Vendor: Symantec

Exam Code: ST0-095

Exam Name: 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. 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

8. What is one of the benefits of the assessment step within the security policylifecycle, 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 policythrough 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. 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