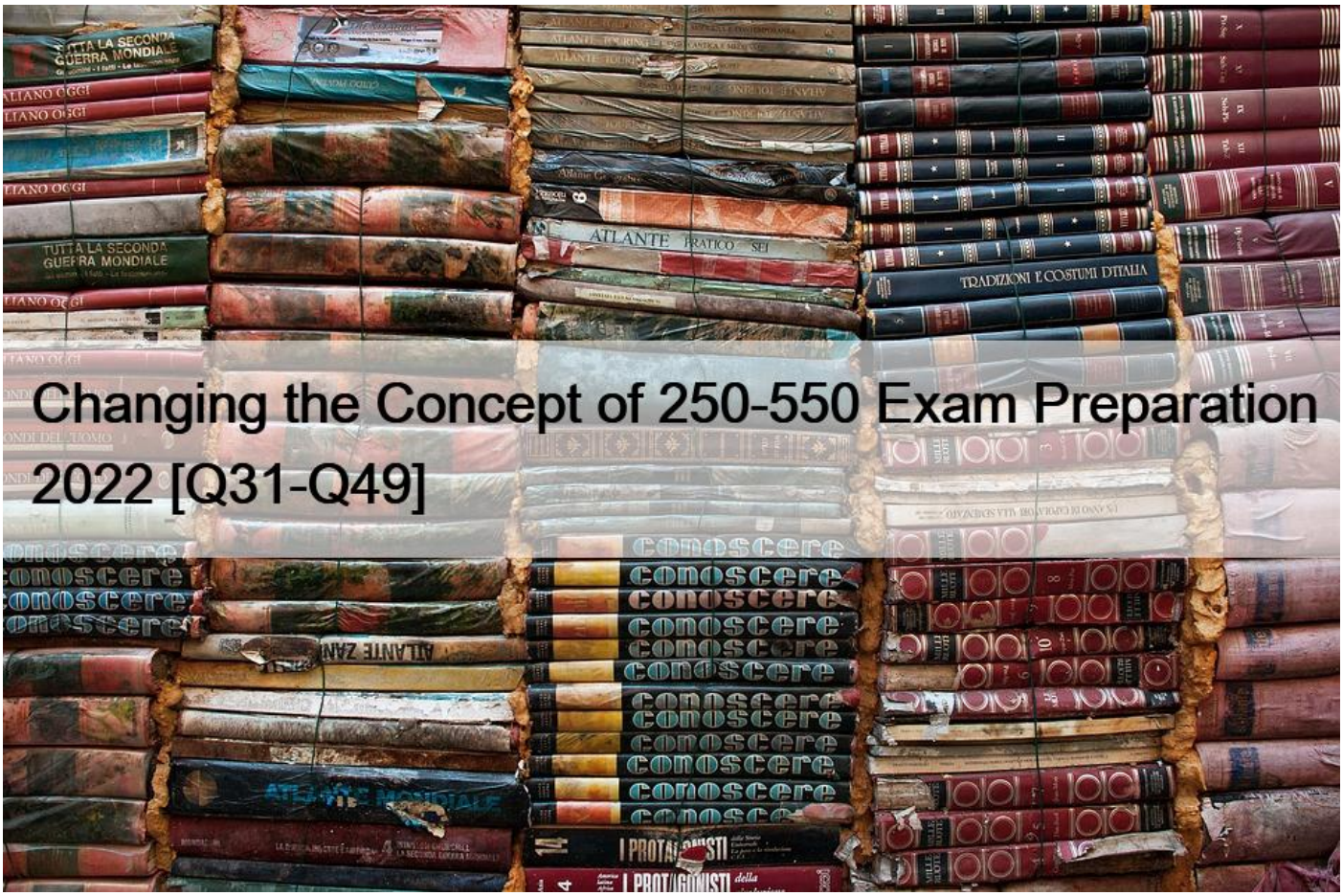
Changing the Concept of 250-550 Exam Preparation 2022 [Q31-Q49



Changing the Concept of 250-550 Exam Preparation 2022
Getting 250-550 Certification Made Easy! Get professional help from our 250-550 Dumps PDF

Symantec 250-550 Exam Syllabus Topics:

TopicDetailsTopic 1- Describe device control and how SES can be used to control device access- Describe the requirements and process for SEPM integration with the Cyber Defense Manager platform used in SESTopic 2- Describe how content updates can be modified for various network configurations- Describe the benefits of adopting a cloud-based endpoint security solutionTopic 3- Describe the SES system requirements and supported operating systems- Describe the account access and authentication methods available in SESTopic 4- Describe threat artifacts and the best practices to follow after a major endpoint security event- Describe LiveUpdate functionality and configuration optionsTopic 5- Describe the various methods SES uses to identify unmanaged endpoints- Describe various Memory Exploit Mitigation techniques and how SES protects against themTopic 6- Describe false positives, their impact, and how SES can be used to mitigate them- Describe how SES can be used to protect endpoints against zero-day attacksTopic 7- Describe the tools and techniques included in SES to adapt security policies based upon threat detections- Describe the steps that can be taken to remediate threats locally on an endpointTopic 8- Describe IPS and how it is used in detecting and preventing unwanted network traffic- Describe the client communication model and how to verify client connectivityTopic 9- Describe how to use the SES management console to configure administrative reports- Describe SES content update types and how they are distributed to endpoints

NEW QUESTION 31

An administrator learns of a potentially malicious file and wants to proactively prevent the file from ever being executed.

