250-561$^{\text{Q\&As}}$

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.leads4pass.com/250-561.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

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 2

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

A. SEHOP

B. ROPHEAP

C. ASLR

D. ForceDEP

Correct Answer: C

QUESTION 3

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 4

Which two (2) Discovery and Deploy features could an administrator use to enroll MAC endpoints? (Select two)

A. Push Enroll

B. A custom Installation package creator pact

C. A default Direct Installation package

D. Invite User

E. A custom Direct installation package

Correct Answer: BE

QUESTION 5

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

A. Sapient

B. ITCS

C. Emulator

D. Reputation

Correct Answer: B

QUESTION 6

Which antimalware intensity level is defined by the following: "Blocks files that are most certainly bad or potentially bad files. Results in a comparable number of false positives and false negatives."

A. Level 5

B. Level 2

C. Level 1

D. Level 6

Correct Answer: D

QUESTION 7

Which report template includes a summary of risk distribution by devices, users, and groups?

A. Device Integrity

B. Threat Distribution

C. Comprehensive

D. Weekly

Correct Answer: B

QUESTION 8

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 9

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 10

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 11

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 12

Which statement best describes Artificial Intelligence?

A. A program that automates tasks with a static set of instructions

B. A program that can predict when a task should be performed

C. A program that is autonomous and needs training to perform a task

D. A program that learns from experience and perform autonomous tasks

Correct Answer: A

QUESTION 13

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 14

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 15

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

250-561 Practice Test 250-561 Study Guide 250-561 Braindumps