最新SPLK-2003題庫資源，SPLK-2003考題免費下載

BONUS!!! 免費下載Testpdf SPLK-2003考試題庫的完整版：https://drive.google.com/open?id=1VIxD-7nRqXAb0a7v23Vwvv3JQBR3_b6B

我們Testpdf Splunk的SPLK-2003考試培訓資料給所有需要的人帶來最大的成功率，通過微軟的SPLK-2003考試是一個具有挑戰性的認證考試。現在除了書籍，互聯網被認為是一個知識的寶庫，在Testpdf你也可以找到屬於你的知識寶庫，這將是一個對你有很大幫助的網站，你會遇到複雜的測試方面的試題，我們Testpdf可以幫助你輕鬆的通過考試，它涵蓋了所有必要的知識Splunk的SPLK-2003考試。

獲得 Splunk Phantom 認證管理員認證可以使各種角色的專業人員受益，包括安全分析師、安全工程師和 IT 專業人員。此認證證明了對 Splunk Phantom 的全面理解和有效管理和自動化安全操作的能力。此外，此認證可以增強在資訊安全行業中的就業機會和增加收入潛力。

>> 最新SPLK-2003題庫資源 <<

SPLK-2003考題免費下載 & SPLK-2003題庫更新資訊

“如果放棄了，那比賽同時也就結束了。”這是來自安西教練的一句大家都熟知的名言。比賽是這樣，同樣考試也是這樣的。有很多人因為沒有充分的時間準備考試從而放棄了參加SPLK-2003認證考試。但是，如果使用了好的資料，即使只有很短的時間來準備，你也完全可以以高分通過SPLK-2003考試。不相信嗎？Testpdf的考古題就是這樣的資料。趕快試一下吧。

Splunk SPLK-2003考試是IT專業人員的重要認證，旨在展示他們在管理Splunk Phantom方面的專業知識。通過此認證，個人可以提升職業生涯、增加收入，並在競爭激烈的就業市場中脫穎而出。通過準備並通過考試，候選人可以證明他們具備管理和維護Splunk Phantom的知識和技能。

最新的 Splunk SOAR Certified Automation Developer SPLK-2003 免費考試真題 (Q85-Q90):

問題 #85
Which Phantom VPE Nock S used to add information to custom lists?

- A. Action blocks
- B. API blocks
- C. Filter blocks
- D. Decision blocks

答案：B

解題說明：
Filter blocks are used to add information to custom lists in Phantom VPE. Filter blocks allow the user to specify a list name and a filter expression to select the data to be added to the list. Action blocks are used to execute app actions, API blocks are used to make REST API calls, and decision blocks are used to evaluate conditions and branch the playbook execution. In the Phantom Visual Playbook Editor (VPE), an API block is used to interact with various external APIs, including custom lists within Phantom. Custom lists are key-value stores that can be used to maintain state, aggregate data, or track information across multiple playbook runs.
API blocks allow the playbook to make GET, POST, PUT, and DELETE requests to these lists, facilitating the addition, retrieval, update, or removal of information. This makes API blocks a versatile tool in managing custom list data within playbooks.

問題 #86
Which of the following expressions will output debug information to the debug window in the Visual Playbook Editor?

- A. phantom.exception()
- B. phantom.assert()
- C. phantom.print ()
- D. phantom.debug()

答案：B

問題 #87
How can a playbook run searches on a Splunk search head?

- A. Using the run_query action from the Splunk app.
- B. Using the phantom.run_query() API function.
- C. Using the search action of the Search app.
- D. Use the HTTP app's get_data action to access the SOAR .../rest/splunk/query endpoint.

答案：A

問題 #88
Seventy can be set during ingestion and later changed manually. What other mechanism can change the severity or a container?

- A. Playbooks
- B. Service level agreement (SLA) expiration
- C. Notes
- D. Actions

答案：A

解題說明：
The severity of a container in Splunk Phantom can be set manually or automatically during the ingestion process. In addition to these methods, playbooks can also change the severity of a container. Playbooks are automated workflows that define a series of actions based on certain triggers and conditions. Within a playbook, actions can be defined to adjust the severity level of a container depending on the analysis of the event data, the outcome of actions taken, or other contextual factors. This dynamic adjustment allows for a more accurate and responsive incident prioritization as new information becomes available during the investigation process.

問題 #89

After a playbook has run, where are the results stored?

- A. Splunk Index
- B. Log file
- C. Container
- D. Case

答案：C

解題說明：
Explanation
The correct answer is C because after a playbook has run, the results are stored in the container that triggered the playbook. The container is a data object that represents an event or a case in Phantom. The container contains information such as the name, the description, the severity, the status, the owner, and the labels of the event or case. The container also contains the artifacts, the action results, the comments, the notes, and the phases and tasks associated with the event or case. The answer A is incorrect because after a playbook has run, the results are not stored in a Splunk index, which is a data structure that stores events from various data sources in Splunk. The Splunk index is not directly accessible by Phantom, but can be queried by Phantom using the Splunk app. The answer B is incorrect because after a playbook has run, the results are not stored in a case, which is a type of container that represents a security incident in Phantom. The case is a subset of the container, and not all containers are cases. The answer D is incorrect because after a playbook has run, the results are not stored in a log file, which is a file that records the activities or events that occur in a system or a process. The log file is not a data object in Phantom, but can be a data source for Phantom. Reference: Splunk SOAR User Guide, page 19.

問題 #90
.....

7nRqXAb0a7v23Vwvv3JQBR3_b6B