SPLK-2003 Latest Exam Camp | SPLK-2003 VCE Dumps

What's more, part of that DumpsTests SPLK-2003 dumps now are free: https://drive.google.com/open?id=1aMB7MFiq-un-6MQnZdbz7uw4p9R_0B6N

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.

Obtaining the SPLK-2003 Certification demonstrates that an individual has the knowledge and skills required to administer the Splunk Phantom platform. Splunk Phantom Certified Admin certification is highly valued by employers and can lead to better job opportunities and higher salaries. It also validates an individual's expertise in SOAR and cybersecurity automation, which are in high demand in today's rapidly evolving cybersecurity landscape.

To prepare for the SPLK-2003 exam, candidates should have a strong understanding of security operations and incident response processes. They should also be familiar with Splunk Phantom's architecture, features, and capabilities. Splunk offers a range of training courses and resources to help candidates prepare for the exam, including the Phantom Certified Admin Course and the Phantom Fundamentals eLearning course. Additionally, candidates can benefit from hands-on experience working with the platform and participating in Splunk's online community to learn from other users and experts. Obtaining the Splunk Phantom Certified Admin certification can help IT professionals advance their careers in security operations and demonstrate their expertise in using advanced automation and orchestration tools to improve their organization's security posture.

>> SPLK-2003 Latest Exam Camp <<

SPLK-2003 VCE Dumps & SPLK-2003 Latest Materials

If you DumpsTests, DumpsTests can ensure you 100% pass Splunk Certification SPLK-2003 Exam. If you fail to pass the exam, DumpsTests will full refund to you.

Splunk Phantom Certified Admin Sample Questions (Q50-Q55):

NEW QUESTION # 50
Which of the following are examples of things commonly done with the Phantom REST APP

- A. Use Django queries; use curl to create a container and add artifacts to it; remove temporary lists.
- B. Use Django queries; use Docker to create a container and add artifacts to it; remove temporary lists.
- C. Use SQL queries; use curl to create a container and add artifacts to it; remove temporary lists.
- D. Use Django queries; use curl to create a container and add artifacts to it; add action blocks.

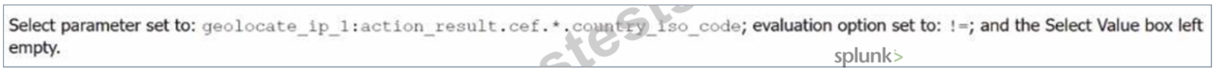
Answer: D

Explanation:
The Phantom REST API, often interacted with through the Phantom REST APP, is a powerful tool for automating and integrating Splunk SOAR with other systems. Common uses of the Phantom REST APP include using Django queries to interact with the SOAR database, using curl commands to programmatically create containers and add artifacts to them, and configuring action blocks within playbooks for automated actions. This flexibility allows for a wide range of automation and integration possibilities, enhancing the SOAR platform's capability to respond to security incidents and manage data.

NEW QUESTION # 51

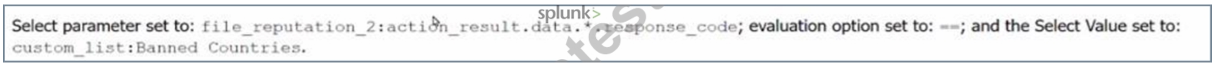
Two action blocks, geolocate_ip 1 and file_reputation_2, are connected to a decision block. Which of the following is a correct configuration for making a decision on the action results from one of the given blocks?

- A.



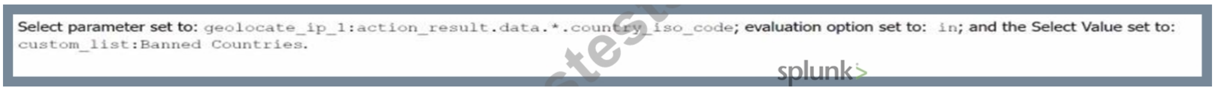
Select parameter set to: `geolocate_ip_1:action_result.cef.*.country_iso_code`; evaluation option set to: `!=`; and the Select Value box left empty.

- B.



