Symantec

Exam Questions 250-438

Administration of Symantec Data Loss Prevention 15

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
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 3
Which option correctly describes the two-tier installation type for Symantec DLP?

A. Install the Oracle database on the host, and install the Enforce server and a detection server on a second host.
B. Install the Oracle database on a local physical host, and install the Enforce server and detection servers on virtual hosts in the Cloud.
C. Install the Oracle database and a detection server in the same host, and install the Enforce server on a second host.
D. Install the Oracle database and Enforce server on the same host, and install detection servers on separate hosts.

Answer: D

Explanation:
Reference: https://www.symantec.com/connect/forums/deployment-enforce-and-detection-servers

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
What detection method utilizes Data Identifiers?

A. Indexed Document Matching (IDM)
B. Described Content Matching (DCM)
C. Directory Group Matching (DGM)
D. Exact Data Matching (EDM)

Answer: D

Explanation:
Reference: https://www.symantec.com/connect/forums/edm-policy-exception

NEW QUESTION 7
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

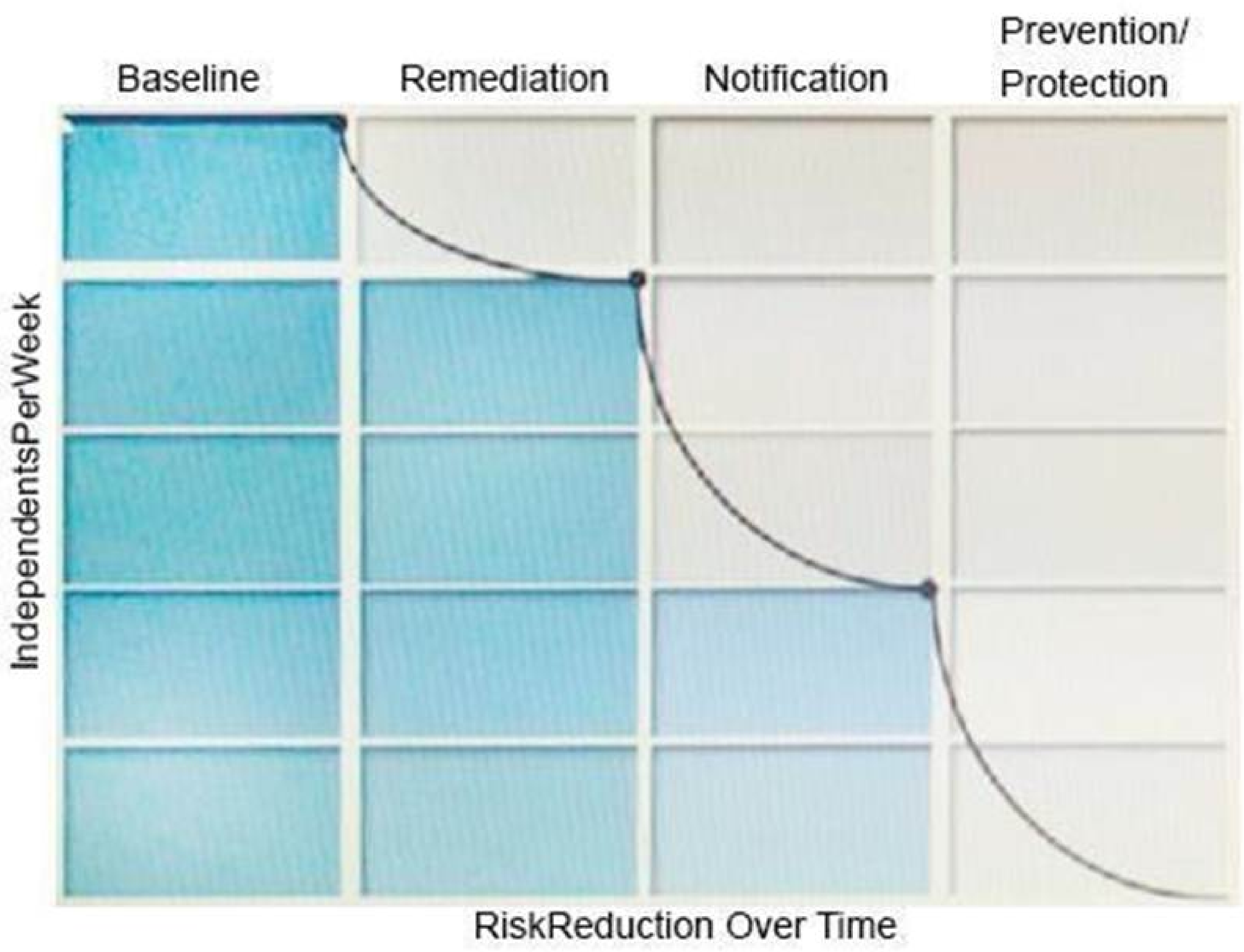
NEW QUESTION 8
Which tool must a DLP administrator run to certify the database prior to upgrading DLP?

