

Symantec ST0-192

**Symantec Tech. Found: Security Solutions 2.0 Tech.
Assmt.
Version: 4.0**

QUESTION NO: 1

Which two events could potentially be seen by a network monitoring solution in the context of information protection? (Select two.)

- A. an employee sharing their login credentials with another person
- B. a hacker exfiltrating data out of an organization
- C. an employee emailing data out of an organization
- D. an employee on their home ISP webmailing confidential data
- E. a malicious insider copying files to a removable storage device

Answer: B,C

Explanation:

QUESTION NO: 2

What is an example of monitoring the usage of confidential data?

- A. tracking file copy operations between users in an organization
- B. blocking a file going to an external USB device
- C. checking firewall logs for file access history
- D. inspecting data being emailed out of an organization

Answer: D

Explanation:

QUESTION NO: 3

What makes a security policy effective and functional?

- A. technical detail
- B. user education
- C. support from management
- D. strict enforcement

Answer: C

Explanation:

QUESTION NO: 4

Which process can be integrated with patch management to reduce deployment time and risk to the business?

- A. remediation management
- B. vulnerability management
- C. release management
- D. change management

Answer: D

Explanation:

QUESTION NO: 5

What does patch management need to accurately target computers within an environment?

- A. a system management software package
- B. an accurate up-to-date list of patches
- C. an endpoint management system
- D. an accurate up-to-date inventory

Answer: D

Explanation:

QUESTION NO: 6

Which condition would require performing a remote exploit on a machine?

- A. presence of a malicious insider
- B. end-users leaking sensitive data
- C. unpatched system
- D. anonymous FTP login allowed

Answer: C

Explanation:

QUESTION NO: 7

Which two pieces of information from a customer will help to uncover a need for the Altiris IT Management Suite? (Select two.)

- A. whether the customer is planning to migrate to Windows 7
- B. whether the customer is going to be deploying Google Android tablets or other mobile devices.
- C. whether the customer requires reports on vulnerability information
- D. whether the customer allows users to connect to their network via VPN using cloud enabled management
- E. whether the customer needs to prioritize and quickly deploy patches

Answer: A,E

Explanation:

QUESTION NO: 8

Which two questions are appropriate to ask a customer in order to uncover a need for Symantec Control Compliance Suite? (Select two.)

- A. Are you meeting your required backup windows?
- B. Have you recently gone through a merger or acquisition, requiring new entitlements and controls?
- C. Do you need to archive email for legal discovery purposes?
- D. Is your operations team struggling to keep on top of IT audit-related tasks?
- E. Do you need to ensure critical servers are deployed by authorized personnel?

Answer: B,D

Explanation:

QUESTION NO: 9

Which information from a customer helps to uncover a need for Symantec Data Loss Prevention?

- A. how servers with data are deployed and patched
- B. where confidential data is stored and how it is being used and managed
- C. the types of servers in the data center
- D. how employees back up data on their laptops and cell phones

Answer: D

Explanation:

QUESTION NO: 10

Which analysis techniques increase detection of unstructured confidential data?

- A. Collection of all known confidential data items to create a fingerprinting profile.
- B. Analysis of a sample set of data items which is used to create a statistical profile.
- C. Generation of a keyword list that is used to create a detection profile.
- D. Data matching content analysis that uses a compiled description of collected known confidential data.

Answer: B

Explanation:

QUESTION NO: 11

What is an example of why context is important for accurate detection of confidential data?

- A. Detection of both structured and unstructured confidential data is important.
- B. Detection technologies need to hold up under a heavy production load.
- C. Unstructured data can contain significant confidential data.
- D. Confidential data going to a trusted partner may be acceptable.

Answer: D

Explanation:

QUESTION NO: 12

What are two types of targets that should be scanned to see if they contain confidential information at rest? (Select two.)

- A. firewalls
- B. routers
- C. file servers
- D. encryption gateways
- E. databases

Answer: A,B

Explanation:

QUESTION NO: 13

What are two components of the policy management lifecycle according to the Security Solutions 2.0 course? (Select two.)

- A. manage
- B. develop
- C. review
- D. authorize
- E. secure

Answer: B,C

Explanation:

QUESTION NO: 14

What is the primary goal when creating a security policy?

- A. to assist in the compliance process
- B. to ensure that procedures are followed
- C. to protect information
- D. to enforce system configurations

Answer: C

Explanation:

QUESTION NO: 15

What standardized management process is used to coordinate the impact of incidents and other issues affecting a business caused by errors within the Information Technology infrastructure?

- A. Release Management
- B. Incident Management
- C. Change Management
- D. Problem Management

Answer: D

Explanation:

QUESTION NO: 16

What drives consultative conversations and establishes credibility with an organization?

- A. establishing a security policy
- B. providing industry insight
- C. providing regulatory information
- D. establishing business policies

Answer: B

Explanation:

QUESTION NO: 17

What is an example of fan-out remediation involving information protection incidents?

- A. Incidents are verified and upon management approval escalated to the incident response team
- B. Incidents go to an escalation team and then to a core incident response team.
- C. First incidents levels are baselined, then monitored, and then blocked.
- D. Incidents go to a core incident response team and then to an escalation team.

Answer: D

Explanation:

QUESTION NO: 18

What are the deployment phases of an information protection solution?

- A. workflow, quarantine, remediation, and compliance
- B. endpoint, network, storage, and protection
- C. baseline, remediation, notification, and prevention
- D. baseline, workflow, policies, and prevention

Answer: C

Explanation: