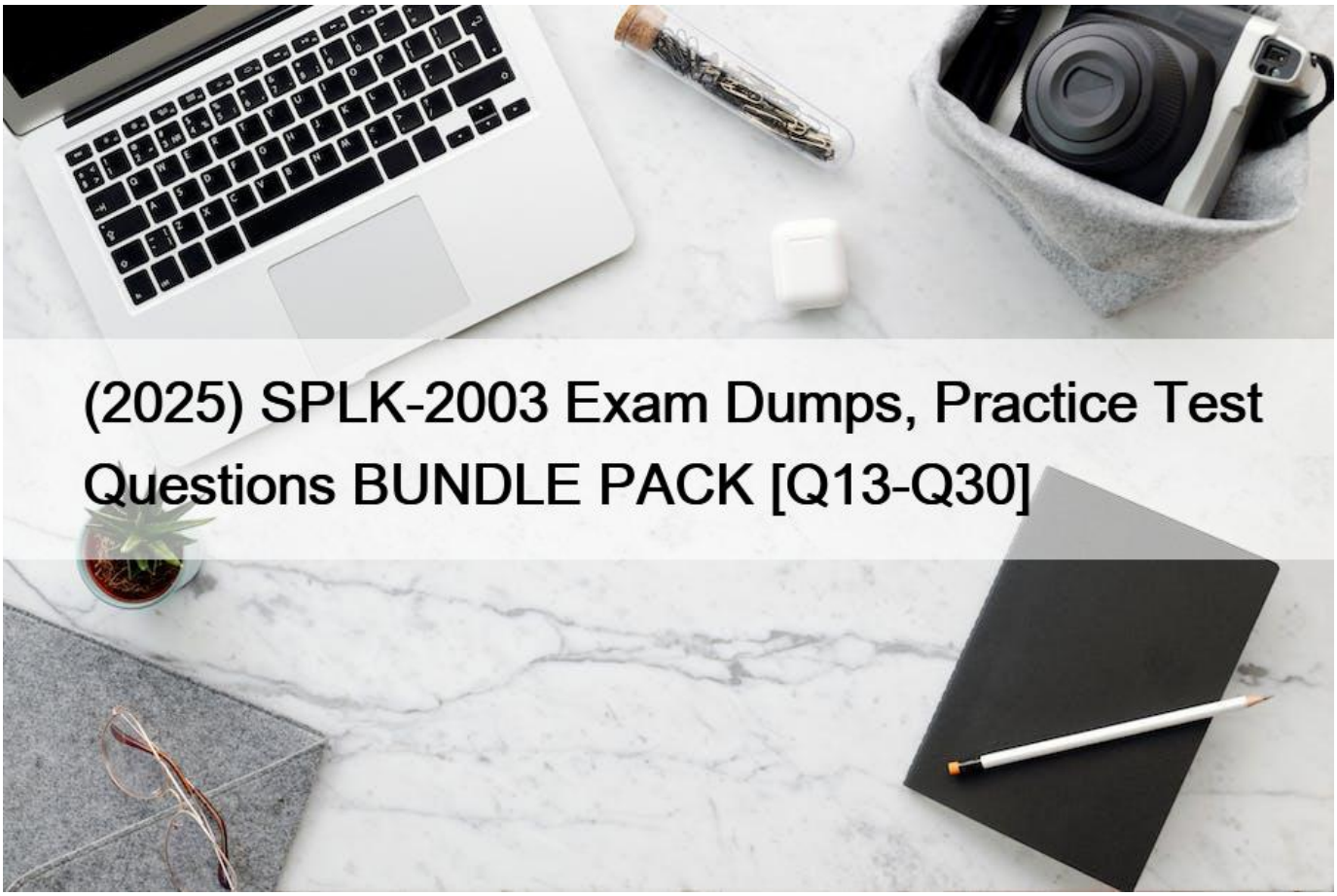
(2025) SPLK-2003 Exam Dumps, Practice Test Questions BUNDLE PACK [Q13-Q30



(2025) SPLK-2003 Exam Dumps, Practice Test Questions BUNDLE PACK Splunk SOAR Certified Automation Developer Certification SPLK-2003 Sample Questions Reliable

Splunk SPLK-2003 exam consists of 60 multiple-choice questions and must be completed within 90 minutes. Candidates must achieve a passing score of 70% or higher to earn the Splunk Phantom Certified Admin certification. SPLK-2003 exam covers a range of topics, including Phantom architecture, installation and configuration, workflow management, playbook creation and configuration, and integration with other security tools. Successful candidates will be able to demonstrate their ability to use Splunk Phantom to automate security operations workflows, streamline incident response, and improve overall security posture. The Splunk SPLK-2003 certification is an excellent way for security professionals to validate their skills and expertise in Splunk Phantom and advance their careers in the security automation and orchestration field.

