Symantec

Exam 250-561

Endpoint Security Complete - Administration R1

Version: 3.0

[Total Questions: 70]

Question No : 1

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

Answer: B

Question No : 2

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

Answer: C

Question No : 3

Wh.ch Firewall rule components should an administrator configure to block facebook.com use during business hours?

A. Action, Hosts(s), and Schedule
B. Action, Application, and Schedule
C. Host(s), Network Interface, and Network Service
D. Application, Host(s), and Network Service

Answer: A

Question No : 4

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

Answer: D

Question No : 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

Answer: D

Question No : 6

What is the primary issue pertaining to managing roaming users while utilizing an on-premise solution?

A. The endpoint is missing timely policy update
B. The endpoint is absent of the management console
C. The endpoint fails to receive content update
D. The endpoint is more exposed to threats

Answer: C

Question No : 7

Which SES security control protects against threats that may occur in the Impact phase?

A. Device Control
B. IPS
C. Antimalware
D. Firewall

Answer: D

Question No : 8

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

Answer: D

Question No : 9

Which SEPM-generated element is required for an administrator to complete the enrollment of SEPM to the cloud console?

A. Token
B. SEPM password
C. Certificate key pair
D. SQL password

Answer: A

Question No : 10

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

Answer: C

Question No : 11

Which Endpoint > Setting should an administrator utilize to locate unmanaged endpoints on a network subnet?

A. Discover Endpoints
B. Endpoint Enrollment
C. Discover and Deploy
D. Device Discovery

Answer: A

Question No : 12

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

Answer: A

Question No : 13

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

Answer: A

Question No : 14

An administrator selects the Discovered Items list in the ICDm to investigate a recent surge in suspicious file activity. What should an administrator do to display only high risk files?

A. Apply a list control
B. Apply a search rule
C. Apply a list filter
D. Apply a search modifier

Answer: B

Question No : 15

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.

Answer: A

Question No : 16

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

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

Answer: C

Question No : 17

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

Answer: A

Question No : 18

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

Answer: B

Question No : 19

A user downloads and opens a PDF file with Adobe Acrobat. Unknown to the user, a hidden script in the file begins downloading a RAT.

Which Anti-malware engine recognizes that this behavior is inconsistent with normal Acrobat functionality, blocks the

behavior and kills Acrobat?

A. SONAR
B. Sapient
C. IPS
D. Emulator

Answer: B

Question No : 20

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

A. Security
B. Diagnostic
C. System

D. Application Activity

Answer: A

Question No : 21

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

Answer: C

Question No : 22

An administrator is evaluating an organization's computers for an upcoming SES deployment. Which computer meets the pre-requisites for the SES client?

A. A computer running Mac OS X 10.8 with 500 MB of disk space, 4 GB of RAM, and an Intel Core 2 Duo 64-bit processor
B. A computer running Mac OS X 10.14 with 400 MB of disk space, 4 GB of RAM, and an Intel Core 2 Duo 64-bit processor
C. A computer running Windows 10 with 400 MB of disk space, 2 GB of RAM, and a 2.4 GHz Intel Pentium 4 processor
D. A computer running Windows 8 with 380 MB of disk space, 2 GB of RAM, and a 2.8 GHz Intel Pentium 4 processor

Answer: C

Question No : 23

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

Answer: C,E

Question No : 24

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

Answer: A

Question No : 25

What does SES's advanced search feature provide when an administrator searches for a specific term?

A. A search modifier dialog
B. A search wizard dialog
C. A suggested terms dialog
D. A search summary dialog

Answer: A

Question No : 26

Which device page should an administrator view to track the progress of an issued device command?

A. Command Status

B. Command History
C. Recent Activity
D. Activity Update

Answer: C

Question No : 27

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

Answer: D

Question No : 28

Which type of organization is likely to be targeted with emerging threats?

A. Small organization with externalized managed security
B. Large organizations with dedicated security teams
C. Large organization with high turnover
D. Small organization with little qualified staff

Answer: D

Question No : 29

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