250-561 Q&As

Endpoint Security Complete - Administration R1

Pass Symantec 250-561 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.passapply.com/250-561.html

100% Passing Guarantee
100% Money Back Assurance

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

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

In which phase of MITRE framework would attackers exploit faults in software to directly tamper with system memory?

A. Exfiltration

B. Discovery

C. Execution

D. Defense Evasion

Correct Answer: D

QUESTION 2

An administrator needs to create a new Report Template that will be used to track firewall activity. Which two (2) report template settings are optional? (Select 2)

A. Output format

B. Generation schedule

C. Email recipients

D. Time frame

E. Size restrictions

Correct Answer: AC

QUESTION 3

Files are blocked by hash in the blacklist policy.

Which algorithm is supported, in addition to MD5?

A. SHA256

B. SHA256 "salted"

C. MD5 "Salted"

D. SHA2

Correct Answer: A

QUESTION 4

What characterizes an emerging threat in comparison to traditional threat?

A. Emerging threats use new techniques and 0-day vulnerability to propagate.

B. Emerging threats requires artificial intelligence to be detected.

C. Emerging threats are undetectable by signature based engines.

D. Emerging threats are more sophisticated than traditional threats.

Correct Answer: A

QUESTION 5

What is the frequency of feature updates with SES and the Integrated Cyber Defense Manager (ICDm)

A. Monthly

B. Weekly

C. Quarterly

D. Bi-monthly

Correct Answer: B

QUESTION 6

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 7

Which term or expression is utilized when adversaries leverage existing tools in the environment?

A. opportunistic attack

B. script kiddies

C. living off the land

D. file-less attack

Correct Answer: B

QUESTION 8

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 9

Which file property does SES utilize to search the VirusTotal website for suspicious file information?

A. File reputation

B. File size

C. File name

D. File hash

Correct Answer: C

QUESTION 10

Which designation should an administrator assign to the computer configured to find unmanaged devices?

A. Discovery Broker

B. Discovery Agent

C. Discovery Manager

D. Discovery Device

Correct Answer: B

QUESTION 11

Which Antimalware technology is used after all local resources have been exhausted?

A. Sapient

B. ITCS

C. Emulator

D. Reputation

Correct Answer: B

QUESTION 12

Which Firewall Stealth setting prevents OS fingerprinting by sending erroneous OS information back to the attacker?

A. Disable OS fingerprint profiling

B. Disable OS fingerprint detection

C. Enable OS fingerprint masqueradi

D. Enable OS fingerprint protection

Correct Answer: C

QUESTION 13

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 14

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 15

After editing and saving a policy, an administrator is prompted with the option to apply the edited policy to any assigned device groups.

What happens to the new version of the policy if the administrator declines the option to apply it?

A. The policy display is returned to edit mode

B. The new version of the policy is deleted

C. An unassigned version of the policy is created

D. The new version of the policy is added to the "in progress" list

Correct Answer: A