DUMPSARENA

Symantec Data Loss Prevention 16.x Administration Technical Specialist

Symantec 250-587

Version Demo

Total Demo Questions: 13

Total Premium Questions: 130

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

QUESTION NO: 1

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: D

Explanation:

The OCR server software must be installed on one or more dedicated (non-detection) Windows servers. In Symantec Data Loss Prevention, OCR processing is provided by an OCR Server component that is deployed separately from the Enforce Server and Detection Servers. This separation provides the Windows-based environment and processing capacity required for converting image-based content into text that DLP can inspect. A dedicated OCR Server can be associated with the DLP environment so that supported detection workflows submit eligible files for OCR analysis without placing this workload on the management server or a Detection Server. Multiple dedicated OCR Servers may be deployed when additional OCR throughput or resiliency is needed. Administrators should use the supported Windows Server versions, sizing guidance, and installation sequence specified for their exact DLP release, then configure the OCR integration in the Enforce management console. Broadcom's DLP documentation portal contains the version-specific installation, system-requirements, and OCR configuration guidance: Symantec Data Loss Prevention documentation. Product compatibility and platform requirements are also maintained in Broadcom's Support Portal.

QUESTION NO: 2

An incident-response team needs to apply the same approved remediation action to many related incidents after reviewing them in the Enforce management console. Which two (2) steps support this workflow? (Choose two.)

A. Select the related incidents in an Incident List report

B. Invoke a configured Smart Response for the selected incidents

C. Modify the Endpoint Agent package on each affected computer

D. Restart the detection server that generated the incidents

E. Convert the Smart Response into an automated response after the incidents exist

ANSWER: A B

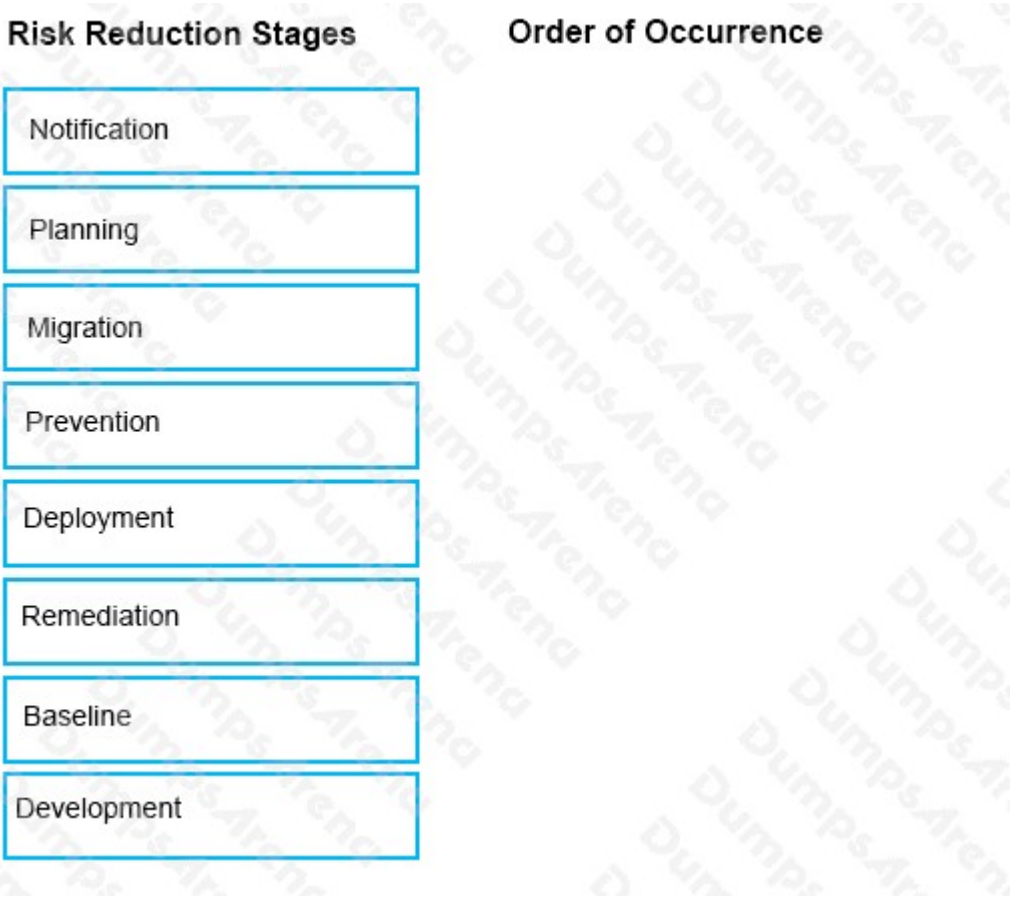
Explanation:

Responders can use an **Incident List report** to identify and select multiple incidents, then invoke a configured **Smart Response** for the selected incidents. This provides a responder-driven bulk workflow. An automated response is evaluated by policy when the incident is generated, rather than being manually initiated for a reviewed set of existing incidents.

