Latest Success Metrics For Actual SPLK-2003 Exam 2025 Realistic Dumps [Q23-Q42

Latest Success Metrics For Actual SPLK-2003 Exam 2025 Realistic Dumps Updated SPLK-2003 Dumps Questions For Splunk Exam Q23. Playbooks typically handle which types of data?
* Container data, Artifact CEF data, Result data. Threat data
* Container CEF data, Artifact data, Result data, List data
* Container data, Artifact CEF data, Result data, List data
* Container data, Artifact data, Result data, Threat data

Playbooks in Splunk SOAR are designed to handle various types of data to automate responses to security incidents. The correct types of data handled by playbooks include:

* Container Data: Containers are used to group related data for an incident or event. Playbooks can access this information to perform actions and make decisions.

* Artifact CEF Data: Artifacts hold detailed information about the event or incident, including CEF (Common Event Format) data. Playbooks often process this CEF data for various actions.

* Result Data: This refers to the data generated from actions executed by the playbook, such as results from API calls, integrations, or automated responses.

* List Data: Lists in Splunk SOAR are collections of reusable data (such as IP blocklists, whitelists, etc.) that playbooks can access to check values or make decisions based on external lists.

The inclusion of List data instead of Threat data distinguishes this option from others, as lists are more directly used by playbooks during execution, whereas threat data is a broader category that is often processed but not always directly handled by playbooks.

References:

* Splunk SOAR Documentation: Playbook Data Handling.

* Splunk SOAR Best Practices: Automating with Playbooks.

Q24. When working with complex data paths, which operator is used to access a sub-element inside another element?
* !(pipe)
* *(asterisk)
* :(colon)
* .(dot)
When working with complex data paths in Splunk SOAR, particularly within playbooks, the dot (.) operator is used to access sub-elements within a larger data structure. This operator allows for the navigation through nested data, such as dictionaries or objects within JSON responses, enabling playbook actions and decision blocks to reference specific pieces of data within the artifacts or action results. This capability is crucial for extracting and manipulating relevant information from complex data sets during incident analysis and response automation.

Q25. 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.
* Reduce large complex playbooks which become difficult to maintain.
* Encourages code reuse in a more compartmentalized form.
* To avoid duplication of code across multiple playbooks.
Creating smaller and more focused playbooks in Splunk SOAR is considered good design practice for several reasons:

*B: It reduces complexity, making playbooks easier to maintain. Large, complex playbooks can become unwieldy and difficult to troubleshoot or update.

*C: Encourages code reuse, as smaller playbooks can be designed to handle specific tasks that can be reused across different scenarios.

*D: Avoids duplication of code, as common functionalities can be centralized within specific playbooks, rather than having the same code replicated across multiple playbooks.

This approach has several benefits, such as:

*Reducing large complex playbooks which become difficult to maintain. Smaller playbooks are easier to read, debug, and update1.

*Encouraging code reuse in a more compartmentalized form. Smaller playbooks can be used as building blocks for multiple scenarios, reducing the need to write duplicate code12.

*Improving performance and scalability. Smaller playbooks can run faster and consume less resources than larger playbooks2.

The other options are not valid reasons for creating smaller and more focused playbooks. Reducing the amount of playbook data

stored in each repo is not a significant benefit, as the playbook data is not very large compared to other types of data in Splunk SOAR. Avoiding duplication of code across multiple playbooks is a consequence of code reuse, not a separate goal.

Q26. After a successful POST to a Phantom REST endpoint to create a new object what result is returned?
* The new object ID.
* The new object name.
* The full CEF name.
* The PostGres UUID.

The correct answer is A because after a successful POST to a Phantom REST endpoint to create a new object, the result returned is the new object ID. The object ID is a unique identifier for each object in Phantom, such as a container, an artifact, an action, or a playbook. The object ID can be used to retrieve, update, or delete the object using the Phantom REST API. The answer B is incorrect because after a successful POST to a Phantom REST endpoint to create a new object, the result returned is not the new object name, which is a human-readable name for the object. The object name can be used to search for the object using the Phantom web interface. The answer C is incorrect because after a successful POST to a Phantom REST endpoint to create a new object, the result returned is not the full CEF name, which is a standard format for event data. The full CEF name can be used to access the CEF fields of an artifact using the Phantom REST API. The answer D is incorrect because after a successful POST to a Phantom REST endpoint to create a new object, the result returned is not the PostGres UUID, which is a unique identifier for each row in a PostGres database. The PostGres UUID is not exposed to the Phantom REST API. Reference: Splunk SOAR REST API Guide, page

17. When a POST request is made to a Phantom REST endpoint to create a new object, such as an event, artifact, or container, the typical response includes the ID of the newly created object. This ID is a unique identifier that can be used to reference the object within the system for future operations, such as updating, querying, or deleting the object. The response does not usually include the full name or other specific details of the object, as the ID is the most important piece of information needed immediately after creation for reference purposes.

