Vendor: Symantec

Exam Code: ST0-134

Exam Name: Symantec EndPoint Protection 12.1 Tcehnical Assessment

Version: Demo

QUESTION 1
Which Symantec Endpoint Protection 12.1 protection technology provides the primary protection layers against zero-day network attacks?

A. SONAR
B. Client Firewall
C. Intrusion Prevention
D. System Lockdown

Correct Answer: C

QUESTION 2
According to Symantec, what is a botnet?

A. systems infected with the same virus strain
B. groups of systems performing remote tasks without the users' knowledge
C. groups of computers configured to steal credit card records
D. compromised systems opening communication to an IRC channel

Correct Answer: B

QUESTION 3
A financial company has a security policy that prevents banking system workstations from connecting to the internet. Which Symantec Endpoint Protection 12.1 protection technology will be prevented from working on the company's workstations?

A. Insight
B. Application and Device Control
C. Network Threat Protection
D. LiveUpdate

Correct Answer: A

QUESTION 4
In addition to performance improvements, which two benefits does Insight provide? (Select two.)

A. reputation scoring for documents
B. zero-day threat detection
C. protection against system files modifications
D. false positive mitigation
E. blocking of malicious websites

Correct Answer: BD

QUESTION 5
How does the Intrusion Prevention System add an additional layer of protection to Network Threat Protection?

A. It inspects the TCP packet headers and tracks the sequence number.
B. It performs deep packet inspection, reading the packet headers, and data portion.
C. It examines TCP/IP traffic from the application and traces the source of the traffic.
D. It monitors IP datagrams for abnormalities.

Correct Answer: B

QUESTION 6
The fake antivirus family "PC scout" infects systems with a similar method regardless of its variant. Which SONAR sub-feature can block new variants of the same family, based on sequence of events?

A. artificial intelligence
B. behavioral heuristic
C. human authored signatures
D. behavioral policy lockdown

Correct Answer: C

QUESTION 7
Drive-by downloads are a common vector of infections. Some of these attacks use encryption to bypass traditional defense mechanisms. Which Symantec Endpoint Protection 12.1 protection technology blocks such obfuscated attacks?

A. SONAR
B. Bloodhound heuristic virus detection
C. Client Firewall
D. Browser Intrusion Prevention

Correct Answer: D

QUESTION 8
Which Symantec Endpoint Protection 12.1 defense mechanism provides protection against worms like W32.Silly.FDC, which propagate from system to system through the use of autorun.inf files?

A. Application Control
B. SONAR
C. Client Firewall
D. Exceptions

Correct Answer: A

QUESTION 9
A company is experiencing a malware outbreak. The company deploys Symantec Endpoint Protection 12.1, with only Virus and Spyware Protection, Application and Device Control, and Intrusion Prevention technologies. Why would Intrusion Prevention be unable to block all communications from an attacking host?

A. Intrusion Prevention needs the firewall component to block all traffic from the attacking host.
B. Intrusion Prevention blocks the attack only if the administrator wrote a signature for it.
C. Intrusion Prevention definitions are out-of-date.
D. Intrusion Prevention is set to log only.

Correct Answer: A

QUESTION 10
Which Symantec Endpoint Protection 12.1 component uses reputation to evaluate a file?

A. Shared Insight Cache server
B. Symantec Endpoint Protection client
C. Symantec Endpoint Protection Manager
D. LiveUpdate Administrator server

Correct Answer: B

QUESTION 11
Which Symantec Endpoint Protection 12.1 component provides services to improve the performance of virtual client scanning?

A. Shared Insight Cache server

B. LiveUpdate Administrator server
C. Symantec Protection Center
D. Group Update Provider

Correct Answer: A

QUESTION 12
How many Symantec Endpoint Protection Managers can be connected to an embedded database?

A. 1
B. 2
C. 5
D. 10

Correct Answer: A

QUESTION 13
Which component is required in order to run Symantec Endpoint Protection 12.1 protection technologies?

A. Symantec Endpoint Protection Manager
B. Symantec Endpoint Protection client
C. LiveUpdate Administrator server
D. Symantec Protection Center

Correct Answer: B

QUESTION 14
Which Symantec Endpoint Protection 12.1 component provides single-sign-on to the Symantec Endpoint Protection Manager and other products, along with cross-product reporting?

A. Symantec Reporting server
B. Symantec Security Information Manager
C. IT Analytics
D. Symantec Protection Center

Correct Answer: D

QUESTION 15

Which Symantec Endpoint Protection 12.1 component uses Sybase SQL Anywhere?

A. Symantec Endpoint Protection Manager embedded database
B. Symantec Endpoint Protection Manager remote database
C. LiveUpdate Administrator server
D. Shared Insight Cache server

Correct Answer: A

EnsurePass.com Members Features:

1. Verified Answers researched by industry experts.
2. Q&As are downloadable in PDF and VCE format.
3. 98% success Guarantee and **Money Back** Guarantee.
4. Free updates for **180** Days.
5. **Instant Access to download the Items**

View list of All Exam provided:
http://www.ensurepass.com/certfications?index=A

To purchase Lifetime Full Access Membership click here:
http://www.ensurepass.com/user/register

Valid Discount Code for 2015: JREH-G1A8-XHC6

To purchase the HOT Exams:

Cisco		CompTIA		Oracle	VMWare	IBM
100-101	640-554	220-801	LX0-101	1Z0-051	VCAD510	C2170-011
200-120	200-101	220-802	N10-005	1Z0-052	VCP510	C2180-319
300-206	640-911	BR0-002	SG0-001	1Z0-053	VCP550	C4030-670
300-207	640-916	CAS-001	SG1-001	1Z0-060	VCAC510	C4040-221
300-208	640-864	CLO-001	SK0-003	1Z0-474	VCP5-DCV	RedHat
350-018	642-467	ISS-001	SY0-301	1Z0-482	VCP510PSE	EX200
352-001	642-813	JK0-010	SY0-401	1Z0-485		EX300
400-101	642-832	JK0-801	PK0-003	1Z0-580		
640-461	642-902			1Z0-820		