Free Questions for SPLK-2003

Shared by Herman on 22-07-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Which of the following supported approaches enables Phantom to run on a Windows server?

Options:

A- Install the Phantom RPM in a GNU Cygwin implementation.
B- Run the Phantom OVA as a cloud instance.
C- Install the Phantom RPM file in Windows Subsystem for Linux (WSL).
D- Run the Phantom OVA as a virtual machine.

Answer:

D

Explanation:

Splunk SOAR (formerly Phantom) does not natively run on Windows servers as it is primarily designed for Linux environments. However, it can be deployed on a Windows server through virtualization. By running the Phantom OVA (Open Virtualization Appliance) as a virtual machine, users can utilize virtualization platforms like VMware or VirtualBox on a Windows server to host the Phantom environment. This approach allows for the deployment of Phantom in a Windows-centric infrastructure by leveraging virtualization technology to encapsulate the Phantom application within a supported Linux environment provided by the OVA.

Question 2

Question Type: MultipleChoice

Some of the playbooks on the Phantom server should only be executed by members of the admin role. How can this rule be applied?

Options:

A- Add a filter block to al restricted playbooks that Titters for runRole - 'Admin''.
B- Add a tag with restricted access to the restricted playbooks.
C- Make sure the Execute Playbook capability is removed from al roles except admin.

D- Place restricted playbooks in a second source repository that has restricted access.

Answer:

C

Explanation:

The correct answer is C because the best way to restrict the execution of playbooks to members of the admin role is to make sure the Execute Playbook capability is removed from all roles except admin. The Execute Playbook capability is a permission that allows a user to run any playbook on any container. By default, all roles have this capability, but it can be removed or added in the Phantom UI by going to Administration > User Management > Roles. Removing this capability from all roles except admin will ensure that only admin users can execute playbooks. SeeSplunk SOAR Documentationfor more details. To ensure that only members of the admin role can execute specific playbooks on the Phantom server, the most effective approach is to manage role-based access controls (RBAC) directly. By configuring the system to remove the 'Execute Playbook' capability from all roles except for the admin role, you can enforce this rule. This method leverages Phantom's built-in RBAC mechanisms to restrict playbook execution privileges. It is a straightforward and secure way to ensure that only users with the necessary administrative privileges can initiate the execution of sensitive or critical playbooks, thus maintaining operational security and control.

Question 3

Question Type: MultipleChoice

Which of the following accurately describes the Files tab on the Investigate page?

Options:

A- A user can upload the output from a detonate action to the the files tab for further investigation.
B- Files tab items and artifacts are the only data sources that can populate active cases.
C- Files tab items cannot be added to investigations. Instead, add them to action blocks.
D- Phantom memory requirements remain static, regardless of Files tab usage.

Answer:

A

Explanation:

The Files tab on the Investigate page allows the user to upload, download, and view files related to an investigation. A user can upload the output from a detonate action to the Files tab for further investigation, such as analyzing the file metadata, content, or hash. Files tab items and artifacts are not the only data sources that can populate active cases, as cases can also include events, tasks, notes, and comments. Files tab items can be added to investigations by using the add file action block or the Add File button on the Files tab. Phantom memory requirements may increase depending on the Files tab usage, as files are stored in the Phantom database.

The Files tab on the Investigate page in Splunk Phantom is an area where users can manage and analyze files related to an investigation. Users can upload files, such as outputs from a 'detonate file' action which analyzes potentially malicious files in a sandbox environment. The files tab allows users to store and further investigate these outputs, which can include reports, logs, or any other file types that have been generated or are relevant to the investigation. The Files tab is an integral part of the investigation process, providing easy access to file data for analysis and correlation with other incident data.

Question 4

Question Type: MultipleChoice

A customer wants to design a modular and reusable set of playbooks that all communicate with each other. Which of the following is a best practice for data sharing across playbooks?

Options:

A- Use the py-postgresql module to directly save the data in the Postgres database.
B- Cal the child playbooks getter function.
C- Create artifacts using one playbook and collect those artifacts in another playbook.
D- Use the Handle method to pass data directly between playbooks.