Q27. What does a user need to do to have a container with an event from Splunk use context-aware actions designed for notable events?
* Include the notable event’s event_id field and set the artifacts label to aplunk notable event id.
* Rename the event_id field from the notable event to splunkNotableEventId.
* Include the event_id field in the search results and add a CEF definition to Phantom for event_id, datatype splunk notable event id.
* Add a custom field to the container named event_id and set the custom field’s data type to splunk notable event id.

Explanation

The correct answer is A because to have a container with an event from Splunk use context-aware actions designed for notable events, you need to include the notable event’s event_id field and set the artifact’s label to splunk notable event id. Context-aware actions are actions that are specific to a certain type of artifact, such as Splunk notable events, Jira tickets, ServiceNow incidents, etc. To use context-aware actions, you need to label the artifacts with the appropriate type and include the required fields. For Splunk notable events, the required field is event_id, which is the unique identifier of the event in Splunk. See Splunk SOAR Documentation for more details.

Q28. How can more than one user perform tasks in a workbook?
* Any user in a role with write access to the case’s workbook can be assigned to tasks.
* Add the required users to the authorized list for the container.
* Any user with a role that has Perform Task enabled can execute tasks for workbooks.
* The container owner can assign any authorized user to any task in a workbook.

In Splunk SOAR, tasks within workbooks can be performed by any user whose role has the ‘Perform Task’ capability enabled. This capability is assigned within the role configuration and allows users with the appropriate permissions to execute tasks. It is not limited to users with write access or the container owner; rather, it is based on the specific permissions

granted to the role with which the user is associated.

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

The default embedded search engine used by Splunk SOAR (formerly known as Phantom) is the embedded Splunk search engine. Here’s a detailed explanation:

Embedded Splunk Search Engine:

Splunk SOAR uses an embedded, preconfigured version of Splunk Enterprise as its native search engine.

This integration allows for powerful searching capabilities within Splunk SOAR, leveraging Splunk’s robust search and indexing features.

Search Configuration:

While the embedded Splunk search engine is the default, organizations have the option to configure Splunk SOAR to use a different Splunk Enterprise deployment or an external Elasticsearch instance.

This flexibility allows organizations to tailor their search infrastructure to their specific needs and existing environments.

Search Capabilities:

The embedded Splunk search engine enables users to perform complex searches, analyze data, and generate reports directly within the Splunk SOAR platform.

It supports the full range of Splunk’s search processing language (SPL) commands, functions, and visualizations.

References:

Splunk SOAR Documentation: Configure search in Splunk Phantom1.

Splunk SOAR Documentation: Configure search in Splunk SOAR (On-premises)2.

In summary, the embedded Splunk search engine is the default search engine in Splunk SOAR, providing a seamless and powerful search experience for users within the platform.

Q30. What is the default embedded search engine used by Phantom?
* Embedded Splunk search engine.
* Embedded Phantom search engine.
* Embedded Elastic search engine.
* Embedded Django search engine.

Explanation

The default embedded search engine used by Phantom is the Embedded Elastic search engine. This engine provides fast and scalable search capabilities for Phantom data. The other options are not valid search engines for Phantom. See [Search engine configuration] for more information.

Q31. During a second test of a playbook, a user receives an error that states: ‘an empty parameters list was passed to phantom.act().” What does this indicate?
* The playbook debugger’s scope is set to all.
* The playbook is using an incorrect container.
* The container has artifacts not parameters.
* The playbook debugger’s scope is set to new.

Explanation

The correct answer is C because the error message indicates that the playbook debugger’s scope is set to new.

The scope option determines which containers are used for debugging the playbook. If the scope is set to new, the debugger will only use containers that are created after the debugger is started. If the scope is set to all, the debugger will use all containers that match the playbook’s filter criteria. The error message means that the debugger did not find any new containers with parameters to pass to the phantom.act() function. See Splunk SOAR Documentation for more details.

Q32. Phantom supports multiple user authentication methods such as LDAP and SAML2. What other user authentication method is supported?
* SAML3
* PIV/CAC
* Biometrics
* OpenID

Explanation

The correct answer is B because Phantom supports PIV/CAC as another user authentication method besides LDAP and SAML2. PIV/CAC stands for Personal Identity Verification (PIV) or Common Access Card (CAC) and is a smart card that can be used to authenticate users to Phantom. SAML3 is not a valid authentication method. Biometrics and OpenID are not supported by Phantom. See Splunk SOAR Documentation for more details.

