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.pass2lead.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

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 2

Which dashboard should an administrator access to view the current health of the environment?

A. The Antimalware Dashboard

B. The SES Dashboard

C. The Device Integrity Dashboard

D. The Security Control Dashboard

Correct Answer: D

QUESTION 3

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

QUESTION 4

Which file should an administrator create, resulting Group Policy Object (GPO)?

A. Symantec__Agent_package_x64.zip

B. Symantec__Agent_package_x64.msi

C. Symantec__Agent_package__32-bit.msi

D. Symantec__Agent_package_x64.exe

Correct Answer: C

QUESTION 5

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 6

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

QUESTION 7

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 8

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 9

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 10

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 11

Which Security Control dashboard widget should an administrator utilize to access detailed areas for a given security control ?

A. Learn More

B. Quick Links

C. More Info

D. Latest Tasks

Correct Answer: D

QUESTION 12

Which framework, open and available to any administrator, is utilized to categorize adversarial tactics and for each phase of a cyber attack?

A. MITRE RESPONSE

B. MITRE ATTandCK

C. MITRE ADVandNCE

D. MITRE ATTACK MATRIX

Correct Answer: C

QUESTION 13

Which alert rule category includes events that are generated about the cloud console?

A. Security

B. Diagnostic

C. System

D. Application Activity

Correct Answer: A

QUESTION 14

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 15

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

A. Sapient

B. ITCS

C. Emulator

D. Reputation

Correct Answer: B