What should the administrator do?
* Add the file SHA1 to a blacklist policy
* Increase the Antimalware policy Intensity to Level 5
* Add the filename and SHA-256 hash to a Blacklist policy
* Adjust the Antimalware policy age and prevalence settings

NEW QUESTION 32

The ICDm has generated a blacklist task due to malicious traffic detection. Which SES component was utilized to make that detection?
* Antimalware
* Reputation
* Firewall
* IPS

NEW QUESTION 33

An administrator suspects that several computers have become part of a botnet. What should the administrator do to detect botnet activity on the network?
* Enable the Command and Control Server Firewall
* Add botnet related signatures to the IPS policy’s Audit Signatures list
* Enable the IPS policy’s Show notification on the device setting
* Set the Antimalware policy’s Monitoring Level to 4

NEW QUESTION 34

What happens when an administrator blacklists a file?
* The file is assigned to the Blacklist task list
* The file is automatically quarantined
* The file is assigned to a chosen Blacklist policy
* The file is assigned to the default Blacklist policy

NEW QUESTION 35

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?
* SONAR
* Sapient
* IPS
* Emulator

NEW QUESTION 36

Which type of security threat is used by attackers to exploit vulnerable applications?
* Lateral Movement
* Privilege Escalation
* Command and Control
* Credential Access

NEW QUESTION 37

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?
* The policy display is returned to edit mode
* The new version of the policy is deleted
* An unassigned version of the policy is created
* The new version of the policy is added to the “in progress” list

NEW QUESTION 38

Which rule types should be at the bottom of the list when an administrator adds device control rules?
* General “catch all” rules
* General “brand defined” rules
* Specific “device type” rules
* Specific “device model” rules

NEW QUESTION 39

Which SEPM-generated element is required for an administrator to complete the enrollment of SEPM to the cloud console?
* Token
* SEPM password
* Certificate key pair
* SQL password

NEW QUESTION 40

Which framework, open and available to any administrator, is utilized to categorize adversarial tactics and for each phase of a cyber attack?
* MITRE RESPONSE
* MITRE ATT&CK
* MITRE ADV&NCE
* MITRE ATTACK MATRIX

NEW QUESTION 41

Which Symantec component is required to enable two factor authentication with VIP on the Integrated Cyber Defense manager (ICDm)?
* A physical token or a software token
* A software token and a VIP server

* A software token and an active directory account
* A physical token or a secure USB key

NEW QUESTION 42

What is the frequency of feature updates with SES and the Integrated Cyber Defense Manager (ICDm)
* Monthly
* Weekly
* Quarterly
* Bi-monthly

NEW QUESTION 43

What does SES’s advanced search feature provide when an administrator searches for a specific term?
* A search modifier dialog
* A search wizard dialog
* A suggested terms dialog
* A search summary dialog

NEW QUESTION 44

Which SES advanced feature detects malware by consulting a training model composed of known good and known bad fries?
* Signatures
* Advanced Machine Learning
* Reputation
* Artificial Intelligence

NEW QUESTION 45

Which two (2) Discovery and Deploy features could an administrator use to enroll MAC endpoints? (Select two)
* Push Enroll
* A custom Installation package creator pact
* A default Direct Installation package
* Invite User
* A custom Direct installation package

NEW QUESTION 46

Which communication method is utilized within SES to achieve real-time management?
* Heartbeat
* Standard polling
* Push Notification
* Long polling

NEW QUESTION 47

What characterizes an emerging threat in comparison to traditional threat?
* Emerging threats use new techniques and 0-day vulnerability to propagate.
* Emerging threats requires artificial intelligence to be detected.
* Emerging threats are undetectable by signature based engines.

* Emerging threats are more sophisticated than traditional threats.

NEW QUESTION 48

Files are blocked by hash in the blacklist policy.

Which algorithm is supported, in addition to MD5?
* SHA256
* SHA256 “salted”
* MD5 “Salted”
* SHA2

NEW QUESTION 49

Which security control is complementary to IPS, providing a second layer of protection against network attacks?
* Host Integrity
* Antimalware
* Firewall
* Network Protection

250-550 Exam Crack Test Engine Dumps Training With 72 Questions:
https://www.examslabs.com/Symantec/Symantec-SCS-Certification/best-250-550-exam-dumps.html]