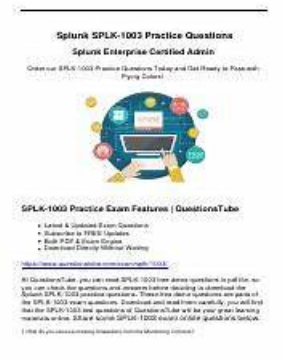
100% Pass Quiz Splunk - SPLK-2003 Updated Free Practice



BTW, DOWNLOAD part of Prep4cram SPLK-2003 dumps from Cloud Storage: https://drive.google.com/open?id=1QAeHzZ9kwDVcpAHyWZ33XVdOf7eyK_rU

Our SPLK-2003 quiz torrent can help you get out of trouble regain confidence and embrace a better life. Our SPLK-2003 exam question can help you learn effectively and ultimately obtain the authority certification of Splunk, which will fully prove your ability and let you stand out in the labor market. We have the confidence and ability to make you finally have rich rewards. Our SPLK-2003 Learning Materials provide you with a platform of knowledge to help you achieve your wishes. Our SPLK-2003 study materials have unique advantages for you to pass the SPLK-2003 exam.

Splunk SPLK-2003 certification exam is designed for IT professionals who want to demonstrate their expertise in managing and administering the Splunk Phantom platform. Splunk Phantom is a security orchestration, automation, and response (SOAR) platform that helps organizations automate their security operations and reduce response times to security incidents. The SPLK-2003 Exam is targeted at administrators and operators who are responsible for configuring, managing, and deploying Splunk Phantom in their organization.

>> Free SPLK-2003 Practice <<

Quiz Unparalleled Splunk - SPLK-2003 - Free Splunk Phantom Certified Admin Practice

Prep4cram regularly updates Splunk Phantom Certified Admin (SPLK-2003) practice exam material to ensure that it keeps in line with the test. In the same way, Prep4cram provides a free demo before you purchase so that you may know the quality of the

SPLK-2003 dumps. Similarly, the Splunk SPLK-2003 practice test creates an actual exam scenario on each and every step so that you may be well prepared before your actual SPLK-2003 examination time. Hence, it saves you time and money. Prep4cram provides three months of free updates if you purchase the Splunk SPLK-2003 questions and the content of the examination changes after that.

Splunk Phantom Certified Admin Sample Questions (Q96-Q101):

NEW QUESTION # 96
When configuring a Splunk asset for SOAR to connect to a Splunk Cloud instance, the user discovers that they need to be able to run two different on_poll searches. How is this possible?

- A. Install a second Splunk app and configure the query in the second app.
- B. Configure a second Splunk asset with the second query.
- C. Configure the second query in the Splunk App for SOAR Export.
- D. Enter the two queries in the asset as comma separated values.

Answer: B

Explanation:
In Splunk SOAR, when needing to run multiple on_poll searches to a Splunk Cloud instance, the recommended approach is to configure a second Splunk asset specifically for the second query.
This method allows each Splunk asset to maintain its own settings and query configurations, ensuring that each search can be managed and optimized independently. This separation also helps in troubleshooting and maintaining clarity in the configuration.
When configuring a Splunk asset for SOAR to connect to a Splunk Cloud instance and there is a need to run two different on_poll searches, the appropriate action is to configure a second Splunk asset with the second query. This allows each Splunk asset to have its own unique on_poll search configuration, enabling them to run independently and retrieve different sets of data as required. The other options, such as installing a second app or entering queries as comma- separated values, are not standard practices for managing multiple on_poll searches in Splunk SOAR.

NEW QUESTION # 97
When writing a custom function that uses regex to extract the domain name from a URL, a user wants to create a new artifact for the extracted domain. Which of the following Python API calls will create a new artifact?

- A. phantom.add_artifact ()
- B. phantom.new_artifact ()
- C. phantom. update ()
- D. phantom.create_artifact ()

Answer: D

Explanation:
In the Splunk SOAR platform, when writing a custom function in Python to handle data such as extracting a domain name from a URL, you can create a new artifact using the Python API call phantom.create_artifact().
This function allows you to specify the details of the new artifact, such as the type, CEF (Common Event Format) data, container it belongs to, and other relevant information necessary to create an artifact within the system.

NEW QUESTION # 98
What do assets provide for app functionality?

