ST0-025

Symantec Security Information Manager 4.5 (STS)

DEMO

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

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 theNetScan 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

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