# ST0-237$^{\text{Q\&As}}$

Symantec Data Loss Prevention 12 Technical Assessment

## Pass Symantec ST0-237 Exam with 100% Guarantee

**QUESTION 1**

Which two actions should an organization take when deploying Endpoint Prevent according to Symantec best practices? (Select two.)

A. Test the agent on a variety of end-user images

B. Enable monitoring of the local file system

C. Enable monitoring of many destinations and protocols simultaneously

D. Configure, test, and tune filters

E. Delete the pre-defined filters and create its own

Correct Answer: AD

**QUESTION 2**

How are permissions to user-defined objects granted to individual users?

A. Permissions are automatically assigned by role.

B. A custom role must be created to grant access.

C. The administrator must manually assign permissions.

D. They are granted through Active Directory.

Correct Answer: C

**QUESTION 3**

Which command line diagnostic utilities would give a user the operating system version of the detection servers?

A. Environment Check Utility

B. Log Collection Utility

C. NormalizationConfigCheck.exe

D. SC.exe

Correct Answer: A

**QUESTION 4**

Which interface provides single sign-on access for the purpose of administering Data Loss Prevention servers, managing policies, and remediating incidents?

A. Symantec Information Manager

B. Symantec Protection Center

C. Symantec Data Insight

D. Symantec Messaging Gateway

Correct Answer: B

**QUESTION 5**

Which response rule condition allows a policy manager to configure an Automated Response rule to execute while a user is travelling?

A. Endpoint Location

B. Endpoint Device

C. Protocol or Endpoint Monitoring

D. Sender/User Matches Pattern

Correct Answer: A

**QUESTION 6**

How are incidents classified in a Network Prevent plus Data Loss Prevention for Tablets hybrid deployment?

A. All incidents are classified under the Network category.

B. Classification for all incidents depends on traffic destination.

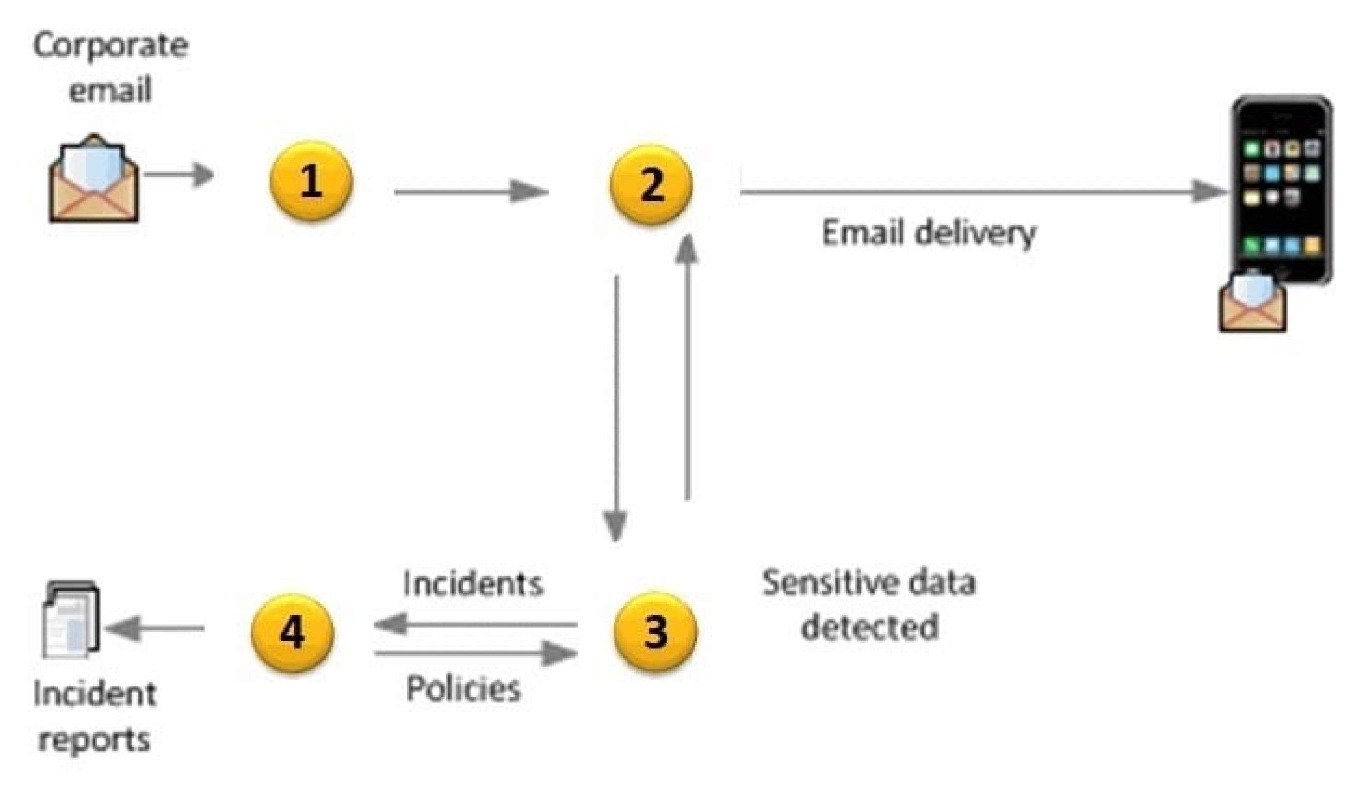
C. Incidents created by all traffic sources are generically categorized.