A. Lob_Tablespace Reclamation Tool
B. Upgrade Readiness Tool
C. SymDiag
D. EnforceMigrationUtility

Answer: B

Explanation:
Reference: https://support.symantec.com/en_US/article.DOC10667.html

NEW QUESTION 9
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 10
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 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 14
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

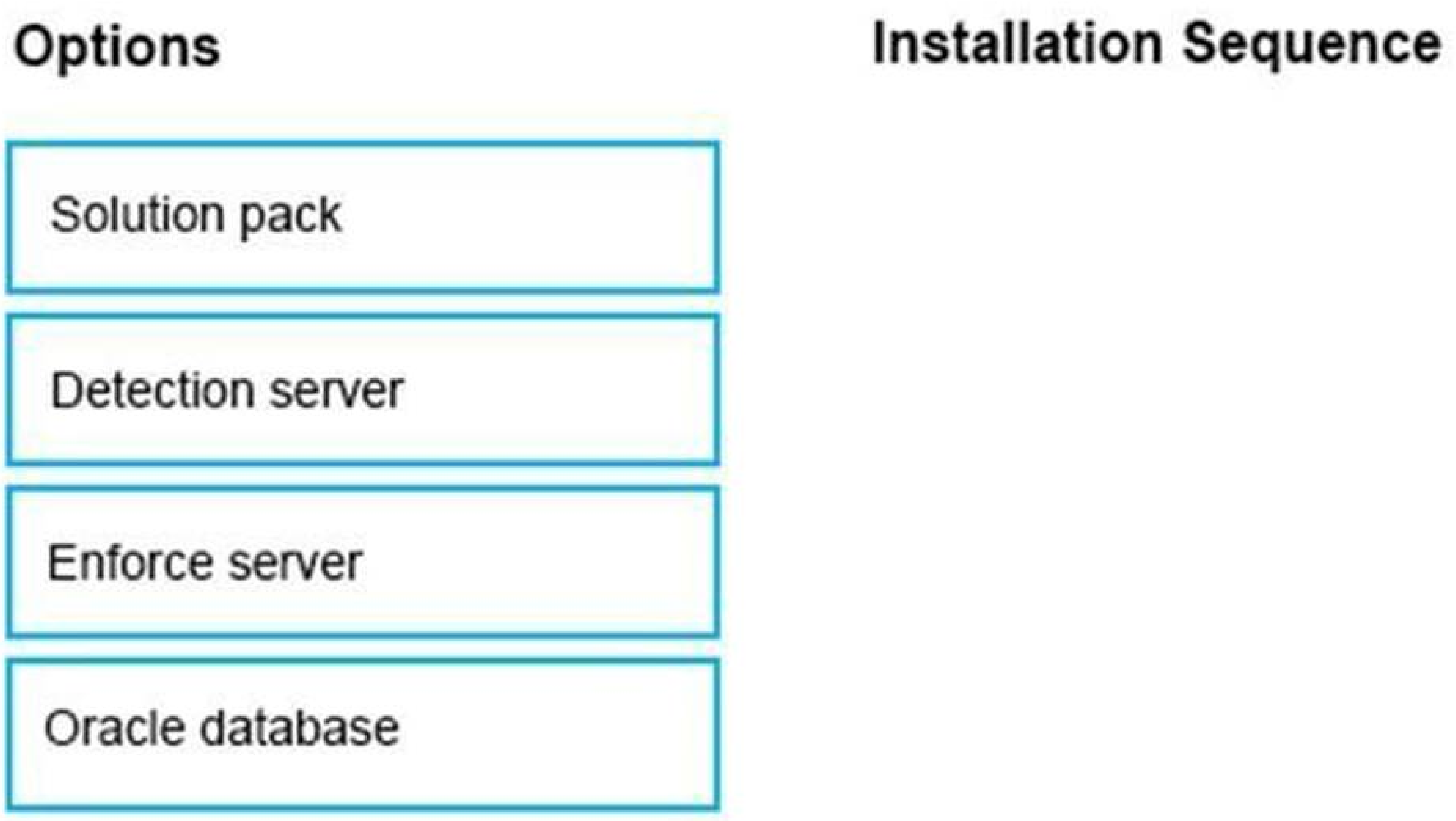
NEW QUESTION 19
A DLP administrator is testing Network Prevent for Web functionality. When the administrator posts a small test file to a cloud storage website, no new incidents are reported. What should the administrator do to allow incidents to be generated against this file?

