

Exam : Symantec ST0-025

**Title : Symantec Security
Information Manager 4.5
(STS)**

Version : Demo

1. Symantec Security Information Manager Series Appliance installs which operating system by default?

- A. Solaris
- B. Windows
- C. SUSE
- D. Red Hat

Answer: D

2. How do you install a valid DeepSight Integration License?

- A. open the Symantec Security Information Manager Console; select Configure Appliance; click on DeepSight Integration Manager Configuration
- B. open Symantec Security Information Manager Console; select Configure Appliance; click on Licenses
- C. on the appliance, place the license in the /opt/Symantec/license folder
- D. use the Install License Wizard

Answer: A

3. You are in the process of installing and configuring a new Symantec Security Information Manager (SSIM) solution. Your company uses a CheckPoint firewall.

Which two tasks must you perform to allow the CheckPoint collector to receive log information from the CheckPoint firewall? (Choose two.)

- A. create the OPSEC application
- B. configure CheckPoint ACL to communicate with the SSIM appliance
- C. configure the CheckPoint LEA server
- D. configure CheckPoint to forward syslog events to the SSIM appliance

Answer: AC

4. Which Symantec Security Information Manager feature provides a centralized list of the hosts and devices in a network that are subject to security event correlation?

- A. Assets Table
- B. Correlation Database
- C. Host Table

D. Security Object Database

Answer: A

5. When an event is received by the Symantec Security Information Manager (SSIM), the Event Logger component inserts events into the archive without doing other processing. This is the default behavior. Depending on the configuration and the components installed on the SSIM, how can the inserted events be processed?

- A. correlate events
- B. filter events
- C. isolate events
- D. send the events to SSIM internal compiler

Answer: A

6. How does Symantec Security Information Manager allow the user to modify the tables in the event data archive?

- A. add, delete, and modify pre-existing columns
- B. add, delete, and rename predetermined columns
- C. add, delete, and reorganize predetermined rows
- D. add, delete, and reorganize predetermined columns

Answer: D

7. Which three are valid file archive suffixes? (Choose three.)

- A. .xml
- B. .sar
- C. .csv
- D. .ndx
- E. .vdx

Answer: BDE

8. What is the purpose of the critical business assets management feature?

- A. It enables automatic identification and prioritization of security threats that impact business-critical applications.
- B. It obtains an overview of business assets.
- C. It makes it possible to change collectors' configurations to meet business assets needs.
- D. It provides a visual picture of where critical business assets are located.

Answer: A

9. How can an organization connect to the Integrated Global Security Intelligence to receive updates?

- A. by licensing the Integrated Global Security Intelligence product
- B. by licensing the DeepSight Security feature Global Security Intelligence product
- C. by enabling this feature within the console
- D. by using the default settings within the console

Answer: B

10. The Symantec Security Information Manager includes a(n) _____ feature that allows the security administrator to instantly access a customized view of major security indicators.

- A. reports
- B. intelligence page
- C. dashboard
- D. events

Answer: C

11. From the Information Manager Console, the _____ feature allows you to prioritize remediation efforts on critical network devices.

- A. assets
- B. reports
- C. rules
- D. tickets

Answer: A

12. On the Information Manager's Console, you can select the _____ tab to determine who is working on a problem.

- A. Tickets
- B. Reports
- C. Incidents
- D. Events

Answer: A

13. Which tab on the Information Manager Console allows you to view threat and vulnerability information?

- A. Rules
- B. Dashboard
- C. Reports
- D. Intellegence

Answer: D

14. Symantec Security Information Manager automatically escalates security events into incidents based on a number of pre-defined and user-defined _____.

- A. rules
- B. events
- C. incidents
- D. tickets

Answer: A

15. Once all rules are properly defined, the Correlation Engine can analyze events against _____.

- A. the rule criteria, create triggers, and correlate conclusions into incidents
- B. false positives, create conclusions, and correlate conclusions into incidents
- C. the rule criteria, create conclusions, and correlate conclusions into incidents
- D. the rule criteria, create conclusions, and send conclusions to the database

Answer: C

16. Symantec Security Information Manager ____ Series provides dynamic correlation and centralized management of large, distributed enterprise deployments.

- A. 9600
- B. 9630
- C. 9650
- D. 9850

Answer: C

17. What are the hard drive specifications for the 9650?

- A. 6 drives (2 mirrored and 4 in RAID 5)
- B. 6 drives (2 mirrored and 4 in RAID 10)
- C. 6 drives (RAID 5)
- D. 2 drives (mirrored)

Answer: A

18. Which third-party software components support LDAP for users, roles, and configurations?

- A. IBM Directory Server 6.0
- B. IBM Directory Server 7.0
- C. IBM DB2 8.1
- D. IBM DB2 8.2

Answer: A

19. Which database houses incidents and summary data?

- A. Oracle
- B. MySQL
- C. MSSQL
- D. IBM DB2

Answer: D

20. Which general release version of JRE is installed with the product?

A. 1.4.2

B. 1.2

C. 1.5.0

D. 2.0

Answer: C