Q13. Which of the following can be done with the System Health Display?
* Create a temporary, edited version of a process and test the results.
* Partially rewind processes, which is useful for debugging.
* View a single column of status for SOAR processes. For metrics, click Details.

* Reset DECIDED to reset playbook environments back to at-start conditions.

System Health Display is a dashboard that shows the status and performance of the SOAR processes and components, such as the automation service, the playbook daemon, the DECIDED process, and the REST API. One of the things that can be done with the System Health Display is to reset DECIDED, which is a core component of the SOAR automation engine that handles the execution of playbooks and actions. Resetting DECIDED can be useful for troubleshooting or debugging purposes, as it resets the playbook environments back to at-start conditions, meaning that any changes made by the playbooks are discarded and the playbooks are reloaded. To reset DECIDED, you need to click on the Reset DECIDED button on the System Health Display dashboard. Therefore, option D is the correct answer, as it is the only option that can be done with the System Health Display. Option A is incorrect, because creating a temporary, edited version of a process and testing the results is not something that can be done with the System Health Display, but rather with the Debugging dashboard, which allows you to modify and run a process in a sandbox environment. Option B is incorrect, because partially rewinding processes, which is useful for debugging, is not something that can be done with the System Health Display, but rather with the Rewind feature, which allows you to go back to a previous state of a process and resume the execution from there. Option C is incorrect, because viewing a single column of status for SOAR processes is not something that can be done with the System Health Display, but rather with the Status Display dashboard, which shows a simplified view of the SOAR processes and their status.

Q14. Which of the following roles is appropriate for a Splunk SOAR account that will only be used to execute automated tasks?

* Non-Human
* Automation
* Automation Engineer
* Service Account

In Splunk SOAR, the ‘Non-Human’ role is appropriate for accounts that are used exclusively to execute automated tasks. This role is designed for service accounts that interact with the SOAR platform programmatically rather than through a human user. It ensures that the account has the necessary permissions to perform automated actions while restricting access that would be unnecessary or inappropriate for a non-human entity.

Q15. What are the differences between cases and events?

* Case: potential threats.

Events: identified as a specific kind of problem and need a structured approach.

* Cases: only include high-level incident artifacts.

Events: only include low-level incident artifacts.

* Cases: contain a collection of containers.

Events: contain potential threats.

* Cases: incidents with a known violation and a plan for correction.

Events: occurrences in the system that may require a response.

Explanation

Cases and events are two types of containers in Phantom. Cases are incidents with a known violation and a plan for correction, such as a malware infection, a phishing attack, or a data breach. Events are occurrences in the system that may require a response, such as an alert, a log entry, or an email. Cases and events can contain both high-level and low-level incident artifacts, such as IP addresses, URLs, files, or users. Cases do not contain a collection of containers, but rather a collection of artifacts, tasks, notes, and comments. Events are not necessarily potential threats, but rather indicators of potential threats. Reference, page 9.

Q16. Why is it good playbook design to create smaller and more focused playbooks? (select all that apply)

* Reduces amount of playbook data stored in each repo.
* Encourages code reuse in a more compartmentalized form.

* To avoid duplication of code across multiple playbooks.
* Reduce large complex playbooks which become difficult to maintain.

Q17. Which of the following is the complete list of the types of backups that are supported by Phantom?
* Full backups.
* Full, delta, and incremental backups.
* Full and incremental backups.
* Full and delta backups.

Splunk Phantom supports different types of backups to safeguard data. Full backups create a complete copy of the current state of the system, while incremental backups only save the changes made since the last backup.

This approach allows for efficient use of storage space and faster backups after the initial full backup. Delta backups, which would save changes since the last full or incremental backup, are not a standard part of Phantom’s backup capabilities according to available documentation. Therefore, the complete list of backups supported by Phantom would be Full and Incremental backups.

