SPLK-2003$^{Q\&As}$

Splunk SOAR Certified Automation Developer

Pass Splunk SPLK-2003 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.geekcert.com/splk-2003.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Splunk Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

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

A. Reduces amount of playbook data stored in each repo.

B. Reduce large complex playbooks which become difficult to maintain.

C. Encourages code reuse in a more compartmentalized form.

D. To avoid duplication of code across multiple playbooks.

Correct Answer: BCD

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 update.

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 code.

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

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.

QUESTION 2

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?

A. Null IP addresses

B. Non-null IP addresses

C. Non-null destinationAddresses

D. Null values

Correct Answer: B

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.

QUESTION 3

Which of the following is a reason to create a new role in SOAR?

A. To define a set of users who have access to a special label.

B. To define a set of users who have access to a restricted app.

C. To define a set of users who have access to an event\\'s reports.

D. To define a set of users who have access to a sensitive tag.

Correct Answer: A

Creating a new role in Splunk SOAR is often done to define a set of users who have specific access rights, such as access to a special label. Labels in SOAR can be used to categorize data and control access. By assigning a role with access to a particular label, administrators can ensure that only a specific group of users can view or interact with containers, events, or artifacts that have been tagged with that label, thus maintaining control over sensitive data or operations.

QUESTION 4

A user selects the New option under Sources on the menu. What will be displayed?

A. A list of new assets.

B. The New Data Ingestion wizard.

C. A list of new data sources.

D. A list of new events.

Correct Answer: B

Selecting the New option under Sources in the Splunk SOAR menu typically initiates the New Data Ingestion wizard. This wizard guides users through the process of configuring new data sources for ingestion into the SOAR platform. It is designed to streamline the setup of various data inputs, such as event logs, threat intelligence feeds, or notifications from other security tools, ensuring that SOAR can receive and process relevant security data efficiently. This feature is crucial for expanding SOAR\\'s monitoring and response capabilities by integrating diverse data sources. Options A, C,

and D do not accurately describe what is displayed when the New option under Sources is selected, making option B the correct choice. New Data Ingestion wizard allows you to create a new data source for Splunk SOAR (On- premises) by selecting the type of data, the ingestion method, and the configuration options. The other options are incorrect because they do not match the description of the New option under Sources on the menu. For example, option A refers to a list of new assets, which is not related to data ingestion. Option C refers to a list of new data sources, which is not what the New option does. Option D refers to a list of new events, which is not the same as creating a new data source.

QUESTION 5

How can a child playbook access the parent playbook\\'s action results?

A. Child playbooks can access parent playbook data while the parent Is still running.

B. By setting scope to ALL when starting the child.

C. When configuring the playbook block in the parent, add the desired results in the Scope parameter.

D. The parent can create an artifact with the data needed by the did.

Correct Answer: C

In Splunk Phantom, child playbooks can access the action results of a parent playbook through the use of the Scope parameter. When a parent playbook calls a child playbook, it can pass certain data along by setting the Scope parameter to include the desired action results. This parameter is configured within the playbook block that initiates the child playbook. By specifying the appropriate scope, the parent playbook effectively determines what data the child playbook will have access to, allowing for a more modular and organized flow of information between playbooks.