Symantec

250-315 Exam

Administration of Symantec Endpoint Protection 12.1

Thank you for Downloading 250-315 exam PDF Demo

You can Buy Latest 250-315 Full Version Download

https://www.certkillers.net/Exam/250-315

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

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

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

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 file modifications
D. false positive mitigation
E. blocking of malicious websites

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.

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

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

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

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.

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

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

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

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

Answer: B

Question: 13

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

Answer: D

Question: 14

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

Answer: A

Question: 15

Which Symantec Endpoint Protection 12.1 component improves performance because known good

files are skipped?

A. LiveUpdate Administrator server
B. Group Update Provider
C. Shared Insight Cache server
D. Central Quarantine server

Answer: C

Thank You for trying 250-315 PDF Demo

To Buy Latest 250-315 Full Version Download visit link below

https://www.certkillers.net/Exam/250-315

Start Your 250-315 Preparation

[Limited Time Offer] Use Coupon "CKNET" for Further discount on your purchase. Test your 250-315 preparation with actual exam questions.