2014 Latest Pass4sure&Lead2pass Symantec ST0-085 Dumps (81-90)

QUESTION 81
What is the difference between Symantec Security Information Manager (SSIM) on-box and off- box collectors?
"Pass Any Exam. Any Time." - www.actualtests.com 36
Symantec ST0-085 Exam

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 82
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 83
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 84
On which three operating systems can the Symantec Security Information Manager Agent 2.5 be
"Pass Any Exam. Any Time." - www.actualtests.com 37
Symantec ST0-085 Exam
installed?

A. Solaris 9
B. Windows 2000
C. Red Hat 3
D. IBM AIX 5
E. HP-UX 11

Answer: ABC

QUESTION 85
In Symantec Security Information Manager, collectors send events to _____.

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

Answer: D

QUESTION 86
What does the Secure Sockets Layer (SSL) protocol use?

A. Transport Layer Protection, Session-based communication and Trusted Certificates
B. Transport Layer Protection, Session-based communication and Agents to appliance
C. Transport Secure Layer, Session-based communication and Trusted Certificates
D. SSH File Transfer Protocol, Session-based communication and Trusted Certificates

Answer: A

QUESTION 87
What is Device-level aggregation?
"Pass Any Exam. Any Time." - www.actualtests.com 38
Symantec ST0-085 Exam

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 88
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 89
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

QUESTION 90
Which three need to be collected as part of pre-deployment planning?

A. desktop application
"Pass Any Exam. Any Time." - www.actualtests.com 39
Symantec ST0-085 Exam
B. host operating systems
C. number of events per second
D. event-to-incident ratio under normal and peak conditions
E. number of geographical locations

Answer: BCD

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