Vendor: Symantec

Exam Code: ST0-085

Exam Name: Symantec Security Information Manager 4.7 Technical Assessment

Version: Demo

QUESTION NO: 1

Which two default administrative user accounts are created during the installation of Symantec Security Information Manager? (Select two.)

A. Root Administrator
B. Domain Administrator
C. SES Administrator
D. System Administrator E. Local Administrator

Answer: B,C

QUESTION NO: 2

When are the effective privileges of the SES Administrator role and Domain Administrator role equivalent?

A. when there is only one domain in the system
B. when the administrator is assigned the SES Administrator role
C. when the system is newly installed and a domain has not yet been created
D. when the Domain Administrator role is given permission to create users and roles

Answer: A

QUESTION NO: 3

Which role is able to modify permissions within the Symantec Security Information Manager solution?

A. DB2 Administrator
B. Root Administrator
C. System Administrator
D. Domain Administrator

Answer: D

QUESTION NO: 4

How many days of data is stored in the archives before it is purged?

A. 10
B. 30
C. 60
D. unlimited

Answer: D

QUESTION NO: 5

When configuring the Event Archive settings of an Information Manager appliance, which two options can be configured? (Select two.)

A. Auxiliary Storage Device
B. Max Archive Quota
C. Free disk space
D. Purge Start Time
E. Purge certain events

Answer: B,C

QUESTION NO: 6

Which is commonly used to view archived events?

A. Information Manager Event Viewer
B. Archive Management Console tab
C. Event Viewer API
D. Incident Management Console tab

Answer: A

QUESTION NO: 7

Which two user actions can be executed by the Information Manager Event Viewer by default? (Select two.)

A. Finger
B. ping
C. touch
D. nslookup
E. whois

Answer: A,B

QUESTION NO: 8

Which two search templates are pre-defined by Information Manager? (Select two.)

A. Host Activity
B. Internal Activity
C. IDS Activity
D. Firewall Activity
E. Port Activity

Answer: A,E

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: D

QUESTION NO: 10

What is the common way in which new entries can be added to the Assets Table of a Symantec Security Information Manager solution?

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 rule that is monitoring traffic on the network
D. automatic population through a supported vulnerability scanner

Answer: D

QUESTION NO: 11

Which statement is true about rules in a Symantec Security Information Manager solution?

A. Rules can be created that escalate events to incidents, based on policies defined on each asset.
B. The Rules Editor can create policies on each asset to determine what rules are executed when an event occurs.
C. Rules can be configured on each asset that will launch a vulnerability scan when a specific type of event occurs.
D. The Rules tab can be used on the console to automatically identify available ports on an asset.

Answer: A

QUESTION NO: 12

Which two 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? (Select two.)

A. Confidentiality

B. Criticality
C. Severity
D. Priority
E. Integrity

Answer: A,E

QUESTION NO: 13

What are two ways the Assets Table can reduce the reporting of false positive security incidents using built-in functionality? (Select two.)

A. assigns proper CIA values to each asset in the table
B. schedules daily updates of vulnerability information from Symantec's LiveUpdate service
C. populates the Policies tab with policies that apply to each asset
D. uses a supported vulnerability scanner to help prioritize incidents
E. configures normalization of event data captured by the collectors

Answer: C,D

QUESTION NO: 14

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:15

What information is reported by the Nessus scanner when it scans a range of network addresses?

A. configuration data of discovered devices
B. vulnerabilities of discovered network devices
C. patch levels installed on discovered devices
D. the SANS risk level of each discovered device

Answer: B

QUESTION NO: 16

Which service provides Symantec Security Information Manager with updated intelligence about threats?

A. Symantec Security Information Manager
B. DeepSight Global Intelligence Network
C. Symantec Enterprise Security Manager
D. Symantec Endpoint Protection

Answer: B

QUESTION NO: 17

What type of data that comes from DeepSight is mapped to vulnerability, exposure, malicious code, and safeguard mitigation strategies?

A. normalized event signatures
B. correlated incident activities
C. relationships between events
D. correlated event activities

Answer: A

QUESTION NO: 18

Which option allows events to be ignored by the Correlation Rules and no longer be processed?

A. Bypass Rules
B. Conditions
C. Criteria
D. Event Filters

Answer: D

QUESTION NO: 19

Which option in the Rules Monitors list allows for follow-up actions that are required to resolve the incident?

A. Monitors list
B. Actions
C. Properties
D. History

Answer: B

QUESTION NO: 20

Which source is used by Symantec Security Information Manager to create incidents?

A. SANS Internet Storm Center
B. Assets Table
C. analyst input
D. Correlation Rules

Answer: D

QUESTION NO: 21

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: 22

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: 23

What is the unique identifier that normalization provides for each type of event?

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