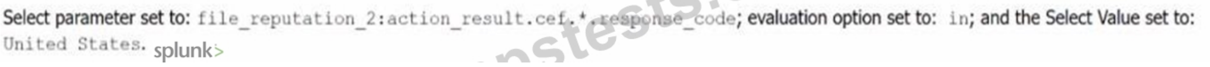
Select parameter set to: `file_reputation_2:action_result.data.*.response_code`; evaluation option set to: `==`; and the Select Value set to: `custom_list:Banned Countries`.

- C.



Select parameter set to: `geolocate_ip_1:action_result.data.*.country_iso_code`; evaluation option set to: `in`; and the Select Value set to: `custom_list:Banned Countries`.

- D.



Select parameter set to: `file_reputation_2:action_result.cef.*.response_code`; evaluation option set to: `in`; and the Select Value set to: `United States`.

Answer: A

Explanation:

In the given decision block, you are trying to evaluate the results of two action blocks: geolocate_ip_1 and file_reputation_2. The correct configuration for making a decision based on the result of geolocate_ip_1 is by checking the country_iso_code field from the action result and setting the evaluation option to != (not equal), with no specific value provided in the "Select Value" box. This essentially checks whether a valid country ISO code exists in the action result and proceeds if it's not empty or different from a specific value. This is a common check when working with geolocation results to see if a response has been returned.

Other options (B, C, and D) include response codes or list comparisons, which do not align with the decision structure mentioned, which needs to operate based on a country_iso_code field.

References:

* Splunk SOAR Playbook Development Guide.

* Splunk SOAR Documentation on Decision Blocks and Action Result Evaluation.

NEW QUESTION # 52

Which of the following applies to filter blocks?

- A. Can be used to select data for use by other blocks.
- B. Can select containers by seventy or status.
- C. Can select assets by tenant, approver, or app.
- D. Can select which blocks have access to container data.

Answer: D

NEW QUESTION # 53

Which of the following can be edited or deleted in the Investigation page?

- A. Approval records
- B. Action results
- C. Artifact values
- D. Comments

Answer: D

Explanation:

On the Investigation page in Splunk SOAR, users have the ability to edit or delete comments associated with an event or a container. Comments are generally used for collaboration and to provide additional context to an investigation. While action results, approval records, and artifact values are typically not editable or deletable to maintain the integrity of the investigative data, comments are more flexible and can be managed by users to reflect the current state of the investigation.

Investigation page allows you to view and edit various information and data related to an event or a case. One of the things that you can edit or delete in the Investigation page is the comments that you or other users have added to the activity feed. Comments are a way of communicating and collaborating with other users during the investigation process. You can edit or delete your own comments by clicking on the three-dot menu icon next to the comment and selecting the appropriate option. You can also reply to other users' comments by clicking on the reply icon.

NEW QUESTION # 54

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. Rename the event_id field from the notable event to splunkNotableEventId.
- B. Include the event_id field in the search results and add a CEF definition to Phantom for event_id, datatype splunk notable event id.
- C. Add a custom field to the container named event_id and set the custom field's data type to splunk notable event id.
- D. Include the notable event's event_id field and set the artifacts label to aplunk notable event id.

Answer: D

Explanation:

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.

NEW QUESTION # 55

......

- Splunk SPLK-2003 Latest Exam Camp: Splunk Phantom Certified Admin - Pdfvce Help you Pass Once □ Open website 【 www.pdfvce.com 】 and search for ➡ SPLK-2003 □□□ for free download □SPLK-2003 Latest Test Labs
- Certification SPLK-2003 Exam □ SPLK-2003 Valuable Feedback □ SPLK-2003 Valid Exam Voucher □ Search for ☀ SPLK-2003 □☀□ and download exam materials for free through 《 www.pass4leader.com 》 □SPLK-2003 Reliable Braindumps Ppt
- myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, tedcole945.oblogation.com, myportal.utt.edu.tt, erp.thetechgenacademy.com, www.mukalee.com, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, careerxpand.com, pct.edu.pk, Disposable vapes

BTW, DOWNLOAD part of DumpsTests SPLK-2003 dumps from Cloud Storage: https://drive.google.com/open?id=1aMB7MFiq-un-6MQnZdbz7uw4p9R_0B6N