QUESTION NO: 3 - (DRAG DROP)

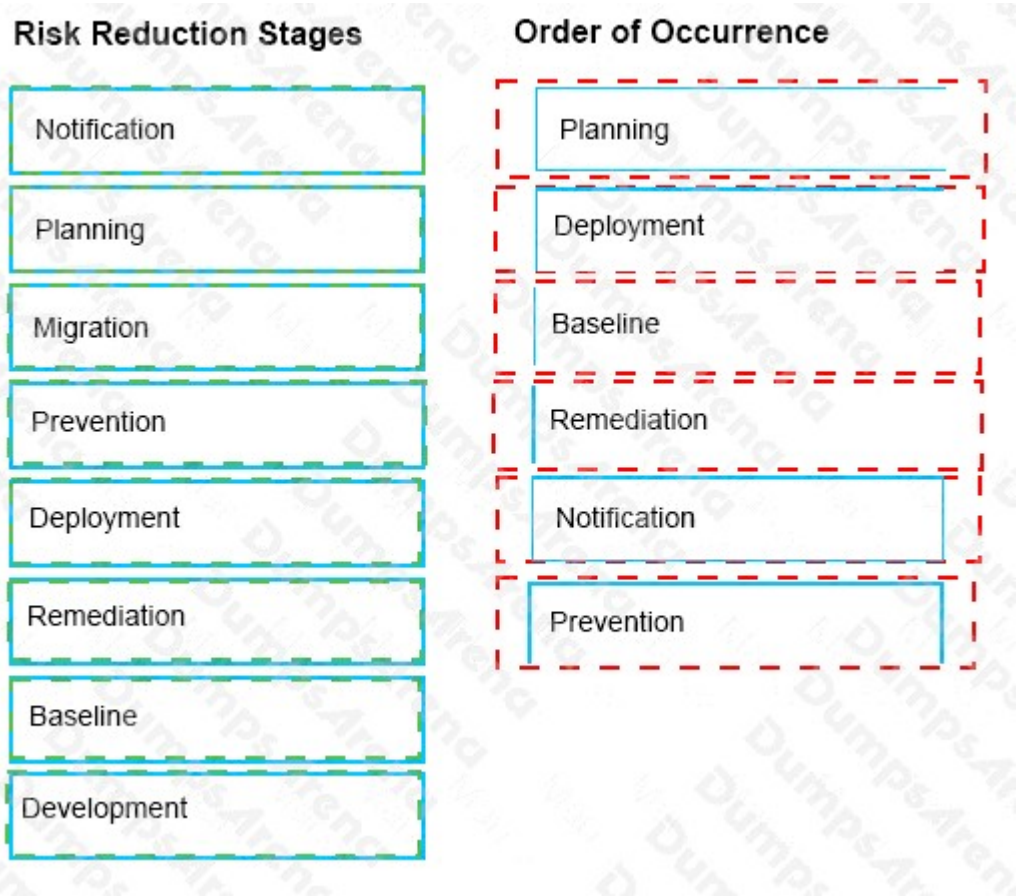
The Symantec Data Loss risk reduction approach has six stages.

Drag and drop the six correct risk reduction stages in the proper order of Occurrence column.



ANSWER:

Answer:



Answer:

Explanation:

[References:, ,]

Explanation:

The correct risk-reduction progression starts with **Planning**, where the organization identifies the sensitive-information risks it needs to address, establishes objectives, defines ownership, and determines how Data Loss Prevention will support the broader security program. **Deployment** follows because the required DLP components, detection policies, response rules, and relevant monitoring channels must be put into operation before meaningful risk data can be collected.

After deployment, **Baseline** is established. Baseline activity gives administrators a measured view of normal information movement, policy match volumes, users, locations, and business processes. This provides the factual starting point needed to prioritize work appropriately. The next stage is **Remediation**, in which the organization investigates the discovered incidents and addresses the underlying exposure, such as incorrect access, insecure workflows, inappropriate storage, or handling practices that create unnecessary data-loss risk.