Q18. What users are included in a new installation of SOAR?
* The admin and automation users are included by default.
* The admin, power, and user users are included by default.
* Only the admin user is included by default.
* No users are included by default.

The admin and automation users are included by default. Comprehensive Explanation and References of answer: According to the Splunk SOAR (On-premises) default credentials, script options, and sample

configuration files documentation1, the default credentials on a new installation of Splunk SOAR (On-premises) are:

Web Interface Username: soar_local_admin password: password

On Splunk SOAR (On-premises) deployments which have been upgraded from earlier releases the user account admin becomes a normal user account with the Administrator role.

The automation user is a special user account that is used by Splunk SOAR (On-premises) to run actions and playbooks. It has the Automation role, which grants it full access to all objects and data in Splunk SOAR (On-premises).

The other options are incorrect because they either omit the automation user or include users that are not created by default. For example, option B includes the power and user users, which are not part of the default installation. Option C only includes the admin user, which ignores the automation user. Option D claims that no users are included by default, which is false.

In a new installation of Splunk SOAR, two default user accounts are typically created: admin and automation.

The admin account is intended for system administration tasks, providing full access to all features and settings within the SOAR platform. The automation user is a special account used for automated processes and scripts that interact with the SOAR platform, often without requiring direct human intervention. This user has specific permissions that can be tailored for automated tasks. Options B, C, and D do not accurately represent the default user accounts included in a new SOAR installation, making option A the correct answer.

Q19. Which of the following are examples of things commonly done with the Phantom REST APP
* Use Django queries; use curl to create a container and add artifacts to it; remove temporary lists.
* Use Django queries; use curl to create a container and add artifacts to it; add action blocks.
* Use Django queries; use Docker to create a container and add artifacts to it; remove temporary lists.
* Use SQL queries; use curl to create a container and add artifacts to it; remove temporary lists.

Explanation

The correct answer is A because using Django queries, using curl to create a container and add artifacts to it, and removing temporary lists are examples of things commonly done with the Phantom REST APP. The Phantom REST APP is a built-in app that allows you to interact with the Phantom server using REST API calls. You can use the run query action to execute Django queries on the Phantom database and return the results as JSON. You can use the curl command to send HTTP requests to the Phantom server and perform various operations, such as creating containers, adding artifacts, running playbooks, etc. You can use the remove list action to delete temporary lists that are no longer needed. See Splunk SOAR Documentation for more details.

Q20. When the Splunk App for SOAR Export executes a Splunk search, which activities are completed?
* CEF fields are mapped to CIM flelds and a container is created on the SOAR server.
* CIM fields are mapped to CEF fields and a container is created on the SOAR server.
* CEF fields are mapped to CIM and a container is created on the Splunk server.
* CIM fields are mapped to CEF and a container is created on the Splunk server.

When the Splunk App for SOAR Export executes a Splunk search, it typically involves mapping Common Information Model (CIM) fields from Splunk to the Common Event Format (CEF) used by SOAR, after which a container is created on the SOAR server to house the related artifacts and information. This process allows for the integration of data between Splunk, which uses CIM for data normalization, and Splunk SOAR, which uses CEF as its data format for incidents and events.

Splunk App for SOAR Export is responsible for sending data from your Splunk Enterprise or Splunk Cloud instances to Splunk SOAR. The Splunk App for SOAR Export acts as a translation service between the Splunk platform and Splunk SOAR by performing the following tasks:

*Mapping fields from Splunk platform alerts, such as saved searches and data models, to CEF fields.

*Translating CIM fields from Splunk Enterprise Security (ES) notable events to CEF fields.

*Forwarding events in CEF format to Splunk SOAR, which are stored as artifacts.

Therefore, option B is the correct answer, as it states the activities that are completed when the Splunk App for SOAR Export executes a Splunk search. Option A is incorrect, because CEF fields are not mapped to CIM fields, but the other way around. Option C is incorrect, because a container is not created on the Splunk server, but on the SOAR server. Option D is incorrect, because a container is not created on the Splunk server, but on the SOAR server.

Q21. What is enabled if the Logging option for a playbook’s settings is enabled?
* More detailed logging information Is available m the Investigation page.
* All modifications to the playbook will be written to the audit log.
* More detailed information is available in the debug window.
* The playbook will write detailed execution information into the spawn.log.

