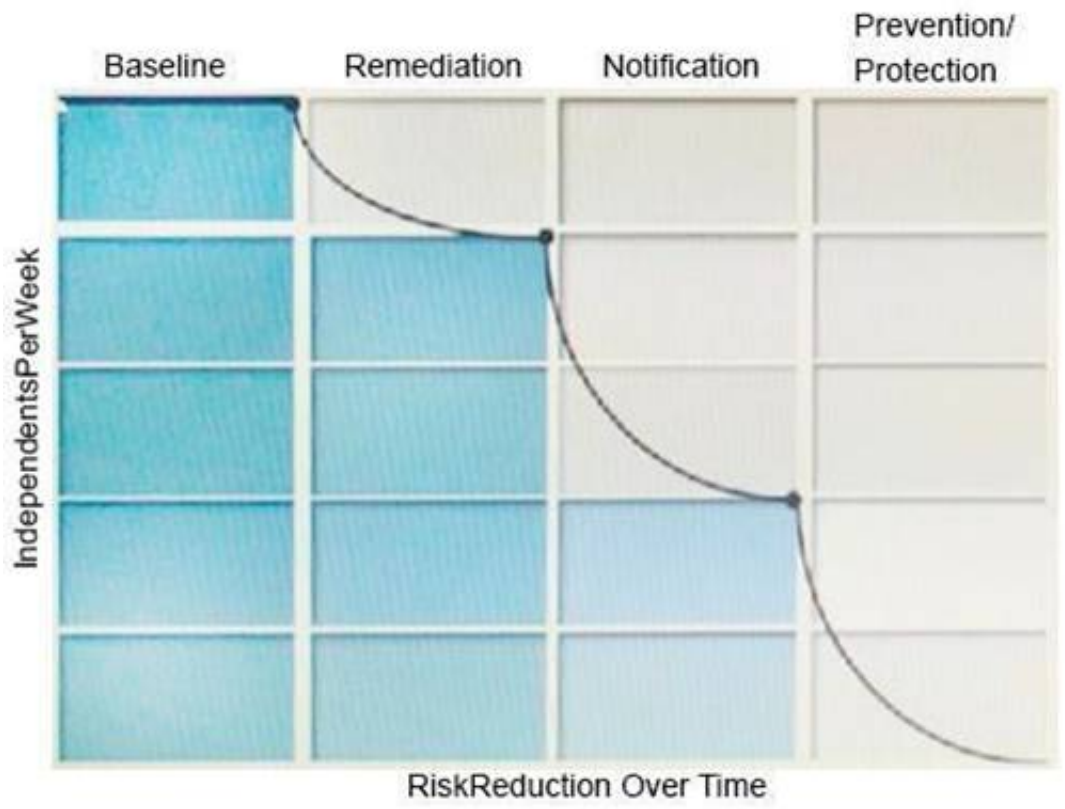
Explanation:
Reference: https://docs.mcafee.com/bundle/data-loss-prevention-11.0.400-product-guide-epolicy-orchestrator/page/GUID-0F81A895-0A46-4FF8-A869-0365D6620185.html

NEW QUESTION 3
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 4
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 5
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 6
A DLP administrator is testing Network Prevent for Web functionality. When the administrator posts a small test file to a cloud storage website, no new incidents are reported. What should the administrator do to allow incidents to be generated against this file?

A. Change the “Ignore requests Smaller Than” value to 1
B. Add the filename to the Inspect Content Type field
C. Change the “PacketCapture.DISCARD_HTTP_GET” value to “false”
D. Uncheck trial mode under the ICAP tab

Answer: A

Explanation:
Reference: https://help.symantec.com/cs/dlp15.0/DLP/id-SF0B0161467_v120691346/Configuring-Network-Prevent-for-Web-Server?locale=EN_US

NEW QUESTION 7
Which statement accurately describes where Optical Character Recognition (OCR) components must be installed?

A. The OCR engine must be installed on detection server other than the Enforce server.
B. The OCR server software must be installed on one or more dedicated (non-detection) Linux servers.
C. The OCR engine must be directly on the Enforce server.
D. The OCR server software must be installed on one or more dedicated (non-detection) Windows servers.

Answer: C

Explanation:
Reference: https://help.symantec.com/cs/dlp15.0/DLP/v122760174_v120691346/Setting-up-OCR-Servers?locale=EN_US

NEW QUESTION 8
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 9
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 10
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 10
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 13
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 15
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 17
A DLP administrator created a new agent configuration for an Endpoint server. However, the endpoint agents fail to receive the new configuration. What is one possible reason that the agent fails to receive the new configuration?

A. The new agent configuration was saved but not applied to any endpoint groups.
B. The new agent configuration was copied and modified from the default agent configuration.
C. The default agent configuration must be disabled before the new configuration can take effect.
D. The Endpoint server needs to be recycled so that the new agent configuration can take effect.

Answer: C

NEW QUESTION 20
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 21
.....

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