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 20
DRAG DROP
What is the correct installation sequence for the components shown here, according to the Symantec Installation Guide? Place the options in the correct installation sequence.
Select and Place:



Options

Installation Sequence

Solution pack

Detection server

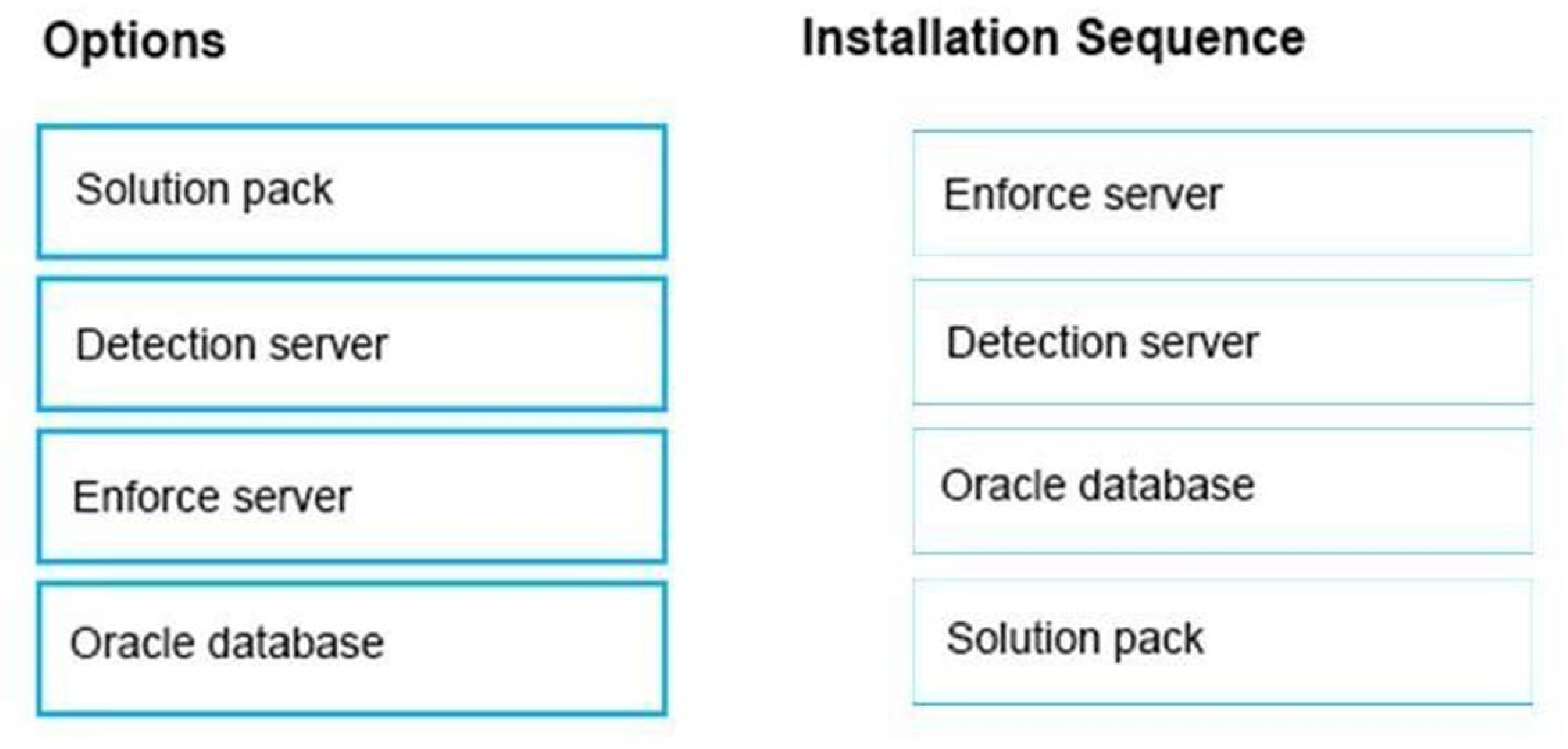
Enforce server

Oracle database

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Options

Solution pack

Detection server

Enforce server

Oracle database

Installation Sequence

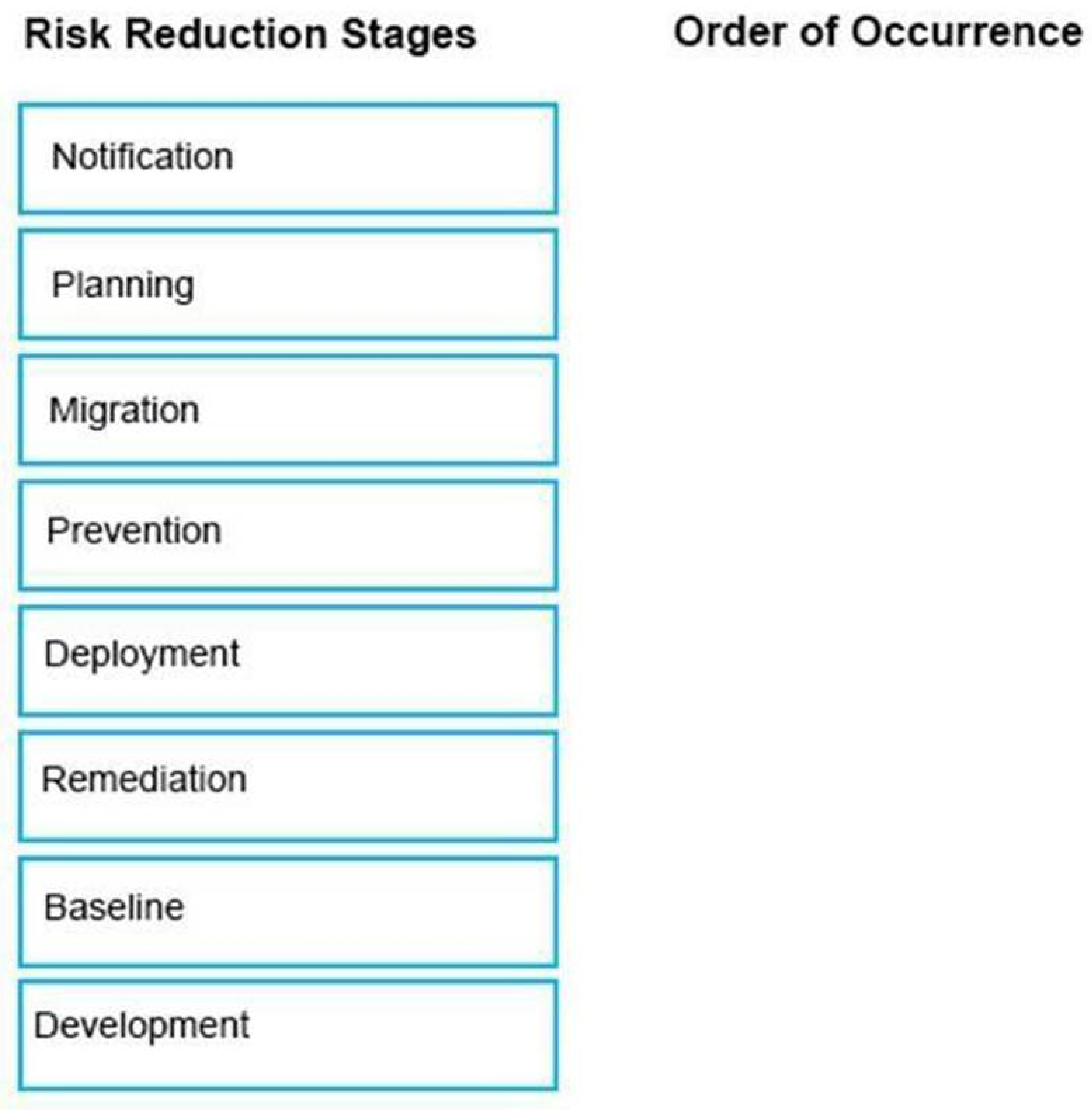
Enforce server

Detection server

Oracle database

Solution pack

NEW QUESTION 23
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:



Risk Reduction Stages

Order of Occurrence

Notification

Planning

Migration

Prevention

Deployment

Remediation

Baseline

Development

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 27
Which Network Prevent action takes place when the Network Incident list shows the message is “Modified”?

A. Remove attachments from an email
B. Obfuscate text in the body of an email