Once remediation activity is operating, **Notification** communicates policy events and required actions to the appropriate users, managers, incident responders, or business owners. Notifications make the DLP program actionable and help build awareness of approved data-handling behavior. The final stage is **Prevention**. At this point, the organization can confidently enforce controls that block or otherwise prevent unacceptable transmission or movement of protected information, using the knowledge and tuning gained through the earlier stages.

This order reflects a practical DLP maturity path: establish the program, implement it, understand actual risk, correct it, communicate expectations, and then enforce preventative controls. Broadcom's Symantec Data Loss Prevention documentation portal provides the product administration and policy-management documentation that supports these operational activities.

QUESTION NO: 4

Which two (2) DLP products support Optical Character Recognition (OCR)? (Choose two.)

A. Network Discover

B. Endpoint Prevent

C. Network Prevent for Email

D. Endpoint Discover

E. Information Centric Analytics

ANSWER: A D

Explanation:

Network Discover and **Endpoint Discover** support Optical Character Recognition (OCR) because both products perform data-at-rest discovery scans on repositories and endpoint file systems. During these scans, DLP can submit supported image-based content for OCR processing, extract recognizable text, and apply the configured detection policies to that extracted text. This enables discovery policies to identify sensitive information that is present in scanned documents or image files rather than only in natively selectable document text. OCR is therefore used as part of the Discover scanning workflow and its content-inspection pipeline, where the system can process stored files and report policy incidents based on the recognized content. Administrators must configure the relevant OCR capabilities and ensure that scanned content meets the supported file-type, size, and image-quality requirements; OCR results are dependent on the quality and legibility of the source image. Broadcom's Symantec DLP documentation describes Discover as the data-at-rest solution family and provides product documentation for configuring content detection and discovery scans. See the Symantec Data Loss Prevention documentation portal and the Broadcom Data Loss Prevention product page.

QUESTION NO: 5

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:

The **Upgrade Readiness Tool** is the required utility for certifying the Symantec Data Loss Prevention Enforce database before an upgrade. It evaluates the database's readiness for the target DLP release, including schema-related prerequisites and conditions that could prevent the upgrade from completing safely. The tool produces a readiness report that the administrator should review and resolve before starting the Enforce upgrade procedure. This pre-upgrade certification is important because the Enforce database contains the incident, policy, configuration, and detection data that must remain structurally consistent throughout the upgrade. Running the tool as part of planned maintenance gives administrators an opportunity to identify and correct database issues while the existing DLP deployment is still operational, rather than discovering them during an upgrade window. Broadcom's DLP documentation includes upgrade planning and database preparation as required stages of the Enforce upgrade workflow, and administrators should use the documentation that corresponds to both their currently installed version and the intended target version. See the Symantec Data Loss Prevention 16.0 documentation and the Broadcom Support portal for version-specific upgrade guidance and utilities.

QUESTION NO: 6

What is the recommended ratio of Enforce servers to Oracle database servers when deploying Symantec DLP?

A. 1:1

B. 1:2

C. 2:1

D. 3:1

ANSWER: A

Explanation:

The recommended ratio is **1:1**: each Symantec Data Loss Prevention Enforce server should use its own Oracle Database server instance in a production deployment. The Enforce Server is the central management component that stores policy configuration, incident information, detection-server status, user and role data, reporting data, and other operational records in its Oracle database. A dedicated database relationship provides predictable performance, simplifies sizing and maintenance, and isolates Enforce operations from workloads belonging to another Enforce environment. This architecture also supports clear backup, recovery, upgrade, and troubleshooting procedures, because the Enforce Server and its database remain paired as a deployment unit. Oracle may be installed on a separate host from the Enforce Server, as is normally recommended for production capacity and resilience, but the database host is still dedicated to that Enforce Server at the recommended ratio. Broadcom's Data Loss Prevention documentation identifies Oracle as the Enforce Server's required repository and provides the installation and deployment guidance used to size and configure this relationship. See the Broadcom Symantec Data Loss Prevention documentation portal and the Broadcom Knowledge Base for current platform, database, and deployment requirements.

