# ST0-025

# Symantec Security Information Manager 4.5

**Version 3.1**

# ST0-025

**Topic 1, Volume A**

**QUESTION NO:** 1

What are two ways in which new entries can be added to the Assets Table of a Symantec Security Information Manager solution? (Choose two.)

A. through the Lookup Tables pane of the Information Manager Console

B .importing from HP OpenView through the OpenView Integration feature

C. importing from a .CSV file exported from Active Directory

D. automatic population through a supported vulnerability scanner

**Answer:** C, D

**QUESTION NO:** 2

Which three ratings does the Information Manager Assets Table use to quantify the importance of the device and help determine how to escalate security incidents related to that device? (Choose three.)

A. Confidentiality

B. Criticality

C. Availability

D. Priority

E. Integrity

**Answer:** A, C, E

**QUESTION NO:** 3

How can you determine which ports are potentially vulnerable on a given host in the Assets Table?

A. by running the NetScan user action on the asset

B. by looking at the Services tab on the asset

C. by viewing the Details tab for the asset

D. by running the Host Information report on the asset

**Answer:** B

**QUESTION NO:** 4

How do you install the Symantec Security Information Manager (SSIM) Console?

A. on the SSIM DVD, go to Tools and install the client

B. go to the SSIM web interface, download the client and click Run

C. from the SSIM appliance, deploy the console to your machine

D. No installation is necessary because SSIM is a browser-based tool.

**Answer:** B

**QUESTION NO:** 5

Which menu options do you select in the user interface to shut down or reboot the Symantec Security Information Manager (SSIM) appliance?

A. System --> Shutdown/Restart

B. SSIM Console --> Shutdown/Restart

C. SSIM --> Configure Appliance --> Shutdown/Restart

D. SSIM Console --> Systems tab

**Answer:** C

**QUESTION NO:** 6

Where do you configure LiveUpdate for Symantec Security Information Manager (SSIM)?

A. SSIM Start Page --> Configure Appliance --> LiveUpdate tab

B. SSIM Console --> Systems tab --> LiveUpdate tab

C. from a command prompt

D. SSIM Client --> Maintenance tab --> LiveUpdate tab

**Answer:** A

**QUESTION NO:** 7

By default, event archives are stored for up to _____ days.

A. 10

B. 30

C. 60

D. 90

**Answer:** A

**QUESTION NO:** 8

# ST0-025

Which two are commonly used to view archived events? (Choose two.)

A. Information Manager Event Viewer

B. Archive Management Console tab

C. Query Wizard

D. Incident Management Console tab

**Answer:** A, C

**QUESTION NO:** 9

When querying archived event data, how can you make a query available to other users of the system?

A. save it in Published Queries

B. save it in Public Templates

C. grant Read Query permission to the domain

D. check the Shared option on the saved query

**Answer:** A

**QUESTION NO:** 10

Normalization provides a unique identifier for each type of event and _____.

A. adds Correlation Manager-specific data to the translated incident

B. adds Correlation Manager-specific data to the translated event

C. maps events to a device-specific signature

D. maps incidents to a device-specific signature

**Answer:** B

**QUESTION NO:** 11

What is the correct Symantec Security Information Manager incident identification pipeline?

A. collection --> normalization --> rule processing --> attack tracing --> correlation to vulnerabilities --> incident prioritization

B. normalization --> collection --> rule processing --> attack tracing --> correlation to vulnerabilities --> incident prioritization

C. rule processing --> normalization --> collection --> attack tracing --> correlation to vulnerabilities --> incident prioritization

D. attack tracing --> rule processing --> normalization --> collection --> correlation to vulnerabilities --> incident prioritization

**Answer:** A

**QUESTION NO:** 12

Security data is continuously gathered from thousands of security sensors worldwide through the integrated _____.

A. Symantec Security Information Manager

B. DeepSight Global Intelligence Network

C. Symantec Enterprise Security Manager

D. Symantec Sygate Solution

**Answer:** B

# ST0-025

**QUESTION NO:** 13

What is the purpose of normalization?

A. to minimize the number of events affecting multiple devices for the Correlation Manager to strategize the events more quickly

B. to correlate events across multiple devices for the Correlation Manager to compare all events equally

C. to standardize events across multiple devices for the Correlation Manager to compare all events equally

D. to process the events across multiple devices for the Correlation Manager to strategize the events more quickly

**Answer:** C

**QUESTION NO:** 14

What is Device-level aggregation?

A. parsing data with data sensors

B. grouping data to reduce traffic and database size

C. forwarding event data to the appliance

D. event and log sensoring

**Answer:** B

**QUESTION NO:** 15

What are on-box collectors?

A. PIX, UNIX Syslog and Sygate

B. Checkpoint, Snort and PIX

C. PIX, Snort and Symantec Mail Security

D. Checkpoint, UNIX Syslog and Symantec Network Security

**Answer:** B

**QUESTION NO:** 16

Which Symantec Security Information Manager component retrieves security content from Symantec?

A. LiveUpdate

B. LiveUpdate and licensed DeepSight Integration Module simultaneously

C. Licensed DeepSight Integration Module

D. Security content retrieval is automatic.

**Answer:** C

**QUESTION NO:** 17

In Symantec Security Information Manager, collectors send events to _____.

A. Event Disposition

B. Event Archive

C. Event Reporting

D. Event Logger