Vendor: Symantec

Exam Code:ST0-134

Exam Name: Symantec EndPoint Protection 12.1 Technical Assessment

Version: Demo

QUESTION 1

An employee is taking leave for four months and the employee\\'s workstation will be powered off and locked in an office. Why does the workstation disappear from the Symantec Endpoint Protection Manager (SEPM) Reports and Client view after 30 days?

A. Administrators used the "reclaim license" option.

B. The SEPM purges offline clients after a set amount of time.

C. The SEPM quarantines offline clients after a set amount of time.

D. The SEPM purges clients with expired licenses.

Correct Answer: B

QUESTION 2

An administrator needs to ensure that a specific network threat can be detected. The attack signatures for this threat may be found across multiple packets. What can the administrator do to ensure the best chance of detecting this threat?

A. Ensure that Symantec IPS signatures are updated.

B. Create custom IPS signatures

C. Enable TCP resequencing

D. Create a Firewall rule for this threat

Correct Answer: A

QUESTION 3

A company is running the Symantec Endpoint Protection 12.1 firewall with the default policy. At the bottom of the ruleset, there is a rule called "Block all other IP traffic and log" which will block all IP traffic. A financial application is being blocked by this rule. What should be changed to allow the application without sacrificing security?

A. The existing rule should be changed.

B. A new rule should be created.

C. An existing rule should be deleted.

D. An existing rule needs to be reordered.

Correct Answer: B

QUESTION 4

Which feature can be configured to increase or decrease performance of scheduled scans?

A. scan frequency

B. CPU throttling

C. heartbeat interval

D. tuning options

Correct Answer: A

QUESTION 5

A customer is downloading newly-created company files from an internal website and is being blocked by Download Insight based on reputation. How can the customer prevent this?

A. Change the minimum number of days in the Download Insight settings.

B. Change the minimum number of users in the Download Insight settings.

C. Increase the sensitivity slider in the Download Insight settings.

D. Enable the option to trust files downloaded from an intranet website in the Download Insight settings.

Correct Answer: D

QUESTION 6

A company has 10,000 Symantec Endpoint Protection (SEP) clients deployed using two Symantec Endpoint Protection Managers (SEPMs). Which configuration is recommended to ensure that each SEPM is able to effectively handle the communications load with the SEP clients?

A. Push mode

B. Client control mode

C. Server control mode

D. Pull mode

Correct Answer: D

QUESTION 7

In addition to preventing Symantec Endpoint Protection 12.1 (SEP) from being stopped maliciously, which other two functions does Tamper Protection perform? (Select two.)

A. It prevents a user from stopping the SEP services.

B. It prevents the SEP Registry keys from being deleted.

C. It prevents SEP from stopping third party applications.

D. It prevents the SEP files and folders from being changed.

E. It prevents the user from opening the SEP client interface.

Correct Answer: BD

QUESTION 8

An administrator plans to implement a multi-site Symantec Endpoint Protection (SEP) deployment. The administrator needs to determine whether replication is viable without needing to make network firewallchanges or change defaults in SEP.Which port should the administrator verify is open on the path of communication between the two proposed sites?

A. 1433

B. 2967

C. 8014

D. 8433

Correct Answer: D

QUESTION 9

Which action must a Symantec Endpoint Protection administrator take before creating custom Intrusion Prevention signatures?

A. change the custom signature order

B. create a Custom Intrusion Prevention Signature library

C. define signature variables

D. enable signature logging

Correct Answer: B

QUESTION 10

An administrator is logged in to the Symantec Endpoint Protection Manager (SEPM) console for a system named SEPM01. The groups and policies that were previously in the SEPM01 console are unavailable and have been replaced with unfamiliar groups and policies. What was a possible reason for this change?

A. The administrator was modified from using Computer mode to User mode.

B. The administrator was logged in to the incorrect domain for SEPM01.

C. The administrator was changed from a limited administrator to a system administrator.

D. The administrator was using the Web console instead of the Java console.

Correct Answer: B

QUESTION 11

An administrator needs to exclude some servers from an Intrusion Prevention System (IPS) policy. When specifying an excluded host in an IPS policy, which two methods can be used? (Select two.)

A. DNS host

B. IP address

C. MAC address

D. DNS domain

E. subnet

Correct Answer: BE

QUESTION 12

Which operation can be performed using the Database Back Up and Restore utility found in the Windows Start menu?

A. on-demand backup of the database

B. scheduled monthly backup of the database

C. selection of the Symantec Endpoint Protection Manager to backup

D. selection of the backup location

Correct Answer: A