QUESTION NO: 7

A company needs to implement Data Owner Exception so that incidents 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:

Exact data matching (EDM) is the appropriate detection method because it compares content against a protected data set that the organization supplies, such as employee records containing personally identifiable information. When preparing an EDM data source, an administrator can designate a data-owner field. That field associates each protected record with the employee who owns the information. The Data Owner Exception then uses this ownership association to prevent an incident from being created when the detected sensitive record is handled by its designated owner in the allowed direction or context. This makes EDM suitable for protecting a centralized population of employee personal data while avoiding unnecessary alerts for employees legitimately accessing or transmitting their own records. The implementation requires accurately identifying the owner in the EDM source data, configuring the EDM profile with the relevant indexed fields, and enabling the applicable data-owner exception in the policy rule. This capability is based on structured record matching and owner metadata, rather than merely identifying similar documents or applying statistical content classification. Symantec Data Loss Prevention documentation describes EDM as a method for detecting exact values from a configured data source and documents policy and detection configuration in the DLP Administration guides. See the Broadcom Symantec Data Loss Prevention 16.1 documentation and the Symantec Data Loss Prevention documentation portal.

QUESTION NO: 8

What is Application Detection Configuration?

A. The Cloud Detection Service (CDS) process that tells Enforce a policy has been violated

B. The Data Loss Prevention (DLP) policy which has been pushed into Cloud Detection Service (CDC) for files in transit to or residing in Cloud apps

C. The terminology describing the Data Loss Prevention (DLP) process within the CloudSOC administration portal

D. the setting configured within the user interface (UI) that determines whether CloudSOC should send a file to Cloud Detection Service (CDS) for analysis.

ANSWER: D

Explanation:

The setting configured within the user interface (UI) that determines whether CloudSOC should send a file to Cloud Detection Service (CDS) for analysis is correct. Application Detection Configuration is part of the CloudSOC-to-DLP detection workflow: it controls whether content associated with a particular cloud application is forwarded to the Cloud Detection Service for inspection. When the configuration enables detection for the relevant application and traffic, CloudSOC submits eligible files to CDS, where the applicable DLP detection policies can be evaluated. This configuration therefore governs the handoff of cloud content for analysis rather than being the policy itself or a notification generated after a violation. Administrators use these application-level detection settings to align scanning behavior with the cloud services that their organization monitors and the content flows that require DLP inspection. Broadcom's DLP documentation describes Cloud Detection Service as the component used to inspect cloud content, while CloudSOC documentation covers the application integration and configuration context in which cloud content is selected for detection. See the Broadcom Data Loss Prevention documentation and the Broadcom CloudSOC documentation.

QUESTION NO: 9

Which of the following would have to be a custom attribute (and not an out-of -the-box system attribute) in incident snapshots?

A. Network Prevent Action

B. Endpoint Location

C. Employee Phone Number

D. See Before

ANSWER: C

Explanation:

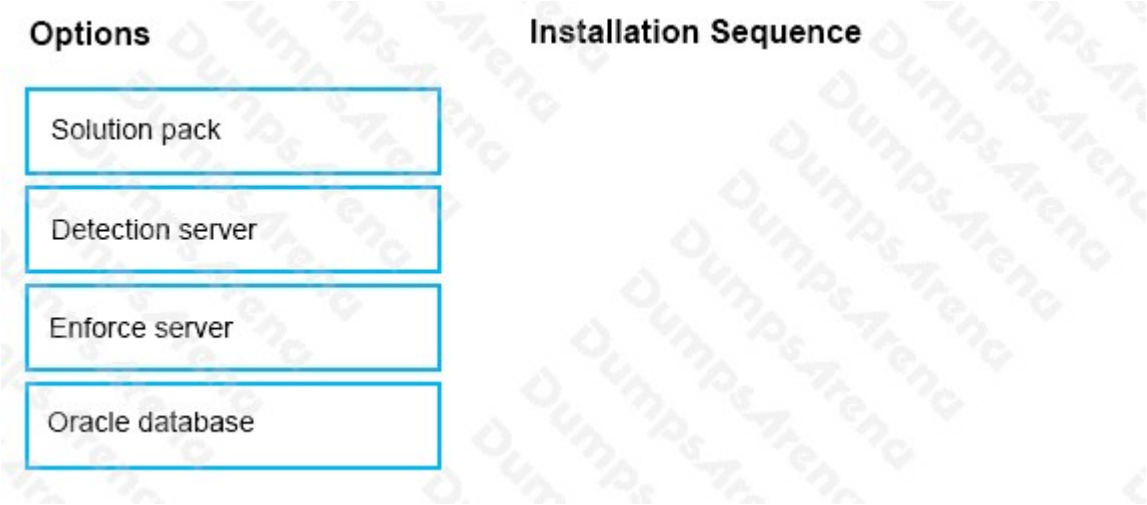
Employee Phone Number would have to be configured as a custom incident attribute. Symantec Data Loss Prevention incident snapshots include a defined set of out-of-the-box system attributes that are populated from incident processing, detection-server data, and endpoint or network monitoring context. Organizations can extend the information retained and displayed for incidents by creating custom attributes for business-specific data that is not part of that predefined system-attribute set.

