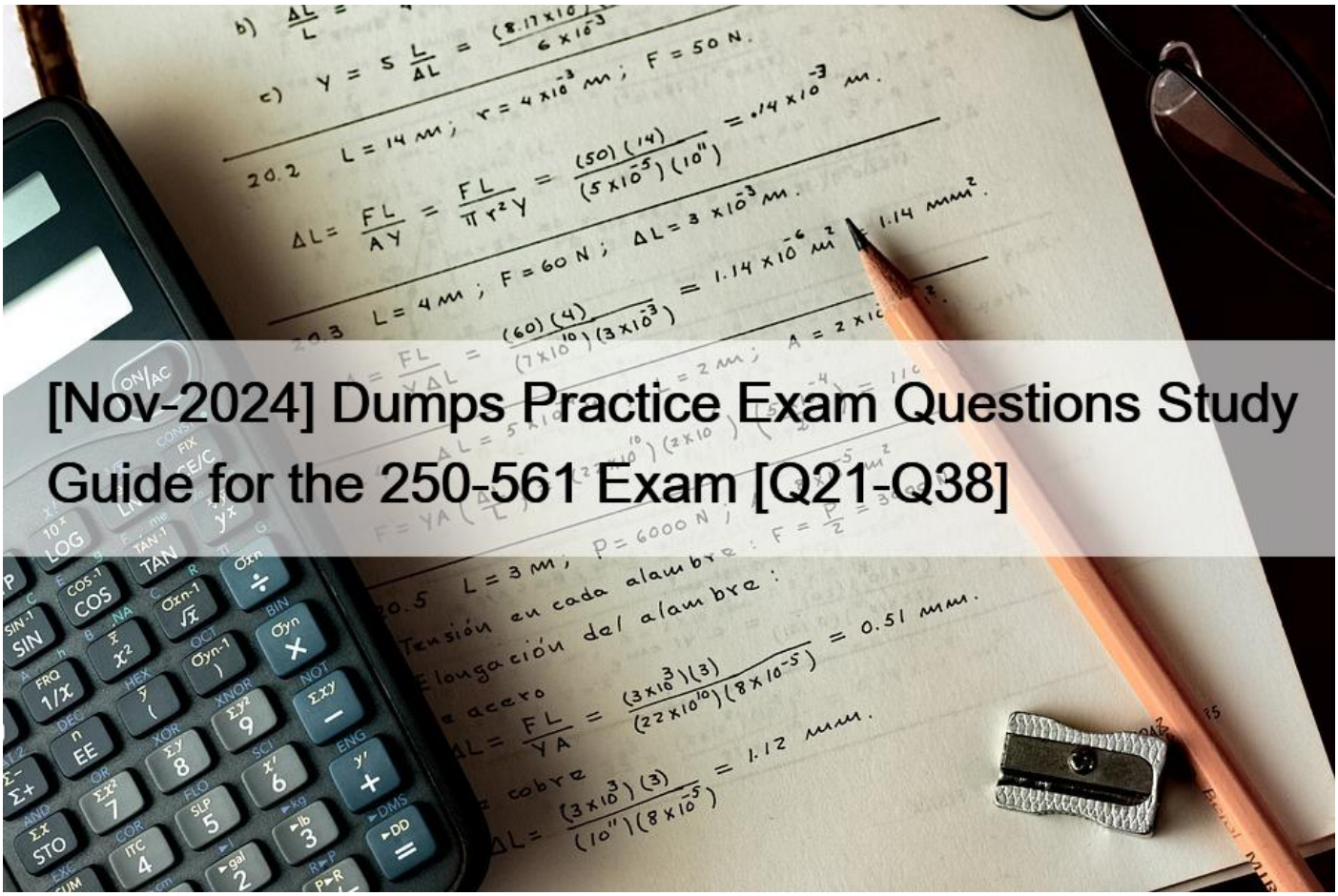
# [Nov-2024 Dumps Practice Exam Questions Study Guide for the 250-561 Exam [Q21-Q38




[Nov-2024] Dumps Practice Exam Questions Study Guide for the 250-561 Exam
250-561 Dumps with Practice Exam Questions Answers

**NO.21** Why would an administrator choose the Server-optimized installation option when creating an installation package?
* To limit the Intrusion Prevention policy to use server-only signatures.
* To add the Server-optimized Firewall policy
* To add the SES client’s Optimize Memory setting to the default server installation.
* To reduce the SES client’s using resources that are required for other server-specific processes.

**NO.22** Which designation should an administrator assign to the computer configured to find unmanaged devices?
* Discovery Broker
* Discovery Agent
* Discovery Manager
* Discovery Device

**NO.23** Which technique randomizes the e memory address map with Memory Exploit Mitigation?
* SEHOP

* ROPHEAP
* ASLR
* ForceDEP

**NO.24** Which two (2) options is an administrator able to use to prevent a file from being fasely detected (Select two)
* Assign the file a SHA-256 cryptographic hash
* Add the file to a Whitelist policy
* Reduce the Intensive Protection setting of the Antimalware policy
* Register the file with Symantec’s False Positive database
* Rename the file

**NO.25** 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

**NO.26** Which SES feature helps administrator apply policies based on specific endpoint profiles?
* Device Groups
* Device Profiles
* Policy Bundles
* Policy Groups

**NO.27** 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

**NO.28** 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

**NO.29** What version number is assigned to a duplicated policy?
* One
* Zero
* The original policy’s number plus one
* The original policy’s version numb

**NO.30** Which option should an administrator utilize to temporarily or permanently block a file?
* Delete
* Hide
* Encrypt
* Blacklist

**NO.31** 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

**NO.32** 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

**NO.33** Which statement best defines Machine Learning?
* A program that needs user input to perform a task.
* A program that teams from observing other programs.
* A program that learns from experience to optimize the output of a task.
* A program that require data to perform a task.

**NO.34** In which phase of MITRE framework would attackers exploit faults in software to directly tamper with system memory?
* Exfiltration
* Discovery
* Execution
* Defense Evasion

**NO.35** 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

**NO.36** An endpoint is offline, and the administrator issues a scan command. What happens to the endpoint when it restarts, if it lacks connectivity?
* The system is scanning when started.
* The system downloads the content without scanning.
* The system starts without scanning.
* The system scans after the content update is downloaded.

**NO.37** What are the Exploit Mitigation security control’s mitigation techniques designed to prevent?
* Packed file execution
* Misbehaving applications
* File-less attacks
* Rootkit downloads

**NO.38** What characterizes an emerging threat in comparison to traditional threat?
* Emerging threats are undetectable by signature based engines.
* Emerging threats are more sophisticated than traditional threats.
* Emerging threats requires artificial intelligence to be detected.

* Emerging threats use new techniques and 0-day vulnerability to propagate.

Symantec 250-561 exam is a comprehensive test that covers a wide range of topics related to endpoint security. Some of the areas that the exam covers include the installation and configuration of the SEP client, server, and manager, the management of policies, groups, and locations, and the troubleshooting of various issues that may arise during the deployment and administration of SEP. 250-561 exam also tests the candidates' knowledge of the various features and functionalities of SEP, such as the advanced threat protection, intrusion prevention, and firewall capabilities.

**Free Symantec SCS 250-561 Exam Question:**
https://www.examslabs.com/Symantec/Symantec-SCS/best-250-561-exam-dumps.html]