250-561 Q&As

Endpoint Security Complete - Administration R1

Pass Symantec 250-561 Exam with 100% Guarantee

QUESTION 1

Which two (2) scan range options are available to an administrator for locating unmanaged endpoints? (Select two)

A. IP range within network

B. IP range within subnet

C. Entire Network

D. Entire Subnet

E. Subnet Range

Correct Answer: AE

QUESTION 2

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 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 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 5

Which security control is complementary to IPS, providing a second layer of protection against network attacks?

A. Host Integrity

B. Antimalware

C. Firewall

D. Network Protection

Correct Answer: D

QUESTION 6

Which statement best defines Machine Learning?

A. A program that needs user input to perform a task.

B. A program that teams from observing other programs.

C. A program that learns from experience to optimize the output of a task.

D. A program that require data to perform a task.

Correct Answer: B

QUESTION 7

Which SEPM-generated element is required for an administrator to complete the enrollment of SEPM to the cloud console?

A. Token

B. SEPM password

C. Certificate key pair

D. SQL password

Correct Answer: A

QUESTION 8

What does an end-user receive when an administrator utilizes the Invite User feature to distribute the SES client?

A. An email with a link to directly download the SES client

B. An email with a link to a KB article explaining how to install the SES Agent

C. An email with the SES_setup.zip file attached

D. An email with link to register on the ICDm user portal

Correct Answer: D

QUESTION 9

Which security threat uses malicious code to destroy evidence, break systems, or encrypt data?

A. Execution

B. Persistence

C. Impact

D. Discovery

Correct Answer: A

QUESTION 10

Which SES security control protects against threats that may occur in the Impact phase?

A. Device Control

B. IPS

C. Antimalware

D. Firewall

Correct Answer: D

QUESTION 11

What happens when an administrator blacklists a file?

A. The file is assigned to the Blacklist task list

B. The file is automatically quarantined

C. The file is assigned to a chosen Blacklist policy

D. The file is assigned to the default Blacklist policy

Correct Answer: A

QUESTION 12

What version number is assigned to a duplicated policy?

A. One

B. Zero

C. The original policy\\'s number plus one

D. The original policy\\'s version numb

Correct Answer: C

QUESTION 13

Which two (2) steps should an administrator take to guard against re-occurring threats? (Select two)

A. Confirm that daily active and weekly full scans take place on all endpoints

B. Verify that all endpoints receive scheduled Live-Update content

C. Use Power Eraser to clean endpoint Windows registries

D. Add endpoints to a high security group and assign a restrictive Antimalware policy to the group

E. Quarantine affected endpoints

Correct Answer: CE

QUESTION 14

What are the Exploit Mitigation security control\\'s mitigation techniques designed to prevent?

A. Packed file execution

B. Misbehaving applications

C. File-less attacks

D. Rootkit downloads

Correct Answer: D

QUESTION 15

Which type of security threat is used by attackers to exploit vulnerable applications?

A. Lateral Movement

B. Privilege Escalation

C. Command and Control

D. Credential Access

Correct Answer: B