C. Add one or more SMTP headers to an email
D. Modify content from the body of an email

Answer: C

NEW QUESTION 30
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
A company needs to implement Data Owner Exception so that incidents are avoided when employees send or receive their own personal information.
What detection method should the company use?

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

Answer: C

Explanation:
Reference: https://help.symantec.com/cs/dlp15.5/DLP/v40148006_v128674454/About-Data-Owner-Exception?locale=EN_US

NEW QUESTION 32
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 37
A DLP administrator is checking the System Overview in the Enforce management console, and all of the detection servers are showing as “unknown”. The Vontu services are up and running on the detection servers. Thousands of .IDC files are building up in the Incidents directory on the detection servers. There is good network connectivity between the detection servers and the Enforce server when testing with the telnet command.
How should the administrator bring the detection servers to a running state in the Enforce management console?

A. Restart the Vontu Update Service on the Enforce server
B. Ensure the Vontu Monitor Controller service is running in the Enforce server
C. Delete all of the .BAD files in the Incidents folder on the Enforce server
D. Restart the Vontu Monitor Service on all the affected detection servers

Answer: B

NEW QUESTION 42
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 47
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 51
What is the Symantec recommended order for stopping Symantec DLP services on a Windows Enforce server?

A. Vontu Notifier, Vontu Incident Persister, Vontu Update, Vontu Manager, Vontu Monitor Controller
B. Vontu Update, Vontu Notifier, Vontu Manager, Vontu Incident Persister, Vontu Monitor Controller
C. Vontu Incident Persister, Vontu Update, Vontu Notifier, Vontu Monitor Controller, Vontu Manager.
D. Vontu Monitor Controller, Vontu Incident Persister, Vontu Manager, Vontu Notifier, Vontu Update.

Answer: D

Explanation:

Reference: https://help.symantec.com/cs/dlp15.1/DLP/v23042736_v125428396/Stopping-an-Enforce-Server-on-Windows?locale=EN_US

NEW QUESTION 53

......