有難いSPLK-2003｜一番優秀なSPLK-2003試験関連情報試験｜試験の準備方法Splunk Phantom Certified Admin合格受験記

BONUS！！！ Xhs1991 SPLK-2003ダンプの一部を無料でダウンロード：https://drive.google.com/open?id=1XUQoyrO6yWl4yxwhcbBw-EzymF57diVo

成功への道を示す指標として、私たちの練習資料はあなたの旅のあらゆる困難を乗り越えることができます。すべての課題をウォークインのように扱うことはできませんが、SPLK-2003シミュレーションの実践により、レビューを効果的にすることができます。それが彼らがラインのプロモデルである理由です。私たちは品質の問題に非妥協的であり、あなたは彼らの習熟度を厳しく完全に確信することができます。

Splunk Phantom認定管理者認定を獲得することは、サイバーセキュリティおよびITオペレーション分野の専門家に多くの利益をもたらすことができます。認定された個人は、Splunk Phantomプラットフォームを深く理解しており、セキュリティ運用とインシデント対応プロセスを効果的に管理するための知識とスキルを備えています。彼らは、サイバーセキュリティの姿勢を強化し、インシデント対応能力を向上させたい組織から非常に求められています。さらに、認定された個人は、より大きな雇用機会とより高い給与の恩恵を受けることができます。

SPLK-2003試験は、Splunk Phantomプラットフォームとその機能を確実に理解する必要がある包括的で挑戦的なテストです。試験の準備をするために、候補者はSplunk Phantomとの協力と、セキュリティの自動化とオーケストレーションの概念を深く理解した経験が必要です。また、一般的なセキュリティツールやテクノロジー、およびセキュリティ運用を管理するためのベストプラクティスにも精通している必要があります。 Splunk Phantom認定管理者認定により、専門家はサイバーセキュリティのこの重要な分野で専門知識を実証し、この分野でのキャリアの機会を強化することができます。

Splunk SPLK-2003は、Splunk Phantomを管理する知識とスキルを検証する業界で認められた資格です。Splunk Phantomプラットフォームは、セキュリティオペレーションの自動化とオーケストレーションの機能を提供し、組織がセキュリティインシデントをより効果的に検出、調査、対応できるようにします。SPLK-2003試験は、個人がSplunk Phantomプラットフォームを設定、管理、トラブルシューティングする能力をテストするために設計されています。

試験SPLK-2003試験関連情報 & 実用的なSPLK-2003合格受験記 | 大人気SPLK-2003模擬モード

Xhs1991は実際の環境で本格的なSplunkのSPLK-2003「Splunk Phantom Certified Admin」の試験の準備過程を提供しています。もしあなたは初心者若しくは専門的な技能を高めたかったら、Xhs1991のSplunkのSPLK-2003「Splunk Phantom Certified Admin」の試験問題があなたが一歩一歩自分の念願に近くために助けを差し上げます。試験問題と解答に関する質問があるなら、当社は直後に解決方法を差し上げます。しかも、一年間の無料更新サービスを提供します。

Splunk Phantom Certified Admin 認定 SPLK-2003 試験問題 (Q10-Q15):

質問 # 10
If no data matches any filter conditions, what is the next block run by the playbook?

- A. The filter block.
- B. The end block.
- C. The start block.
- D. The next block.

正解：D

解説：
In a Splunk SOAR playbook, if no data matches the conditions specified within a filter block, the playbook execution will proceed to the next block that is configured to follow the filter block. The
"next block" refers to whatever action or decision block is designed to be next in the sequence according to the playbook's logic. Filters in Splunk SOAR are used to make decisions based on data conditions, and they control the flow of the playbook. If the conditions in a filter block are not met, the playbook does not simply end or restart; rather, it continues to execute the subsequent blocks that have been set up to handle situations where the filter conditions are not met.
A filter block will typically have different paths for different outcomes--matching and non- matching. If the conditions are matched, one set of blocks will execute, and if not, another set of blocks, which could simply be the next one in the sequence, will execute. This allows for complex logic and branching within the playbook to handle a wide range of scenarios.
In a Splunk SOAR playbook, when no data matches any filter conditions, the playbook continues to run by proceeding to the next block in the sequence. The filter block is designed to specify a subset of artifacts before further processing, and only artifacts matching the specified condition are passed along to downstream blocks for processing. If no artifacts meet the conditions, the playbook does not end or restart; instead, it moves on to the next block, which could be any type of block depending on the playbook's design.

