250-315$^{Q\&As}$

Administration of Symantec Endpoint Protection 12.1

Pass Symantec 250-315 Exam with 100% Guarantee

Following Questions and Answers are all new published by Symantec Official Exam Center

QUESTION 1

What is a characteristic of a Symantec Endpoint Protection (SEP) domain?

A. Each domain has its own management server and database.

B. Every administrator from one domain can view data in other domains.

C. Data for each domain is stored in its own separate SEP database.

D. Domains share the same management server and database.

Correct Answer: D

QUESTION 2

Which two instances could cause Symantec Endpoint Protection to be unable to remediate a file? (Select two.)

A. Another scan is in progress.

B. The detected file is in use.

C. There are insufficient file permissions.

D. The file is marked for deletion by Windows on reboot.

E. The file has good reputation.

Correct Answer: BC

QUESTION 3

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 4

What does SONAR use to reduce false positives?

A. Virus and Spyware definitions

B. File Fingerprint list

C. Symantec Insight

D. Extended File Attributes (EFA) table

Correct Answer: C

QUESTION 5

Administrators at a company share a single terminal for configuring Symantec Endpoint Protection. The administrators want to ensure that each administrator using the console is forced to authenticate using their individual credentials. They are concerned that administrators may forget to log off the terminal, which would easily allow others to gain access to the Symantec Endpoint Protection Manager (SEPM) console.

Which setting should the administrator disable to minimize the risk of non-authorized users logging into the SEPM console?

A. allow users to save credentials when logging on

B. delete clients that have not connected for specified time

C. lock account after the specified number of unsuccessful logon attempts

D. allow administrators to reset the passwords

Correct Answer: A