D. Incidents are classified specifically based on traffic source.

Correct Answer: D

**QUESTION 7**

Refer to the exhibit.



An administrator needs to implement a Mobile Email Monitor solution to inspect corporate emails on mobile devices. Where should the administrator place the web proxy?

A. 1

B. 2

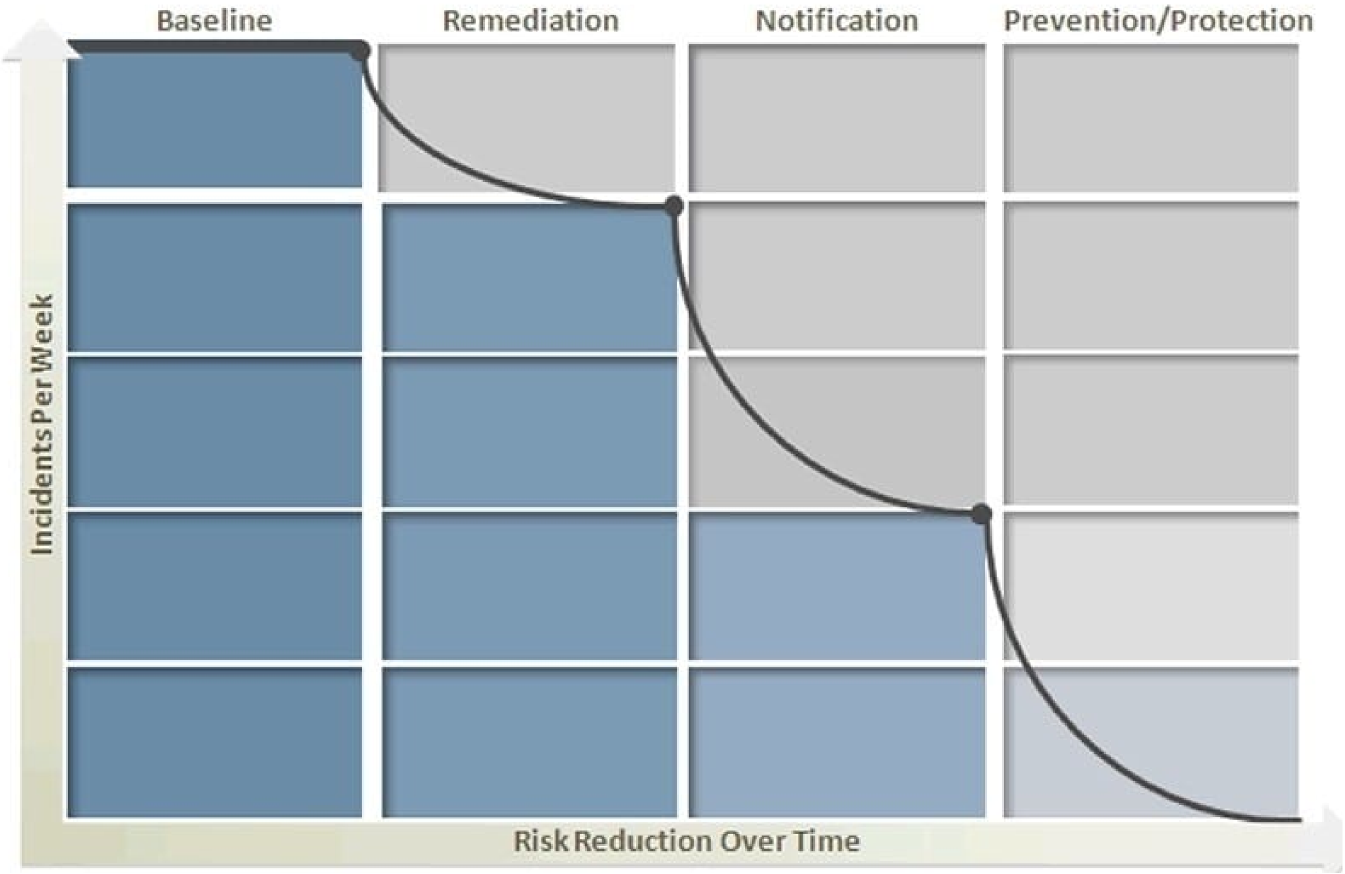
C. 3

D. 4

Correct Answer: B

**QUESTION 8**

Refer to the exhibit.



Symantec Data Loss Prevention\\'s four phases of risk reduction model provides a blueprint for identifying and remediating key risk areas without disrupting legitimate business activity. According to best practices, which option should be enabled during the baseline phase of policy risk reduction?

A. Change automated email responses

B. EDM/IDM detection

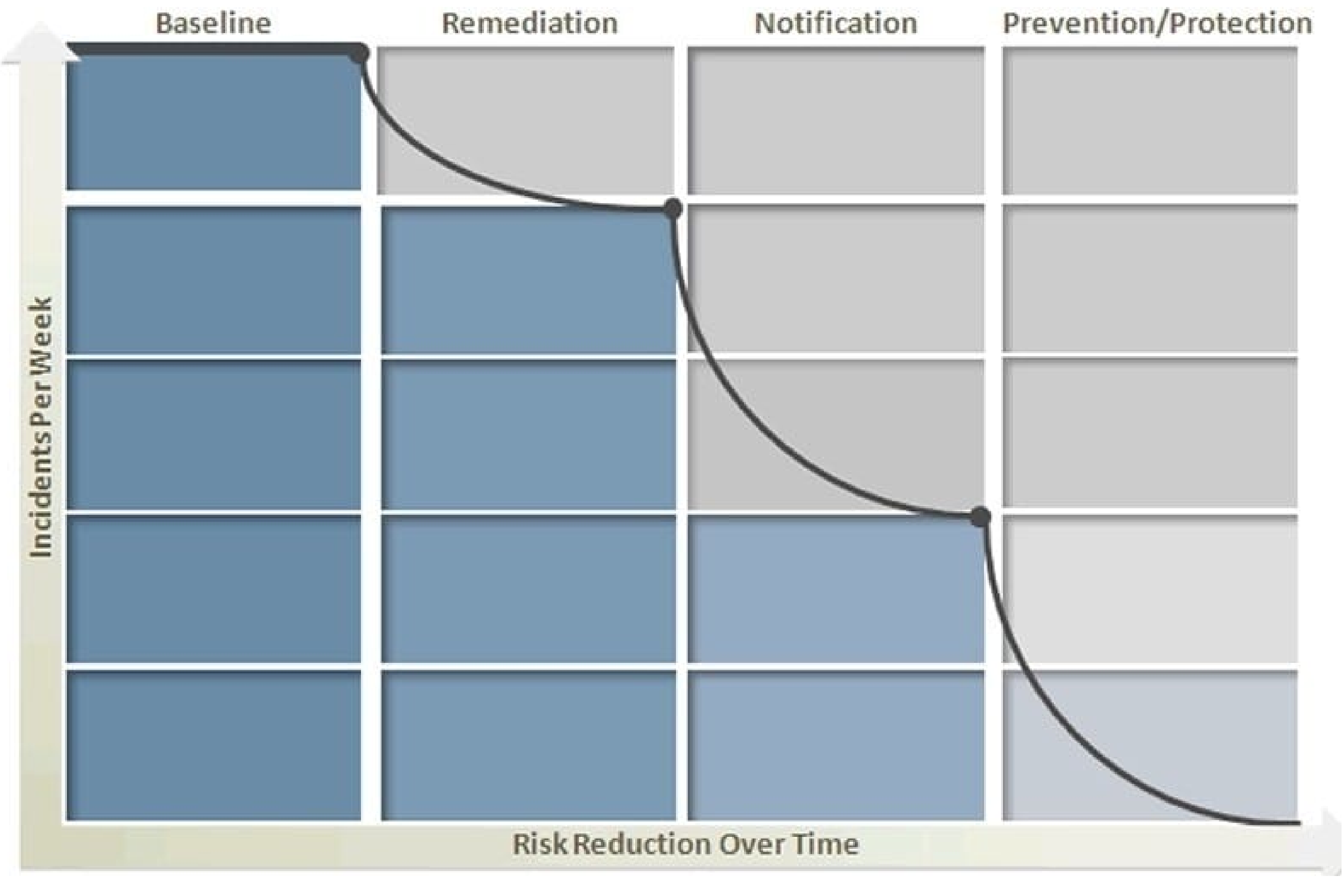
C. Use secure storage

D. Enable auto-encryption

Correct Answer: B

**QUESTION 9**

Refer to the exhibit.



Symantec Data Loss Prevention\\'s four phases of risk reduction model provides a blueprint for identifying and remediating key risk areas without disrupting legitimate business activity. What occurs during the notification phase?

A. Notification helps define confidential information and assign appropriate levels of protection to it using classifications.

B. On-Screen Pop-ups compare existing company information protection polices to best practices.

C. Notification helps develop a plan for integrating appropriate data security practices.

D. Automated sender notification educates employees in real-time about company policy violations.

Correct Answer: D

**QUESTION 10**

What is the most efficient method for designing filters to remove unwanted traffic?

A. policy-based exceptions

B. IP-based filtering per protocol

C. L7 filtering per protocol

D. sampling per protocol

Correct Answer: B

**QUESTION 11**

Which two pieces of system information are collected by Symantec Data Loss Prevention Supportability Telemetry? (Select two.)

A. Currently installed version of the Enforce Server

B. Number of policies currently deployed

C. Cumulative statistics regarding network traffic

D. File types for which there are incidents

E. Number of system alerts generated daily

Correct Answer: AD

**QUESTION 12**

When collecting data from assets, what is the primary factor in determining the types of data that will be collected?

A. scope

B. standard

C. baseline

D. reference asset

Correct Answer: B

**QUESTION 13**

After an exception has been requested, which three approver actions are valid? (Select three.)

A. set the exception request state to In Review

B. forward the exception request to an alternate approver

C. deny the exception request

D. delete the exception request

E. request clarification for the exception request

Correct Answer: ACE

**QUESTION 14**

Which log should be reviewed first if a database issue is suspected?

A. manager_operational.log

B. alert_.log

C. enforce_diagnostics.log

D. manager_jdbc.log

Correct Answer: B

**QUESTION 15**

An administrator is running a Discover Scanner target scan and the scanner is unable to communicate back to the Discover Server.

Where will the files be stored?

A. Discover Server incoming folder

B. scanner\\'s outgoing folder

C. scanner\\'s incoming folder

D. Enforce incident persister

Correct Answer: B