Symantec.250-550.v2022-02-21.q24

Exam Code:	250-550
Exam Name:	Administration of Symantec Endpoint Security - R1
Certification Provider:	Symantec
Free Question Number:	24
Version:	v2022-02-21
# of views:	984
# of Questions views:	240
https://www.dumpsdb.com/dumps/Symantec/250-550/Symantec.250-550.v2022-02-21.q24	

NEW QUESTION: 1
Which report template out format should an administrator utilize to generate graphical reports?
A. XML
B. PFD
C. XML
D. HTML
Answer: D (LEAVE A REPLY)

NEW QUESTION: 2
What option must an administrator choose when rolling back a policy assignment to a previous version?
A. Reverse
B. Go Back
C. Customize
D. Override
Answer: (SHOW ANSWER)

NEW QUESTION: 3
The ICDm has generated a blacklist task due to malicious traffic detection. Which SES component was utilized to make that detection?
A. IPS
B. Firewall
C. Antimalware

D. Reputation
Answer: C (LEAVE A REPLY)

NEW QUESTION: 4
Which technique randomizes the e memory address map with Memory Exploit Mitigation?
A. SEHOP
B. ASLR
C. ForceDEP
D. ROPHEAP
Answer: B (LEAVE A REPLY)

NEW QUESTION: 5
An administrator must create a custom role in ICDm.
Which area of the management console is able to have access restricted or granted?
A. Custom Dashboard Creation
B. Agent deployment
C. Hybrid device management
D. Policy Management
Answer: (SHOW ANSWER)

NEW QUESTION: 6
What does an end-user receive when an administrator utilizes the Invite User feature to distribute the SES client?
A. An email with a link to directly download the SES client
B. An email with the SES_setup.zip file attached
C. An email with a link to a KB article explaining how to install the SES Agent
D. An email with link to register on the ICDm user portal
Answer: (SHOW ANSWER)

NEW QUESTION: 7
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 scans after the content update is downloaded.
B. The system downloads the content without scanning.
C. The system is scanning when started.
D. The system starts without scanning.
Answer: (SHOW ANSWER)

NEW QUESTION: 8
Which Security Control dashboard widget should an administrator utilize to access detailed areas for a given security control ?

A. Quick Links
B. Learn More
C. Latest Tasks
D. More Info
Answer: (SHOW ANSWER)

NEW QUESTION: 9
Which type of security threat is used by attackers to exploit vulnerable applications?
A. Privilege Escalation
B. Lateral Movement
C. Command and Control
D. Credential Access
Answer: A (LEAVE A REPLY)

NEW QUESTION: 10
Which two (2) steps should an administrator take to guard against re-occurring threats? (Select two)
A. Use Power Eraser to clean endpoint Windows registries
B. Quarantine affected endpoints
C. Verify that all endpoints receive scheduled Live-Update content
D. Add endpoints to a high security group and assign a restrictive Antimalware policy to the group
E. Confirm that daily active and weekly full scans take place on all endpoints
Answer: (SHOW ANSWER)

NEW QUESTION: 11
Which communication method is utilized within SES to achieve real-time management?
A. Standard polling
B. Heartbeat
C. Long polling
D. Push Notification
Answer: D (LEAVE A REPLY)

NEW QUESTION: 12
Which SES security control protects against threats that may occur in the Impact phase?
A. Antimalware
B. Device Control
C. Firewall
D. IPS
Answer: (SHOW ANSWER)

NEW QUESTION: 13
Which Antimalware technology is used after all local resources have been exhausted?
A. Sapient
B. Reputation
C. Emulator
D. ITCS
Answer: D (LEAVE A REPLY)

NEW QUESTION: 14
Which SES feature helps administrator apply policies based on specific endpoint profiles?
A. Device Groups
B. Policy Groups
C. Policy Bundles
D. Device Profiles
Answer: (SHOW ANSWER)

NEW QUESTION: 15
Which policy should an administrator edit to utilize the Symantec LiveUpdate server for pre-release content?
A. The System Policy
B. The LiveUpdate Policy
C. The System Schedule Policy
D. The Firewall Policy
Answer: (SHOW ANSWER)

NEW QUESTION: 16
Which term or expression is utilized when adversaries leverage existing tools in the environment?
A. script kiddies
B. file-less attack
C. living off the land
D. opportunistic attack
Answer: A (LEAVE A REPLY)

NEW QUESTION: 17
What characterizes an emerging threat in comparison to traditional threat?
A. Emerging threats are more sophisticated than traditional threats.
B. Emerging threats use new techniques and 0-day vulnerability to propagate.
C. Emerging threats are undetectable by signature based engines.
D. Emerging threats requires artificial intelligence to be detected.
Answer: (SHOW ANSWER)

NEW QUESTION: 18
Which security threat uses malicious code to destroy evidence, break systems, or encrypt data?
A. Execution
B. Impact
C. Discovery
D. Persistence
Answer: (SHOW ANSWER)

NEW QUESTION: 19
Which file property does SES utilize to search the VirusTotal website for suspicious file information?
A. File hash
B. File name
C. File size
D. File reputation
Answer: (SHOW ANSWER)

NEW QUESTION: 20
What is the frequency of feature updates with SES and the Integrated Cyber Defense Manager (ICDm)
A. Quarterly
B. Monthly
C. Bi-monthly
D. Weekly
Answer: D (LEAVE A REPLY)

NEW QUESTION: 21
Which URL is responsible for notifying the SES agent that a policy change occurred in the cloud console?

A. ocsp.digicert.com
B. spoc.norton.com
C. ent-shasta.rrs-symantec.com
D. stnd-ipsg.crsi-symantec.com
Answer: A (LEAVE A REPLY)

NEW QUESTION: 22
What happens when an administrator blacklists a file?
A. The file is assigned to the Blacklist task list
B. The file is automatically quarantined
C. The file is assigned to the default Blacklist policy
D. The file is assigned to a chosen Blacklist policy
Answer: (SHOW ANSWER)

NEW QUESTION: 23
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 ATT&CK
C. MITRE ADV&NCE
D. MITRE ATTACK MATRIX
Answer: C (LEAVE A REPLY)

NEW QUESTION: 24
Which IPS Signature type is Primarily used to identify specific unwanted traffic?
A. Probe
B. Audit
C. Attack
D. Malcode
Answer: C (LEAVE A REPLY)