In Splunk SOAR (formerly known as Phantom), enabling the Logging option for a playbook’s settings primarily affects how logging information is displayed on the Investigation page. When this option is enabled, more detailed logging information is made available on the Investigation page, which can be crucial for troubleshooting and understanding the execution flow of the playbook. This detailed information can include execution steps, actions taken, and conditional logic paths followed during the playbook run.

It’s important to note that enabling logging does not affect the audit logs or the debug window directly, nor does it write execution details to the spawn.log. Instead, it enhances the visibility and granularity of logs displayed on the specific Investigation page related to the playbook’s execution.

References:

Splunk Documentation and SOAR User Guides typically outline the impacts of enabling various settings within the playbook configurations, explaining how these settings affect the operation and logging within the system. For specific references, consulting the latest Splunk SOAR documentation would provide the most accurate and detailed guidance.

Enabling the Logging option for a playbook’s settings in Splunk SOAR indeed affects the level of detail provided on the Investigation page. Here’s a comprehensive explanation of its impact:

Investigation Page Logging:

The Investigation page serves as a centralized location for reviewing all activities related to an incident or event within Splunk SOAR.

When the Logging option is enabled, it enhances the level of detail available on this page, providing a granular view of the playbook’s execution.

This includes detailed information about each action’s execution, such as parameters used, results obtained, and any conditional logic that was evaluated.

Benefits of Detailed Logging:

Troubleshooting: It becomes easier to diagnose issues within a playbook when you can see a detailed log of its execution.

Incident Analysis: Analysts can better understand the sequence of events and the decisions made by the playbook during an incident.

Playbook Optimization: Developers can use the detailed logs to refine and improve the playbook’s logic and performance.

Non-Impacted Areas:

The audit log, which tracks changes to the playbook itself, is not affected by the Logging option.

The debug window, used for real-time debugging during playbook development, also remains unaffected.

The spawn.log file, which contains internal operational logs for the Splunk SOAR platform, does not receive detailed execution information from playbooks.

Best Practices:

Enable detailed logging during the development and testing phases of a playbook to ensure thorough analysis and debugging.

Consider the potential impact on storage and performance when enabling detailed logging in a production environment.

References:

For the most accurate and up-to-date guidance on playbook settings and their effects, I recommend consulting the latest Splunk SOAR documentation and user guides. These resources provide in-depth information on configuring playbooks and understanding the implications of various settings within the Splunk SOAR platform.

In summary, the Logging option is a powerful feature that enhances the visibility of playbook operations on the Investigation page, aiding in incident analysis and ensuring that playbooks are functioning correctly. It is an essential tool for security teams to effectively manage and respond to incidents within their environment.

Q22. What are indicators?
* Action result items that determine the flow of execution in a playbook.
* Action results that may appear in multiple containers.
* Artifact values that can appear in multiple containers.
* Artifact values with special security significance.

Indicators within the context of Splunk SOAR refer to artifact values that have special security significance.

These are typically derived from the data within artifacts and are identified as having particular importance in the analysis and investigation of security incidents. Indicators might include items such as IP addresses, domain names, file hashes, or other data points that can be used to detect, correlate, and respond to security threats. Recognizing and managing indicators effectively is key to leveraging SOAR for enhanced threat intelligence, incident response, and security operations efficiency.

Q23. Which of the following is a step when configuring event forwarding from Splunk to Phantom?
* Map CIM to CEF fields.
* Create a Splunk alert that uses the event_forward.py script to send events to Phantom.
* Map CEF to CIM fields.
* Create a saved search that generates the JSON for the new container on Phantom.

Q24. Which of the following are tabs of an asset configuration?
* Asset Name, Asset IP, Asset URL, Asset Nickname
* Tags, Asset Name, Asset Date, Asset Order
* App Name, App Order, App Expiry, App Version
* Asset Info, Asset Settings, Approval Settings, Access Control

In Splunk SOAR, the asset configuration consists of several key tabs that are essential for setting up and managing an asset. These tabs include:

* Asset Info: Contains general information about the asset, such as its name and description.

* Asset Settings: This tab allows for configuring specific settings related to the asset, including any connections or integrations.

* Approval Settings: This section manages settings related to the approval process for actions that require explicit authorization.

* Access Control: This tab helps control user access to the asset, specifying permissions and roles.

These four tabs are essential for configuring an asset in SOAR, making sure the asset works as expected and that the right people have access to it.