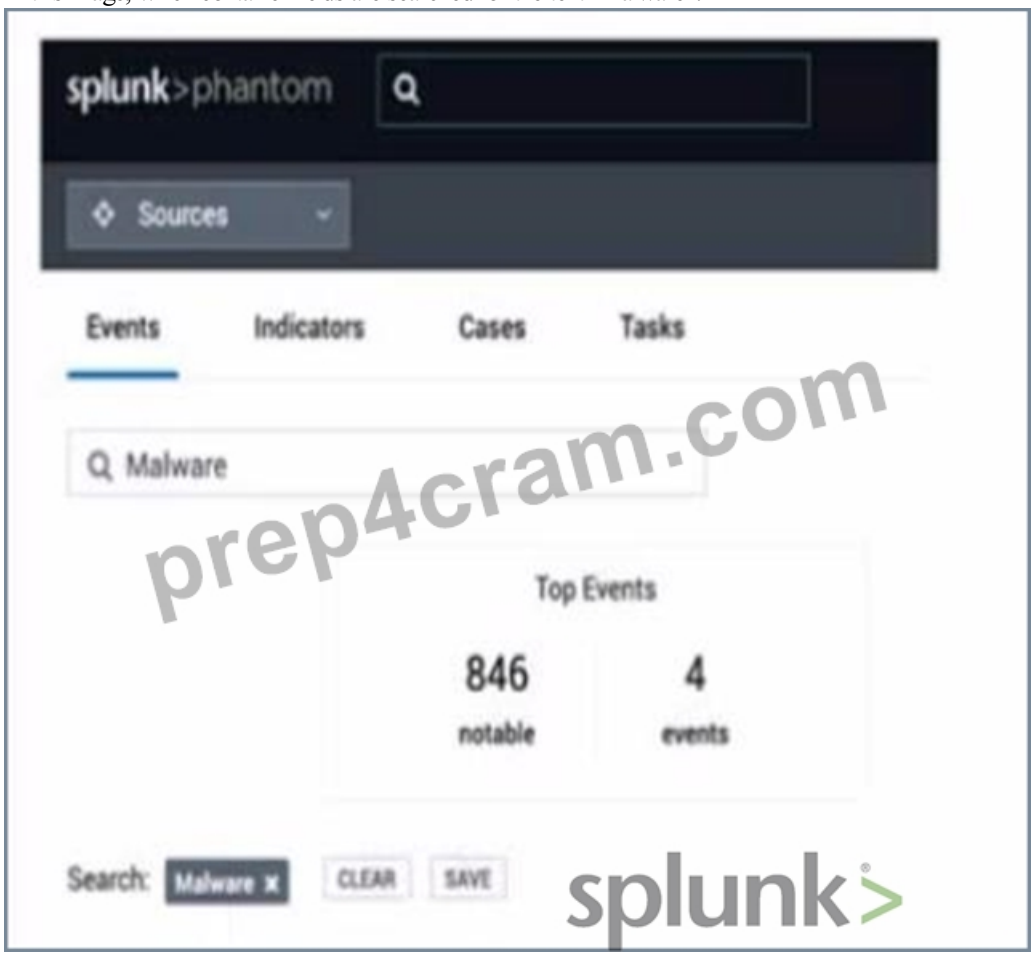
- A. Assets provide firewall, network, and data sources needed to run actions.
- B. Assets provide Python code, REST API, and other capabilities needed to run actions.
- C. Assets provide location, credentials, and other parameters needed to run actions.
- D. Assets provide hostnames, passwords, and other artifacts needed to run actions.

Answer: C

Explanation:
Explanation
The correct answer is A because assets provide location, credentials, and other parameters needed to run actions. Assets are

configurations that define how Phantom connects to external systems or devices, such as firewalls, endpoints, or threat intelligence sources. Assets specify the app, the IP address or hostname, the username and password, and any other settings required to run actions on the target system or device. The answer B is incorrect because assets do not provide hostnames, passwords, and other artifacts needed to run actions, which are data objects that can be created or retrieved by playbooks. The answer C is incorrect because assets do not provide Python code, REST API, and other capabilities needed to run actions, which are provided by apps. The answer D is incorrect because assets do not provide firewall, network, and data sources needed to run actions, which are external systems or devices that can be connected to by assets.
Reference: Splunk SOAR Admin Guide, page 45.

NEW QUESTION # 99
In this image, which container fields are searched for the text "Malware"?



- A. Event Name, Notes, Comments.
- B. Event Name and Artifact Names.
- C. Event Name or ID.

Answer: B

Explanation:
The image shows a user interface of "splunk>phantom" with a search bar at the top, where a search for "Malware" has been initiated. The tabs labeled "Events," "Indicators," "Cases," and "Tasks" suggest that the search functionality could span across various container fields within the Splunk SOAR environment.
Typically, the search would include fields that are most relevant to the user's query, which in this case, are likely to be the Event Name and Artifact Names. These fields are central to identifying and categorizing events and artifacts within Splunk SOAR, making them primary targets for a search term like "Malware" which is commonly associated with security events and indicators17.
References:
* Understanding containers - Splunk Documentation

NEW QUESTION # 100

In the SOAR main menu, there are sub-options below Sources. What is the purpose of these options?

- A. They permit analysts to select the app that is polled to create the containers.
- B. They are only available for admins and would never be used by an analyst.
- C. They permit analysts to select cases related to an investigation.
- D. They filter the container list based on default or user-saved filters.

Answer: D

NEW QUESTION # 101
.....

With the rapid development of society, people pay more and more attention to knowledge and skills. So every year a large number of people take SPLK-2003 tests to prove their abilities. But even the best people fail sometimes. In addition to the lack of effort, may also not make the right choice. A good choice can make one work twice the result with half the effort, and our SPLK-2003 study materials will be your right choice. Since inception, our company has been working on the preparation of SPLK-2003 learning guide, and now has successfully helped tens of thousands of candidates around the world to pass the exam. As a member of the group who are about to take the SPLK-2003 exam, are you worried about the difficulties in preparing for the exam? Maybe this problem can be solved today, if you are willing to spend a few minutes to try our SPLK-2003 actual exam.