

# ***KillTest***

Higher Quality, Better Service!



## **Q&A**

<http://www.killtest.com>

We offer free update service for one year.

**Exam** : **ST0-095**

**Title** : Symantec Technical  
Foundations: Security  
Solutions 1.0 (STS)

**Version** : Demo

1. What is the primary purpose of change control in the context of security?

- A. to apply changes that increase security posture
- B. to prevent changes from decreasing security posture
- C. to automatically apply security changes on a set schedule
- D. to automatically undo changes that cause security problem

Answer: B

2. What are most organizations concerned with when looking at risk as it relates to impact on an asset?

- A. downtime
- B. revenue
- C. response time
- D. exposure

Answer: B

3. How does a denial of service attack work?

- A. It attempts to break the authentication mode.
- B. It imitates the behavior of a valid user.
- C. It cracks passwords, causing the system to crash.
- D. It prevents a legitimate user from using a system or service.

Answer: D

4. Which Symantec solution can identify and block a malicious file from being downloaded in an HTTP session?

- A. Web Gateway
- B. Brightmail Gateway
- C. Network Access Control
- D. Critical System Protection

Answer: A

5. customer is experiencing image-based spam and phishing attacks that are negatively impacting messaging flow. Which Symantec solution should be recommended to this customer?

- A. Brightmail Gateway
- B. Endpoint Protection
- C. Network Access Control
- D. Backup Exec System Recovery

Answer: A

6. Which challenge does security information and event management (SIEM) help solve for customers?

- A. monitoring for performance problem on servers
- B. monitoring configuration changes in applications
- C. monitoring for business compliance issues
- D. monitoring for security violations

Answer: D

7. What are traditional, definition-based malware scanning technologies unable to identify?

- A. new or unique threats unless a sample has been submitted
- B. older threats or threats that are inactive in the wild
- C. polymorphic threats that have been discovered in an antivirus lab
- D. threats that are written to temporary locations in storage

Answer:

8. What is one of the benefits of the assessment step within the security policy lifecycle, according to the Security Solutions 1.0 course?

- A. It provides the actionable configuration standards.
- B. It allows organizations to understand where critical assets reside.
- C. It educates the employees and manages the enforcement of a products.
- D. It analyzes the policy through interviews.

Answer: B

9. Malware that contains a backdoor is placed on a system that will later be used by the cybercriminal to gain access to the system. The cybercriminal was successful in which phase of the breach?

- A: capture
- B: discovery
- C: incursion
- D: exfiltration

Answer: C

10. 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? DE. Do you need to ensure critical servers are deployed by authorized personnel?

11. minimize

Answer:

11. What is a key benefit of integrating multiple security-related solutions?

- A. automates administration across multiple security solutions
- B. develops IT security policies across security solutions
- C. consolidates critical data from separate security solutions
- D. enforces user policies across unrelated security solutions

Answer: C

12. Which type of breach source is Albert Gonzalez, as mentioned in the Security Solutions 1.0 course?

- A. well-meaning insider
- B. malicious insider
- C. cybercriminal
- D. disgruntled employee

Answer: C

13. What is a benefit of a security awareness program, according to the Security Solutions 1.0 course?

- A. It provides an understanding of current system security settings.
- B. It allows the organization to understand where critical systems reside.
- C. It provides an understanding of the operational costs of security.
- D. It ensures that employees understand their roles and responsibilities.

Answer:

14. What is the purpose of defining a technical standard?

- A. to identify minimum system configuration requirements for assets
- B. to define roles and responsibilities within an organization
- C. to create documented exceptions or waivers to a policy
- D. to implement the guidelines directed by management

Answer: A

15. A cybercriminal wants to break into an organization using a SQL injection attack. What will the cybercriminal do to start the attack?

- A. enter a command at a user prompt
- B. locate a user input field on the company's web page
- C. gain administrative access to the database
- D. use SQL slammer malware

Answer: B

16. How do the security program approaches rank in order from least mature to most mature?

- A. compliance, risk, IT security
- B. risk, compliance, IT security
- C. IT security, compliance, risk
- D. IT security, risk, compliance

Answer: C

17. What should be in place before automatically blocking confidential data leaving the organization?

- A. hard drive encryption
- B. well-refined data loss policies
- C. email message encryption
- D. endpoint management software

Answer: B

18. An employee has installed a video game on their company-issued laptop. Which Symantec solution can prevent this installation in the future?

- A. Altiris IT Management Suite
- B. Endpoint Encryption
- C. Brightmail Gateway
- D. Security Information Manager

Answer: A

19. Which framework is used to manage change within an IT organization?

- A. Management of Risk (MOR)
- B. Information Technology Asset Management (IT AM)
- C. Information Technology Infrastructure Library (ITIL)
- D. Control Objectives for Information and Related Technology (CobiT)

Answer: C

20 An employee's computer was recently infected by a virus due to opening an attachment received through email. Which Symantec solution could have prevented this?

- A. Brightmail Traffic Shaper
- B. Brightmail Gateway
- C. Network Access Control
- D. Data Loss Prevention

Answer: B

21. An administrator wants to identify and monitor systems with weak or static passwords. Which Symantec solution can help collect this information?

- A. Data Loss Prevention
- B. Endpoint Protection
- C. Critical System Protection
- D. Control compliance Suite

Answer: D

22. What does the Control Objectives for Information and Related Technology (CobiT) framework focus on, according to the Security Solutions 1.0 course?

- A. IT implementation life cycle
- B. computer security concepts
- C. international security procedures for audit
- D. confidentiality, integrity, and availability

Answer: A

23. What is a critical success factor when implementing workflow software?

- A. It should work well with application integration software.
- B. It should work well with web security software.
- C. It should work well with bug tracking infrastructure.
- D. It should work well with network access controls.

Answer: A

24. Which type of attack would be most successful against the password T63k#s23A?

- A. cross site scripting
- B. brute-force
- C. dictionary

D.SOL injection

Answer: B

25. Which two benefits does patch management provide an organization? (Select two.)

- A. modifies usability or performance of a computer
- B. removes vulnerabilities through software fixes
- C. updates operating systems and ensures compliance
- D. migrates the operating system
- E. counts software licenses installed

Answer: B,C

26. Which WO topics did Art Gilliland state in the Security Solutions 1.0 course as areas that Symantec plans to invest in? (Select WO.)

- A. reputation-based security
- B. identity management
- C. cryptography
- D. cross-product management and reporting
- E. security of social networking sites

Answer: A,D

27. What do software patches affect within a company's environment?

- A. applications only
- B. operating systems only
- C. operating systems and applications only
- D. operating systems, applications, and hardware configurations

Answer: C

28. What is the primary goal when creating a security products?

- A. to assist in the compliance process
- B. to ensure systems have updated patches
- C. to protect information
- D. to report on system configuration

Answer: C

29. What is the primary benefit of a people-based workflow solution?

- A. business process creation
- B. centrally managed collaboration
- C. coordination of web services
- D. user-based task assignment

Answer: B

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

- A. a program storing social security numbers in a SOL database

- B. a hacker exfiltrating data out of an organization
- C. a malicious insider emailing data out of an organization
- D. an employee on their home ISP webmailing confidential data
- E. an administrator incorrectly configuring email servers

Answer: B,C