I S L E V E R

250-512

Administration of Symantec Data Loss
Prevention 11.5

DEMO

https://www.islever.com/250-512.html
https://www.islever.com/symantec.html

Topic 1, Volume A

QUESTION NO: 1

Silent installation can be performed for which component of Symantec Control Compliance Suite 9.0?

A. directory server
B. Data Processing Service
C. application server
D. Response Assessment Module

Answer: B
Explanation:

QUESTION NO: 2

What are two benefits that data loss prevention solutions provide? (Select two.)

A. Provide accurate measurement of encryption strength
B. Give insight into capacity planning for sensitive data
C. Identify who has access to sensitive data
D. Indicate where sensitive data is being sent
E. Meet data retention requirements for business continuity

Answer: C,D
Explanation:

QUESTION NO: 3

What is the minimum number of computers required to configure each Data Processing Service role?

A. 1
B. 2
C. 3
D. 4

Answer: A
Explanation:

QUESTION NO: 4

What are two reasons why a company should implement data loss prevention? (Select two.)

A. To prevent the threat of malware
B. To demonstrate regulatory compliance
C. To protect the CISO from liability due to a security breach
D. To prevent employee malicious activity
E. To protect brand and reputation

Answer: B,E
Explanation:

QUESTION NO: 5

Which three Enterprise Security Manager policy-run options can be configured in Symantec Control Compliance Suite 9.0? (Select three.)

A. Collect data from last policy run
B. Run policy before collecting data
C. Collect data from last n policy runs
D. Run policy n days before collecting data
E. Run policy if data is older than n days

Answer: A,B,E
Explanation:

QUESTION NO: 6

From which organization are Symantec Control Compliance Suite 9.0 Predefined Standards most commonly derived?

A. National Institute of Standards and Technology
B. National Security Agency
C. Center for Internet Security
D. International Organization for Standardization

Answer: C
Explanation:

QUESTION NO: 7

What is the main difference between data loss prevention and other security technologies?

A. It is designed to take a content aware approach to security.
B. It determines the data owner of inbound sensitive information.
C. It quarantines adware before it is able to extract confidential information.
D. It is designed to give visibility into where the company's least sensitive data is stored.

Answer: C
Explanation:

QUESTION NO: 8

Which two statements describe an effective Data Loss Prevention (DLP) program? (Select two.)

A. DLP is best implemented as a departmental initiative.
B. The desktop team primarily manages DLP.
C. DLP eliminates the need to document an incident response workflow.
D. Employee education is important.
E. Business stakeholders are held accountable for risk reduction.

Answer: D,E
Explanation:

QUESTION NO: 9

Which two are prerequisites for importing assets into the asset system for the first time? (Select two.)

A. New asset types must be defined.
B. User-defined reconciliation must be created.
C. An asset filter must be defined.
D. At least one data collector must be configured.
E. A Data Processing Service must be registered to a site.