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.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

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 endpoint is offline, and the administrator issues a scan command. What happens to the endpoint when it restarts, if it lacks connectivity?

A. The system is scanning when started.

B. The system downloads the content without scanning.

C. The system starts without scanning.

D. The system scans after the content update is downloaded.

Correct Answer: B

QUESTION 3

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 4

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 5

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 6

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 7

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 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

What must an administrator check prior to enrolling an on-prem SEPM infrastructure into the cloud?

A. Clients are running SEP 14.2 or later

B. Clients are running SEP 14.1.0 or later

C. Clients are running SEP 12-6 or later

D. Clients are running SEP 14.0.1 or late

Correct Answer: D

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 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 12

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 13

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 14

Which default role has the most limited permission in the Integrated Cyber Defense Manager?

A. Restricted Administrator

B. Limited Administrator

C. Server Administrator

D. Endpoint Console Domain Administrator

Correct Answer: C

QUESTION 15

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