Q33. Which is the primary system requirement that should be increased with heavy usage of the file vault?
* Amount of memory.
* Number of processors.
* Amount of storage.
* Bandwidth of network.

The primary system requirement that should be increased with heavy usage of the file vault is the amount of storage. The file vault is a secure repository for storing files on Phantom. The more files are stored, the more storage space is needed. The other options are not directly related to the file vault usage. See [File vault] for more information.

Heavy usage of the file vault in Splunk SOAR necessitates an increase in the amount of storage available. The file vault is used to securely store files associated with cases, such as malware samples, logs, and other artifacts relevant to an investigation. As the volume of files and the size of stored data grow, ensuring sufficient storage capacity becomes critical to maintain performance and ensure that all necessary data is retained for analysis and evidence.

Q34. Which visual playbook editor block is used to assemble commands and data into a valid Splunk search within a SOAR playbook?
* An action block.
* A filter block.
* A format block.
* A prompt block.

In Splunk SOAR playbook development, the format block is used to assemble commands and data into a valid Splunk search query.

This block allows users to structure and manipulate strings, dynamically inserting variables, and constructing the precise format needed for a search query. By using a format block, playbooks can integrate data from various sources and ensure that it is assembled correctly before passing it to subsequent actions, such as executing a Splunk search.

Other blocks, like action, filter, and prompt blocks, serve different purposes (e.g., running actions, filtering data, or prompting for user input), but the format block is specifically designed for building structured data or queries like Splunk searches.

References:

* Splunk SOAR Documentation: Playbook Blocks Overview.

* Splunk SOAR Playbook Editor Guide: Using the Format Block.

Q35. What is the main purpose of using a customized workbook?
* Workbooks automatically implement a customized processing of events using Python code.
* Workbooks guide user activity and coordination during event analysis and case operations.
* Workbooks apply service level agreements (SLAs) to containers and monitor completion status on the ROI dashboard.
* Workbooks may not be customized; only default workbooks are permitted within Phantom.

The main purpose of using a customized workbook is to guide user activity and coordination during event analysis and case operations. Workbooks can be customized to include different phases, tasks, and instructions for the users. The other options are not valid purposes of using a customized workbook. See Workbooks for more information.

Customized workbooks in Splunk SOAR are designed to guide users through the process of analyzing events and managing cases. They provide a structured framework for documenting investigations, tracking progress, and ensuring that all necessary steps are followed during incident response and case management. This helps in coordinating team efforts, maintaining consistency in response activities, and ensuring that all aspects of an incident are thoroughly investigated and resolved. Workbooks can be customized to fit the specific processes and procedures of an organization, making them a versatile tool for managing security operations.

Q36. 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()

Explanation

The correct answer is A because the phantom.debug() function is used to output debug information to the debug window in the Visual Playbook Editor. This function can be useful for troubleshooting and testing playbooks. The answer B is incorrect because the phantom.exception() function is used to output exception information to the debug window in the Visual Playbook Editor. This function can be useful for handling errors and exceptions in playbooks. The answer C is incorrect because the phantom.print() function is used to output information to the standard output stream in the Phantom server. This function can be useful for logging and auditing purposes. The answer D is incorrect because the phantom.assert() function is used to check if a condition is true or false and raise an exception if it is false. This function can be useful for validating inputs and outputs in playbooks. Reference: Splunk SOAR Playbook Development Guide, page 22.

Q37. Which Phantom API command is used to create a custom list?
* phantom.add_list()
* phantom.create_list()
* phantom.include_list()
* phantom.new_list()

Q38. 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

Explanation

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.

Q39. 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.

Q40. In addition to full backups. Phantom supports what other backup type using backup?
* Snapshot
* Incremental
* Partial
* Differential

Explanation

Phantom supports two types of backups: full and snapshot. A full backup creates a complete copy of the Phantom system, including all data, configuration, and apps. A snapshot backup creates a copy of the Phantom system configuration and apps, but not the data. Incremental and differential backups are not supported by Phantom. Reference, page 4.

Q41. Without customizing container status within Phantom, what are the three types of status for a container?
* New, In Progress, Closed
* Low, Medium, High
* Mew, Open, Resolved
* Low, Medium, Critical

Within Splunk SOAR, containers (which represent incidents, cases, or events) have a lifecycle that is tracked through their status. The default statuses available without any customization are “New”, “In Progress”, and

“Closed”. These statuses help in organizing and managing the incident response process, allowing users to easily track the progress of investigations and responses from initial detection through to resolution.

Q42. 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.

Explanation

The Logging option for a playbook’s settings enables more detailed logging information to be available in the Investigation page. This can help with debugging and troubleshooting the playbook execution. The other options are not related to the Logging

option. See Playbook settings for more information.