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.pass4itsure.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

Without customizing container status within SOAR, what are the three types of status for a container?

A. New, Open, Resolved

B. Low, Medium, High

C. New, In Progress, Closed

D. Low, Medium, Critical

Correct Answer: C

In Splunk SOAR, without any customization, the three default statuses for a container are New, In Progress, and Closed. These statuses are designed to reflect the lifecycle of an incident or event within the platform, from its initial detection

and logging (New), through the investigation and response stages (In Progress), to its final resolution and closure (Closed). These statuses help in organizing and prioritizing incidents, tracking their progress, and ensuring a structured

workflow. Options A, B, and D do not accurately represent the default container statuses within SOAR, making option C the correct answer. containers are the top-level data structure that SOAR playbook APIs operate on. Containers can

have different statuses that indicate their state and progress in the SOAR workflow. Without customizing container status within SOAR, the three types of status for a container are:

New: The container has been created but not yet assigned or investigated.

In Progress: The container has been assigned and is being investigated or automated.

Closed: The container has been resolved or dismissed and no further action is required. Therefore, option C is the correct answer, as it lists the three types of status for a container without customizing container status within SOAR. Option A

is incorrect, because Resolved is not a type of status for a container without customizing container status within SOAR, but rather a custom status that can be defined by an administrator. Option B is incorrect, because Low, Medium, and High

are not types of status for a container, but rather types of severity that indicate the urgency or impact of a container. Option D is incorrect, for the same reason as option B.

Web search results from search_web(query="Splunk SOAR Automation Developer container status")

QUESTION 2

Which of the following applies to filter blocks?

A. Can select which blocks have access to container data.

B. Can select assets by tenant, approver, or app.

C. Can be used to select data for use by other blocks.

D. Can select containers by seventy or status.

Correct Answer: C

The correct answer is C because filter blocks can be used to select data for use by other blocks. Filter blocks can filter data from the container, artifacts, or custom lists based on various criteria, such as field name, value, operator, etc. Filter blocks can also join data from multiple sources using the join action. The output of the filter block can be used as input for other blocks, such as decision, format, prompt, etc. See Splunk SOAR Documentation for more details. Filter blocks within Splunk SOAR playbooks are designed to sift through data and select specific pieces of information based on defined criteria. These blocks are crucial for narrowing down the data that subsequent blocks in a playbook will act upon. By applying filters, a playbook can focus on relevant data, thereby enhancing efficiency and ensuring that actions are taken based on precise, contextually relevant information. This capability is essential for tailoring the playbook\\'s actions to the specific needs of the incident or workflow, enabling more targeted and effective automation strategies. Filters do not directly select blocks for container data access, choose assets by various administrative criteria, or select containers by attributes like severity or status; their primary function is to refine data within the playbook\\'s operational context.

QUESTION 3

What does a user need to do to have a container with an event from Splunk use context- aware actions designed for notable events?

A. Include the notable event\\'s event_id field and set the artifacts label to aplunk notable event id.

B. Rename the event_id field from the notable event to splunkNotableEventId.

C. Include the event_id field in the search results and add a CEF definition to Phantom for event_id, datatype splunk notable event id.

D. Add a custom field to the container named event_id and set the custom field\\'s data type to splunk notable event id.

Correct Answer: C

For a container in Splunk SOAR to utilize context-aware actions designed for notable events from Splunk, it is crucial to ensure that the notable event\\'s unique identifier (event_id) is included in the search results pulled into SOAR. Moreover, by adding a Common Event Format (CEF) definition for the event_id field within Phantom, and setting its data type to something that denotes it as a Splunk notable event ID, SOAR can recognize and appropriately handle these identifiers. This setup facilitates the correct mapping and processing of notable event data within SOAR, enabling the execution of context-aware actions that are specifically tailored to the characteristics of Splunk notable events.

QUESTION 4

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

A. Non-Human

B. Automation

C. Automation Engineer

D. Service Account

Correct Answer: A

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.

QUESTION 5

Which app allows a user to run Splunk queries from within Phantom?

A. Splunk App for Phantom?

B. The Integrated Splunk/Phantom app.

C. Phantom App for Splunk.

D. Splunk App for Phantom Reporting.

Correct Answer: C

The Phantom App for Splunk allows a user to run Splunk queries from within Phantom. This app provides actions such as run query, ingest events, and save search, which enable the user to interact with Splunk from Phantom playbooks or the Phantom UI. The other apps are not relevant for this use case. The Splunk App for Phantom is used to send data from Splunk to Phantom. The Integrated Splunk/Phantom app is a deprecated app that was replaced by the Splunk App for Phantom. The Splunk App for Phantom Reporting is used to generate reports on Phantom activity from Splunk. The Phantom App for Splunk is the application that enables Splunk users to run Splunk queries from within the Splunk Phantom platform. This app integrates Splunk\\'s data and search capabilities into Phantom\\'s security automation and orchestration framework, allowing users to perform actions such as running searches, creating events, and updating records in Splunk directly from Phantom.