References:

* Splunk SOAR Documentation: Asset Configuration.

* Splunk SOAR Best Practices: Asset Management and Configuration.

Q25. After a playbook has run, where are the results stored?
* Splunk Index
* Case
* Container
* Log file

Q26. A filter block with only one condition configured which states: artifact.*.cef .sourceAddress !- , would permit which of the following data to pass forward to the next block?
* Null IP addresses
* Non-null IP addresses
* Non-null destinationAddresses
* Null values

A filter block with only one condition configured which states: artifact.*.cef .sourceAddress !- , would permit only non-null IP addresses to pass forward to the next block. The !- operator means “is not null”. The other options are not valid because they either include null values or other fields than sourceAddress. See Filter block for more details. A filter block in Splunk SOAR that is configured with the condition artifact.*.cef.sourceAddress != (assuming the intention was to use “!=” to denote ‘not equal to’) is designed to allow data that has non-null sourceAddress values to pass through to subsequent blocks. This means that any artifact data within the container that includes a sourceAddress field with a defined value (i.e., an actual IP address) will be permitted to move forward in the playbook. The filter effectively screens out any artifacts that do not have a source address specified, focusing the playbook’s actions on those artifacts that contain valid IP address information in the sourceAddress field.

Q27. Which app allows a user to send Splunk Enterprise Security notable events to Phantom?
* Any of the integrated Splunk/Phantom Apps
* Splunk App for Phantom Reporting.
* Splunk App for Phantom.
* Phantom App for Splunk.

Q28. How does a user determine which app actions are available?
* Add an action block to a playbook canvas area.
* Search the Apps category in the global search field.
* From the Apps menu, click the supported actions dropdown for each app.
* In the visual playbook editor, click Active and click the Available App Actions dropdown.

In Splunk SOAR, a user can determine which app actions are available by navigating to the Apps menu.

From there, the user can click on the supported actions dropdown for each app to view the actions that can be performed by that app. This dropdown menu provides a list of all the actions that the app is capable of executing, allowing the user to understand the functionality provided by the app and how it can be utilized within playbooks11.

References:

Add and configure apps and assets to provide actions in Splunk SOAR (Cloud) – Splunk Documentation

Q29. What is the default embedded search engine used by SOAR?
* Embedded Splunk search engine.
* Embedded SOAR search engine.
* Embedded Django search engine.
* Embedded Elastic search engine.

the default embedded search engine used by SOAR is the SOAR search engine, which is powered by the PostgreSQL database built-in to Splunk SOAR (Cloud). A Splunk SOAR (Cloud) Administrator can configure options for search from the Home menu, in Search Settings under Administration Settings. The SOAR search engine has been modified to accept the * wildcard and supports various operators and filters.

For search syntax and examples, see Search within Splunk SOAR (Cloud)2.

Option A is incorrect, because the embedded Splunk search engine was used in earlier releases of Splunk SOAR (Cloud), but not in

the current version. Option C is incorrect, because Django is a web framework, not a search engine. Option D is incorrect, because Elastic is a separate search engine that is not embedded in Splunk SOAR (Cloud).

1: Configure search in Splunk SOAR (Cloud) 2: Search within Splunk SOAR (Cloud) Splunk SOAR utilizes its own embedded search engine by default, which is tailored to its security orchestration and automation framework. While Splunk SOAR can integrate with other search engines, like the Embedded Splunk search engine, for advanced capabilities and log analytics, its default setup comes with an embedded search engine optimized for the typical data and search patterns encountered within the SOAR platform.

Q30. Which of the following expressions will output debug information to the debug window in the Visual Playbook Editor?
* phantom.debug()
* phantom.exception()
* phantom.print ()
* phantom.assert()

The SPLK-2003 exam covers a wide range of topics related to Splunk Phantom, including automation workflows, playbook creation, data management, system administration, and integration with third-party tools. Candidates must have a good understanding of how to use Splunk Phantom to streamline their organization's security operations, reduce incident response times, and improve overall security posture. A Splunk Phantom Certified Admin can help their organization to leverage the full potential of the platform and achieve better security outcomes.

Prepare for the Actual Splunk SOAR Certified Automation Developer SPLK-2003 Exam Practice Materials Collection: https://www.test4engine.com/SPLK-2003_exam-latest-braindumps.html]