質問 # 11
Where can the Splunk App for SOAR Export be downloaded from?

- A. Splunk Answers and Splunkbase.
- B. SOAR Community and GitHub.
- C. GitHub and Splunkbase.
- D. Splunkbase and SOAR Community.

正解：C

解説：
The Splunk App for SOAR Export can be downloaded from both GitHub and Splunkbase. Splunkbase is the official source for Splunk apps, where users can find, try, and download apps that enhance and extend the capabilities of Splunk, including the Splunk App for SOAR Export1. GitHub is also a common platform for sharing and collaborating on code, including Splunk apps and integrations. It is important to ensure that you are downloading from the official repository or author to avoid any security risks.
References:
Splunkbase, the official source for downloading the Splunk App for SOAR Export

質問 # 12
After a playbook has run, where are the results stored?

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

正解：C

解説：
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.

質問 # 13
A user has written a playbook that calls three other playbooks, one after the other. The user notices that the second playbook starts executing before the first one completes. What is the cause of this behavior?

- A. Incorrect Join configuration on the second playbook.
- B. The steep option for the second playbook is not set to a long enough interval.
- C. Synchronous execution has not been configured.
- D. The first playbook is performing poorly.

正解：C

解説：
The correct answer is D because synchronous execution has not been configured. Synchronous execution is a feature that allows you to control the order of execution of playbook blocks. By default, Phantom executes playbook blocks asynchronously, meaning that it does not wait for one block to finish before starting the next one. This can cause problems when you have dependencies between blocks or when you call other playbooks. To enable synchronous execution, you need to use the sync action in the run playbook block and specify the name of the next block to run after the called playbook completes. See Splunk SOAR Documentation for more details.
In Splunk SOAR, playbooks can be executed either synchronously or asynchronously. Synchronous execution ensures that a playbook waits for a called playbook to complete before proceeding to the next step.
If the second playbook starts executing before the first one completes, it indicates that synchronous execution was not configured for the playbooks. Without synchronous execution, playbooks will execute independently of each other's completion status, leading to potential overlaps in execution. This behavior can be controlled by properly configuring the playbook execution settings to ensure that dependent playbooks complete their tasks in the desired order.

質問 # 14
Where can the Splunk App for SOAR Export be downloaded from?

- A. Splunk Answers and Splunkbase.
- B. SOAR Community and GitHub.
- C. GitHub and Splunkbase.
- D. Splunkbase and SOAR Community.

正解：C

解説：
The Splunk App for SOAR Export can be downloaded from both GitHub and Splunkbase.
Splunkbase is the official source for Splunk apps, where users can find, try, and download apps that enhance and extend the capabilities of Splunk, including the Splunk App for SOAR Export.
GitHub is also a common platform for sharing and collaborating on code, including Splunk apps and integrations. It is important to ensure that you are downloading from the official repository or author to avoid any security risks.

質問 # 15
.....

SPLK-2003テストガイドのサービスは非常に優れています。開発プロセスにおける顧客のニーズを常に考慮します。 SPLK-2003学習質問には、PDF、PC、およびAPPの3つのバージョンがあります。必要に応じて選択できます。もちろん、事前にSPLK-2003試験トレーニングの試用版を使用できます。それを使用した後、あなたはより深い経験を持つことになります。あなたの気持ちに応じて、お気に入りのSPLK-2003学習教材バージョンを選択できます。 SPLK-2003学習質問など、優れたサービス製品を選択する傾向があると思います