



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.pass4itsure.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

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 2

Which Anti-malware technology should an administrator utilize to expose the malicious nature of a file created with a custom packet?

- A. Sandbox
- B. SONAR
- C. Reputation
- D. Emulator

Correct Answer: A

QUESTION 3

Which SES advanced feature detects malware by consulting a training model composed of known good and known bad files?

- A. Signatures
- B. Advanced Machine Learning
- C. Reputation D. Artificial Intelligence

Correct Answer: B

QUESTION 4

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 5

Which URL is responsible for notifying the SES agent that a policy change occurred in the cloud console?

- A. spoc.norton.com
- B. stnd-ipsg.crsi-symantec.com
- C. ent-shasta.rrs-symantec.com
- D. ocsp.digicert.com

Correct Answer: D

QUESTION 6

Which technique randomizes the e memory address map with Memory Exploit Mitigation?

- A. SEHOP
- B. ROPHEAP
- C. ASLR
- D. ForceDEP

Correct Answer: C

QUESTION 7

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 8

An administrator must create a custom role in ICDm.

Which area of the management console is able to have access restricted or granted?

- A. Policy Management
- B. Hybrid device management
- C. Agent deployment
- D. Custom Dashboard Creation

Correct Answer: C

QUESTION 9

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 10

In the ICDm, administrators are assisted by the My Task view. Which automation type creates the tasks within the console?

- A. Artificial Intelligence
- B. Machine Learning
- C. Advanced Machine Learning
- D. Administrator defined rules

Correct Answer: A

QUESTION 11

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 12

What option must an administrator choose when rolling back a policy assignment to a previous version?

- A. Customize
- B. Reverse
- C. Override
- D. Go Back

Correct Answer: C

QUESTION 13

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 14

The ICDm has generated a blacklist task due to malicious traffic detection. Which SES component was utilized to make that detection?

- A. Antimalware
- B. Reputation
- C. Firewall
- D. IPS



Correct Answer: A

QUESTION 15

Why would an administrator choose the Server-optimized installation option when creating an installation package?

- A. To limit the Intrusion Prevention policy to use server-only signatures.
- B. To add the Server-optimized Firewall policy
- C. To add the SES client's Optimize Memory setting to the default server installation.
- D. To reduce the SES client's using resources that are required for other server-specific processes.

Correct Answer: A

[Latest 250-561 Dumps](#)

[250-561 VCE Dumps](#)

[250-561 Practice Test](#)