2014 Latest Pass4sure&Lead2pass Symantec ST0-085 Dumps (1-10)

QUESTION 1
Which database houses incidents and summary data?

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

Answer: C

QUESTION 2
Which component sends events to the Event Service for processing?

A. the Symantec Security Information Manager (SSIM) collector
B. the Symantec Security Information Manager (SSIM) on-box collector
C. the Symantec Security Information Manager (SSIM) off-box collector
D. the Symantec Security Information Manager (SSIM) agent

Answer: D

QUESTION 3
What is the difference between Symantec Security Information Manager (SSIM) on-box and off- box collectors?

A. Off-box collectors are installed on the SSIM products and on-box collectors are installed on the appliance.
B. On-box collectors are installed prior to SSIM software installation and off-box collectors are installed separately.
C. On-box collectors are automatically installed with the SSIM software and off-box collectors are installed separately.
D. Off-box collectors are installed on the appliance and on-box collectors are installed on assets.

Answer: C

QUESTION 4
Which Symantec Security Information Manager component retrieves security content in near-real- time from Symantec?

A. LiveUpdate
B. LiveUpdate and licensed
C. DeepSight Integration Module simultaneously
D. Licensed DeepSight Integration Module
E. Security content retrieval is automatic.

Answer: C

QUESTION 5
Which of the following are all on-box collectors?

A. PIX, UNIX Syslog and Data Leakage Prevention
B. Checkpoint, Snort and PIX

C. PIX, Snort and Symantec Web Gateway
D. Checkpoint, UNIX Syslog and Control Compliance Suite

Answer: B

QUESTION 6
On which two operating systems can the Symantec Security Information Manager Agent be installed? (Select two.)

A. Solaris 9
B. Windows 2000
C. Centos
D. IBM AIX 5
E. HP-UX 11

Answer: AB

QUESTION 7
Where do Symantec Security Information Manager collectors send events?

A. Event Disposition
B. Event Archive
C. Event Reporting
D. Event Logger

Answer: D

QUESTION 8
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 logcensoring

Answer: B

QUESTION 9
What information must be obtained prior to product deployment and configuration of the Symantec Security Information Manager appliance?

A. which on-box collectors are appropriate for installation
B. the number of nodes found in the customer's infrastructure
C. the number of security events per day the appliance will handle
D. the air-conditioning and power requirements

Answer: C

QUESTION 10
What information is necessary to properly size a deployment?

A. hard drive space, events per second and geographic locations
B. events per second,collector types and incident-to-event ratio
C. hard drive space, incidents per second and collector types
D. events per second, geographic locations and event-to-incident ratio

Answer: D

If you want to pass Symantec ST0-085 successfully, donot missing to read latest lead2pass Symantec ST0-085 practice tests. If you can master all lead2pass questions you will able to pass 100% guaranteed.

http://www.lead2pass.com/ST0-085.html