

# **Splunk Phantom Certified Admin Updated Study Material & SPLK-2003 Online Test Simulator & Splunk Phantom Certified Admin Valid Exam Answers**



What's more, part of that DumpsValid SPLK-2003 dumps now are free: [https://drive.google.com/open?id=1nffnzsrtH\\_GYUDP9BCXsuov81snMVs](https://drive.google.com/open?id=1nffnzsrtH_GYUDP9BCXsuov81snMVs)

As is known to us, there are best sale and after-sale service of the SPLK-2003 certification training materials all over the world in our company. Our company has employed many excellent experts and professors in the field in the past years, in order to design the best and most suitable SPLK-2003 Latest Questions for all customers. More importantly, it is evident to all that the SPLK-2003 training materials from our company have a high quality, and we can make sure the quality of our products will be higher than other study materials in the market.

Have similar features to the desktop-based exam simulator Contains actual Splunk SPLK-2003 practice test that will help you grasp every topic Compatible with every operating system Does not require any special plugins to operate. Creates a SPLK-2003 Exam atmosphere making candidates more confident. Keeps track of your progress with self-analysis and Points out mistakes at the end of every attempt.

**>> SPLK-2003 Latest Exam Format <<**

## **Hot SPLK-2003 Latest Exam Format | Professional Splunk SPLK-2003 Test Engine: Splunk Phantom Certified Admin**

We are willing to provide all people with the demo of our SPLK-2003 study tool for free. If you have any doubt about our products that will bring a lot of benefits for you. The trial demo of our SPLK-2003 question torrent must be a good choice for you. By the trial demo provided by our company, you will have the opportunity to closely contact with our SPLK-2003 Exam Torrent, and it will be possible for you to have a view of our products. More importantly, we provide all people with the trial demo for free before you buy our SPLK-2003 exam torrent.

## **Splunk Phantom Certified Admin Sample Questions (Q88-Q93):**

### **NEW QUESTION # 88**

Which of the following is an advantage of using the Visual Playbook Editor?

- A. Easier playbook maintenance.
- B. Supports Python or Javascript.
- C. Eliminates any need to use Python code.
- D. The Visual Playbook Editor is the only way to generate user prompts.

**Answer: A**

Explanation:

Visual Playbook Editor is a feature of Splunk SOAR that allows you to create, edit, and implement automated playbooks using

visual building blocks and execution flow lanes, without having to write code. The Visual Playbook Editor automatically generates the code for you, which you can view and edit in the Code Editor if needed. The Visual Playbook Editor also supports Python and Javascript as scripting languages for custom code blocks. One of the advantages of using the Visual Playbook Editor is that it makes playbook maintenance easier, as you can quickly modify, test, and debug your playbooks using the graphical interface. Therefore, option D is the correct answer, as it states an advantage of using the Visual Playbook Editor. Option A is incorrect, because using the Visual Playbook Editor does not eliminate the need to use Python code, but rather simplifies the process of creating and editing code. You can still add custom Python code to your playbooks using the custom function block or the Code Editor. Option B is incorrect, because the Visual Playbook Editor is not the only way to generate user prompts, but rather one of the ways. You can also generate user prompts using the classic playbook editor or the Code Editor. Option C is incorrect, because supporting Python or Javascript is not an advantage of using the Visual Playbook Editor, but rather a feature of Splunk SOAR in general. You can use Python or Javascript in any of the playbook editors, not just the Visual Playbook Editor.

1: Web search results from search\_web(query="Splunk SOAR Automation Developer Visual Playbook Editor")

### NEW QUESTION # 89

On a multi-tenant Phantom server, what is the default tenant's ID?

- A. Default
- **B. \***
- C. 0
- D. 1

**Answer: B**

### NEW QUESTION # 90

Which of the following can be configured in the ROI Settings?

- A. Time lost.
- B. Analyst hours per month.
- **C. Number of full time employees (FTEs).**
- D. Annual analyst salary.

**Answer: C**

Explanation:

The ROI (Return on Investment) Settings within Splunk SOAR are designed to help organizations assess the value derived from their use of the platform, particularly in terms of resource allocation and efficiency gains. The setting mentioned in the question, "Number of full time employees (FTEs)," relates directly to measuring this efficiency.

Answer "C" is correct because configuring the number of full-time employees (FTEs) in the ROI settings allows an organization to input and monitor how many personnel are dedicated to security operations managed through SOAR. This setting is crucial for calculating the labor cost associated with incident response and routine security tasks. By understanding the number of FTEs involved, organizations can better assess the labor cost savings provided by automation and orchestration in SOAR. This data helps in quantifying the operational efficiency and the overall impact of SOAR on resource optimization.

In contrast, other options like "Analyst hours per month," "Time lost," and "Annual analyst salary" might seem relevant but are not directly configurable within the ROI settings of Splunk SOAR.

