ISLEVER

250-501

intrusion protection solutions

DEMO

https://www.islever.com/250-501.html

https://www.islever.com/symantec.html

For the most up-to-date exam questions and materials, we recommend visiting our website, where you can access the latest content and resources.

QUESTION NO: 1

Which Symantec ManHunt feature can be used to view recorded sessions?

A. traffic playback
B. session replay
C. flow playback
D. session flow replay

Answer: A

QUESTION NO: 2

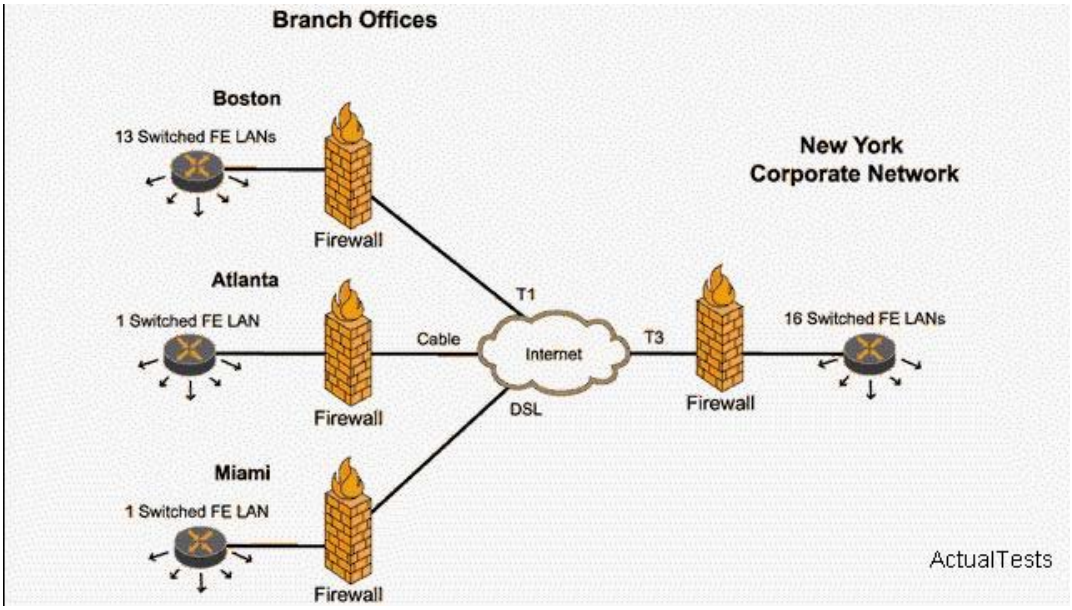
Which three types of analyzers do anomaly-based sensors use? (Choose three.)

A. statistical
B. packet
C. trend
D. file

Answer: A,B,C

QUESTION NO: 3

Click the Exhibit button. The IT group wants to be aware of any unknown network activity in each LAN throughout the company. They also want to analyze intrusion attempts targeting the New York servers. What is the minimum deployment of Symantec ManHunt nodes and Symantec Decoy Servers you should use to achieve the objective?



A. deploy one Symantec ManHunt server in each location; deploy one Symantec Decoy Server in New York
B. deploy two Symantec ManHunt nodes in Boston, three in New York, one in Atlanta, and one in Miami; deploy two Symantec Decoy Servers in New York
C. deploy two Symantec ManHunt nodes in Boston, two in New York, one in Atlanta, and one in Miami; deploy two Symantec Decoy Server in New York
D. deploy two Symantec ManHunt nodes in Boston and two in New York; deploy two Symantec Decoy Servers in New York

Answer: C

QUESTION NO: 4

Which two statements are true about a Symantec ManHunt console deployment? (Choose two.)

A. All nodes within a cluster can be viewed simultaneously.
B. A console supports up to 100 nodes.
C. A console must be deployed on the Symantec ManHunt node.
D. Communication between the console and nodes is authenticated.

Answer: A,D

QUESTION NO: 5

Which activity compromises the integrity of forensic data collected during an incident response investigation of HostA?

A. modification of the network intrusion detection system's signature files
B. modification of firewall settings to collect additional forensic data
C. modification of the intrusion policy at HostA's IPS sensor to block further intrusions
D. modification of the system files on HostA to block further intrusions

Answer: D

QUESTION NO: 6

Which two logs does the Symantec Host IDS Agent service monitor on a UNIX system? (Choose two.)

A. Kernel
B. C2

C. Process Accounting
D. Service

Answer: B,C

QUESTION NO: 7

Which two conditions affect the performance of network-based intrusion detection systems? (Choose two.)

A. presence of a host-based intrusion detection system
B. resource utilization on sensor nodes
C. local area network traffic congestion
D. concurrent support for intrusion detection across multiple platforms

Answer: B,C

QUESTION NO: 8

Which authentication service certifies that attack data are not altered on Symantec Decoy Server?

A. iButton
B. Entrust
C. RSA
D. Verisign

Answer: A

QUESTION NO: 9

Which two functions does the Symantec Enterprise Security Architecture Bridge provide Symantec ManHunt? (Choose two.)

A. collection of event data from third-party devices
B. collection of Symantec ManHunt intrusion event data
C. inclusion of Symantec ManHunt events in Symantec Enterprise Security Architecture reports
D. distribution of Symantec ManHunt response policy.

Answer: B,C