An employee telephone number is organization-specific personnel information. Its source, format, and availability depend on the company's directory, HR system, case-management process, or another internal data source. Therefore, if investigators need this value in an incident snapshot, an administrator must define a custom attribute and arrange for the appropriate value to be populated as part of the organization's DLP workflow. This enables the incident-management process to retain relevant contact information without treating it as a built-in monitoring or incident-processing field. Broadcom's DLP documentation describes incident management and configurable incident data in the Symantec Data Loss Prevention 16.1 documentation. For product documentation and release-specific administrative guidance, see the Broadcom Security Support portal.

QUESTION NO: 10 - (SIMULATION)

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.



ANSWER: Check the explanation for the answer

Explanation:

Correct installation sequence:

1. **Oracle database**
2. **Enforce server**
3. **Detection server**
4. **Solution pack**

The Oracle database must be available before the Enforce Server is installed and configured. Detection Servers are then installed and registered with the Enforce Server. Install the Solution Pack last, after the core DLP components are operational.

QUESTION NO: 11

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: A D

Explanation:

Microsoft Exchange and Microsoft SharePoint are the Network Discover and Cloud Storage target types that support Information Centric Encryption as a policy response. When a Discover scan finds content that matches a policy, this response can apply persistent protection to the affected item rather than merely identifying it in an incident. The protection travels with the content, helping enforce authorized-use controls after the item has been discovered and remediated. This is particularly relevant to collaboration and messaging repositories, where files and attachments may continue to be accessed, forwarded, synchronized, or shared after scanning. Administrators configure the response within the relevant policy rules and must ensure that the Information Centric Encryption integration and associated rights-management configuration are available before using it operationally. Symantec Data Loss Prevention documentation organizes supported response rules by detection-server type and target, so the target capability must be validated when policies are designed or migrated. See the Symantec Data Loss Prevention 16.0 documentation landing page at Broadcom TechDocs: Data Loss Prevention 16.0 and the product documentation portal at Broadcom TechDocs.

QUESTION NO: 12

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: B D

Explanation:

Manual endpoint-location configuration is appropriate when an administrator needs to explicitly associate endpoints with a location based on stable, organization-defined network identifiers. **To specify an IP address or range** is correct because an administrator can define the address ranges used by a particular internal network or site, allowing the Endpoint Agent to classify its current location from its assigned IP address. **To specify domain names** is also correct because DNS domain information can identify a managed corporate network and can be used as a location criterion. These manually defined values are especially useful where automatic network detection is not sufficiently specific for the organization's topology, such as environments with multiple sites, segmented address spaces, or distinct DNS namespaces. The agent evaluates the configured location criteria to determine whether it is operating in the relevant endpoint location; that location can then be

used when applying location-aware endpoint policy behavior. Symantec's documentation portal provides the product documentation and administration guidance for Endpoint Agents and endpoint-location configuration: Broadcom Symantec Data Loss Prevention documentation. See also the Broadcom Support Knowledge Base for DLP Endpoint Agent configuration articles.

QUESTION NO: 13

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: D E

Explanation:

Form Recognition and **Indexed Document Matching (IDM)** are detection technologies supported by the Symantec DLP Endpoint Agent. Form Recognition enables endpoint policies to recognize sensitive information presented in known document-form layouts. The endpoint agent performs the required local inspection when users create, edit, copy, print, upload, or otherwise handle content through monitored endpoint channels. This lets an organization protect standardized business documents even when the sensitive values within those forms vary from one instance to another.

Indexed Document Matching uses an index generated from protected source documents. The DLP agent can use the distributed index to compare endpoint content against those indexed documents and identify protected material, including content that may have been modified from the original source. Because detection occurs at the endpoint, policy enforcement can take place before data leaves the managed device through channels such as removable storage, web traffic, email clients, or cloud applications. Broadcom's DLP documentation identifies the detection technologies and their supported enforcement locations, including Endpoint Prevent. See the Symantec Data Loss Prevention 16.1 documentation and the Symantec Data Loss Prevention product documentation downloads for the applicable detection-technology support matrices.