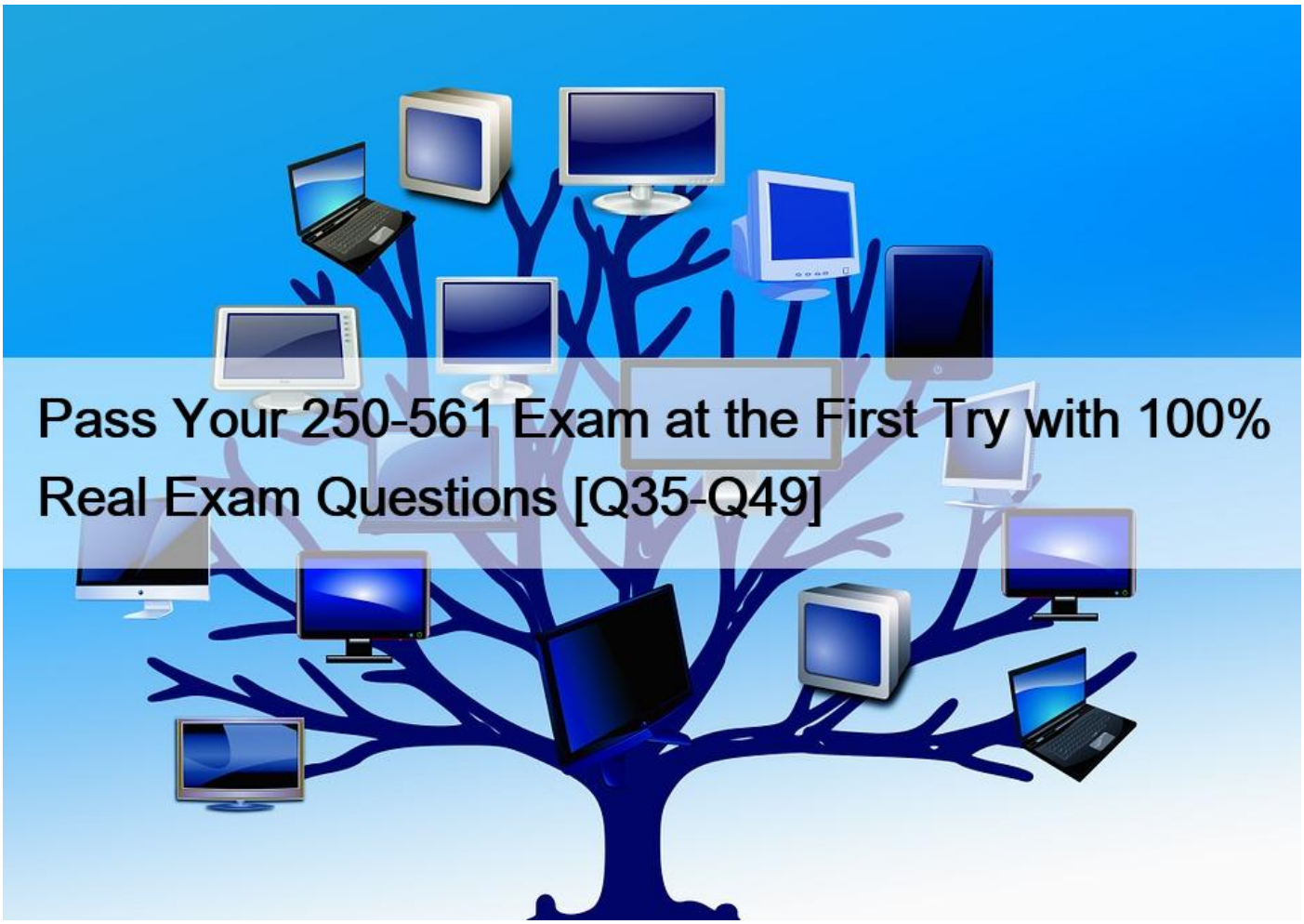
Pass Your 250-561 Exam at the First Try with 100% Real Exam Questions [Q35-Q49



Pass Your 250-561 Exam at the First Try with 100% Real Exam Questions
New Symantec 250-561 Dumps & Questions Updated on 2024

NEW QUESTION 35

Which security threat uses malicious code to destroy evidence, break systems, or encrypt data?
* Execution
* Persistence
* Impact
* Discovery

NEW QUESTION 36

Which report template type should an administrator utilize to create a daily summary of network threats detected?
* Network Risk Report

* Blocked Threats Report
* Intrusion Prevention Report
* Access Violation Report

NEW QUESTION 37

Which type of organization is likely to be targeted with emerging threats?
* Small organization with externalized managed security
* Large organizations with dedicated security teams
* Large organization with high turnover
* Small organization with little qualified staff

NEW QUESTION 38

Which option should an administrator utilize to temporarily or permanently block a file?
* Delete
* Hide
* Encrypt
* Blacklist

NEW QUESTION 39

Which IPS Signature type is Primarily used to identify specific unwanted traffic?
* Attack
* Probe
* Audit
* Malcode

NEW QUESTION 40

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 41

What are two (2) benefits of a fully cloud managed endpoint protection solution? (Select two)
* Increased content update frequency
* Increased visibility
* Reduced 3rd party licensing cost
* Reduced database usage
* Reduced network usage

NEW QUESTION 42

In which phase of MITRE framework would attackers exploit faults in software to directly tamper with system memory?
* Exfiltration

* Discovery
* Execution
* Defense Evasion

NEW QUESTION 43

Wh.ch Firewall rule components should an administrator configure to block facebook.com use during business hours?
* Action, Hosts(s), and Schedule
* Action, Application, and Schedule
* Host(s), Network Interface, and Network Service
* Application, Host(s), and Network Service

NEW QUESTION 44

Which SES security control protects against threats that may occur in the Impact phase?
* Device Control
* IPS
* Antimalware
* Firewall

NEW QUESTION 45

Which report template includes a summary of risk distribution by devices, users, and groups?
* Device Integrity
* Threat Distribution
* Comprehensive
* Weekly

NEW QUESTION 46

Which default role has the most limited permission in the Integrated Cyber Defense Manager?
* Restricted Administrator
* Limited Administrator
* Server Administrator
* Endpoint Console Domain Administrator

NEW QUESTION 47

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

NEW QUESTION 48

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 49

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