Answer:

C

Explanation:

The correct answer is C because creating artifacts using one playbook and collecting those artifacts in another playbook is a best practice for data sharing across playbooks. Artifacts are data objects that are associated with a container and can be used to store information such as IP

addresses, URLs, file hashes, etc. Artifacts can be created using theadd artifactaction in any playbook block and can be collected using theget artifactsaction in thefilterblock. Artifacts can also be used to trigger active playbooks based on their label or type. SeeSplunk SOAR Documentationfor more details.

In the context of Splunk SOAR, one of the best practices for data sharing across playbooks is to create artifacts in one playbook and use another playbook to collect and utilize those artifacts. Artifacts in Splunk SOAR are structured data related to security incidents (containers) that playbooks can act upon. By creating artifacts in one playbook, you can effectively pass data and context to subsequent playbooks, allowing for modular, reusable, and interconnected playbook designs. This approach promotes efficiency, reduces redundancy, and enhances the playbook's ability to handle complex workflows.

Question 5

Question Type: MultipleChoice

Configuring Phantom search to use an external Splunk server provides which of the following benefits?

Options:

A- The ability to run more complex reports on Phantom activities.
B- The ability to ingest Splunk notable events into Phantom.
C- The ability to automate Splunk searches within Phantom.
D- The ability to display results as Splunk dashboards within Phantom.

Answer:

C

Explanation:

The correct answer is C because configuring Phantom search to use an external Splunk server allows you to automate Splunk searches within Phantom using therun queryaction. This action can be used to run any Splunk search command on the external Splunk server and return the results to Phantom. You can also use theformat resultsaction to parse the results and use them in other blocks. SeeSplunk SOAR Documentationfor more details.

Configuring Phantom (now known as Splunk SOAR) to use an external Splunk server enhances the automation capabilities within Phantom by allowing the execution of Splunk searches as part

of the automation and orchestration processes. This integration facilitates the automation of tasks that involve querying data from Splunk, thereby streamlining security operations and incident response workflows. Splunk SOAR's ability to integrate with over 300 third-party tools, including Splunk, supports a wide range of automatable actions, thus enabling a more efficient and effective security operations center (SOC) by reducing the time to respond to threats and by making repetitive tasks more manageable

https://www.splunk.com/en_us/products/splunk-security-orchestration-and-automation-features.html

Question 6

Question Type: MultipleChoice

Which app allows a user to run Splunk queries from within Phantom?

Options:

A- Splunk App for Phantom
B- The Integrated Splunk/Phantom app.
C- Phantom App for Splunk.
D- Splunk App for Phantom Reporting.

Answer:

A

Explanation:

The Splunk App for Phantom allows users to run Splunk queries directly from within the Phantom platform. This app facilitates the integration between Splunk and Phantom, enabling users to post data to Splunk as events, update notable events, run SPL (Search Processing Language) queries, and pull events from Splunk into Phantom.By configuring the asset settings and ingest settings in the configured asset, users can leverage the full capabilities of Splunk within the Phantom environment1.

Integrating Splunk Phantom with Splunk Enterprise - TekStream Solutions

Question 7

Question Type: MultipleChoice

Which of the following can the format block be used for?

Options:

A- To generate arrays for input into other functions.
B- To generate HTML or CSS content for output in email messages, user prompts, or comments.
C- To generate string parameters for automated action blocks.
D- To create text strings that merge state text with dynamic values for input or output.

Answer:

D

Explanation:

The format block in Splunk SOAR is utilized to construct text strings by merging static text with dynamic values, which can then be used for both input to other playbook blocks and output for reports, emails, or other forms of communication. This capability is essential for customizing messages, commands, or data processing tasks within a playbook, allowing for the dynamic insertion of variable data into predefined text templates. This feature enhances the playbook's ability to present information clearly and to execute actions that require specific parameter formats.

Question 8

Question Type: MultipleChoice

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?

Options:

A- Incorrect Join configuration on the second playbook.
B- The first playbook is performing poorly.

C- The steep option for the second playbook is not set to a long enough interval.
D- Synchronous execution has not been configured.

Answer:

D

Explanation:

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 thesyncaction in therun playbookblock and specify the name of the next block to run after the called playbook completes. SeeSplunk SOAR Documentationfor 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.