These aspects could be indirectly calculated or estimated based on the number of FTEs and other operational metrics but are not directly input as settings in the system.

This use of FTEs in ROI calculations is often discussed in materials related to cybersecurity efficiency metrics and SOAR platform utilization. Official Splunk documentation and best practices guides typically provide insights into how to set up and interpret ROI settings, highlighting the importance of accurate configuration for meaningful analytics.

### NEW QUESTION # 91

How does a user determine which app actions are available?

- A. In the visual playbook editor, click Active and click the Available App Actions dropdown.
- **B. Add an action block to a playbook canvas area.**
- C. From the Apps menu, click the supported actions dropdown for each app.
- D. Search the Apps category in the global search field.

**Answer: B**

Explanation:

Explanation

A user can determine which app actions are available by adding an action block to a playbook canvas area.

The action block will show a list of all the apps installed on the Phantom system and the actions supported by each app. The other options do not provide a comprehensive view of the app actions available. Reference, page 11.

**NEW QUESTION # 92**

Where in SOAR can a user view the JSON data for a container?

- A. In the data ingestion display.
- B. In the audit log.
- C. **On the Investigation page.**
- D. In the analyst queue.

**Answer: C**

Explanation:

In Splunk SOAR, the Investigation page is where users can delve into the details of containers, artifacts, and actions. It provides a comprehensive view of the incident or event under investigation, including the JSON data associated with containers. This JSON data represents the structured information about the container, including its attributes, artifacts, and actions taken within the playbook. Options A, C, and D do not typically provide a direct view of the container's JSON data, making option B the correct answer for where a user can view this information within SOAR.

A container is the top-level data structure that SOAR playbook APIs operate on. Every container is a structured JSON object which can nest more arbitrary JSON objects, that represent artifacts. A container is the top-level object against which automation is run. To view the JSON data for a container, you need to navigate to the Investigation page, which shows the details of a container, such as its name, label, owner, status, severity, and artifacts. On the Investigation page, you can click on the JSON tab, which displays the JSON representation of the container and its artifacts. Therefore, option B is the correct answer, as it states where in SOAR a user can view the JSON data for a container. Option A is incorrect, because the analyst queue is not where a user can view the JSON data for a container, but rather where a user can view the list of containers assigned to them or their team. Option C is incorrect, because the data ingestion display is not where a user can view the JSON data for a container, but rather where a user can view the status and configuration of the data sources that ingest data into SOAR. Option D is incorrect, because the audit log is not where a user can view the JSON data for a container, but rather where a user can view the history of actions performed on the SOAR system, such as creating, updating, or deleting objects.

1: Understanding containers in Splunk SOAR (Cloud)

**NEW QUESTION # 93**

.....

SPLK-2003 study material is suitable for all people. Whether you are a student or an office worker, whether you are a veteran or a rookie who has just entered the industry, SPLK-2003 test answers will be your best choice. For office workers, SPLK-2003 test dumps provide you with more flexible study time. You can download learning materials to your mobile phone and study at anytime, anywhere. And as an industry rookie, those unreadable words and expressions in professional books often make you feel mad, but SPLK-2003 Study Materials will help you to solve this problem perfectly.

**SPLK-2003 Test Engine:** <https://www.dumpsvalid.com/SPLK-2003-still-valid-exam.html>

Splunk SPLK-2003 Latest Exam Format For the examinees who are the first time to participate IT certification exam, choosing a good pertinent training program is very necessary, Splunk SPLK-2003 Latest Exam Format And what is the opportunity, You do not need to look around for the latest Splunk SPLK-2003 training materials, because you have to find the best Splunk SPLK-2003 training materials, These latest Splunk Phantom Certified Admin SPLK-2003 exam topics are added in all Splunk SPLK-2003 exam questions formats.

How Ants Exchange Knowledge: Stigmergy, Many Java method calls can be passed SPLK-2003 arguments, For the examinees who are the first time to participate IT certification exam, choosing a good pertinent training program is very necessary.

**Latest Splunk Phantom Certified Admin exam pdf & SPLK-2003 exam**

## torrent

And what is the opportunity, You do not need to look around for the latest Splunk SPLK-2003 Training Materials, because you have to find the best Splunk SPLK-2003 training materials.

These latest Splunk Phantom Certified Admin SPLK-2003 exam topics are added in all Splunk SPLK-2003 exam questions formats, The first feature of DumpsValid SPLK-2003 exam questions is its availability of Splunk Phantom Certified Admin SPLK-2003 exam questions in three formats.

What's more, part of that DumpsValid SPLK-2003 dumps now are free: [https://drive.google.com/open?id=1nfnfzsrtH\\_GYUDP9BCXsuov81snMVs](https://drive.google.com/open?id=1nfnfzsrtH_GYUDP9BCXsuov81snMVs)