Vendor: Symantec

Exam Code:250-561

Exam Name: Endpoint Security Complete - Administration R1

Version: Demo

QUESTION 1

An administrator is evaluating an organization\\'s computers for an upcoming SES deployment. Which computer meets the pre-requisites for the SES client?

A. A computer running Mac OS X 10.8 with 500 MB of disk space, 4 GB of RAM, and an Intel Core 2 Duo 64-bit processor

B. A computer running Mac OS X 10.14 with 400 MB of disk space, 4 GB of RAM, and an Intel Core 2 Duo 64-bit processor

C. A computer running Windows 10 with 400 MB of disk space, 2 GB of RAM, and a 2.4 GHz Intel Pentium 4 processor

D. A computer running Windows 8 with 380 MB of disk space, 2 GB of RAM, and a 2.8 GHz Intel Pentium 4 processor

Correct Answer: C

QUESTION 2

What are two (2) benefits of a fully cloud managed endpoint protection solution? (Select two)

A. Increased content update frequency

B. Increased visibility

C. Reduced 3rd party licensing cost

D. Reduced database usage

E. Reduced network usage

Correct Answer: CD

QUESTION 3

Which rule types should be at the bottom of the list when an administrator adds device control rules?

A. General "catch all" rules

B. General "brand defined" rules

C. Specific "device type" rules

D. Specific "device model" rules

Correct Answer: D

QUESTION 4

Which SES feature helps administrator apply policies based on specific endpoint profiles?

A. Device Groups

B. Device Profiles

C. Policy Bundles

D. Policy Groups

Correct Answer: D

QUESTION 5

What should an administrator know regarding the differences between a Domain and a Tenant in ICDm?

A. A tenant can contain multiple domains

B. A domain can contain multiple tenants

C. Each customer can have one domain and many tenant

D. Each customer can have one tenant and many domains

Correct Answer: A

QUESTION 6

An administrator learns of a potentially malicious file and wants to proactively prevent the file from ever being executed.

What should the administrator do?

A. Add the file SHA1 to a blacklist policy

B. Increase the Antimalware policy Intensity to Level 5

C. Add the filename and SHA-256 hash to a Blacklist policy

D. Adjust the Antimalware policy age and prevalence settings

Correct Answer: D

QUESTION 7

Which two (2) options is an administrator able to use to prevent a file from being fasely detected? (Select two)

A. Assign the file a SHA-256 cryptographic hash

B. Add the file to a Whitelist policy

C. Reduce the Intensive Protection setting of the Antimalware policy

D. Register the file with Symantec\\'s False Positive database

E. Rename the file

Correct Answer: BD

QUESTION 8

A user downloads and opens a PDF file with Adobe Acrobat. Unknown to the user, a hidden script in the file begins downloading a RAT.

Which Anti-malware engine recognizes that this behavior is inconsistent with normal Acrobat functionality, blocks the behavior and kills Acrobat?

A. SONAR

B. Sapient

C. IPS

D. Emulator

Correct Answer: B

QUESTION 9

Which two (2) skill areas are critical to the success of incident Response Teams (Select two)

A. Project Management

B. Incident Management

C. Cyber Intelligence

D. Incident Response

E. Threat Analysis

Correct Answer: CD

QUESTION 10

How long does a blacklist task remain in the My Tasks view after its automatic creation?

A. 180 Days

B. 30 Days

C. 60 Days

D. 90 Days

Correct Answer: B

QUESTION 11

Which Symantec component is required to enable two factor authentication with VIP on the Integrated Cyber Defense manager (ICDm)?

A. A physical token or a software token

B. A software token and a VIP server

C. A software token and an active directory account

D. A physical token or a secure USB key

Correct Answer: B

QUESTION 12

What is the primary issue pertaining to managing roaming users while utilizing an on- premise solution?

A. The endpoint is missing timely policy update

B. The endpoint is absent of the management console

C. The endpoint fails to receive content update

D. The endpoint is more exposed to threats

Correct Answer: C