Splunk SPLK-2003 Mock Exam

Shared by Burt on 17-06-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

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

Options:

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

Answer:

D

Explanation:

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 processing1.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 design1.

Use filters in your Splunk SOAR (Cloud) playbook to specify a subset of artifacts before further processing - Splunk Documentation

Question 2

Question Type: MultipleChoice

After enabling multi-tenancy, which of the Mowing is the first configuration step?

Options:

A- Select the associated tenant artifacts.
B- Change the tenant permissions.
C- Set default tenant base address.
D- Configure the default tenant.

Answer:

D

Explanation:

Upon enabling multi-tenancy in Splunk SOAR, the first step in configuration typically involves setting up the default tenant. This foundational step is critical as it establishes the primary operating environment under which subsequent tenants can be created and managed. The default tenant serves as the template for permissions, settings, and configurations that might be inherited or customized by additional tenants. Proper configuration of the default tenant ensures a stable and consistent framework for multi-tenancy operations, allowing for segregated environments within the same SOAR instance, each tailored to specific operational needs or organizational units.

Question 3

Question Type: MultipleChoice

Splunk user account(s) with which roles must be created to configure Phantom with an external Splunk Enterprise instance?

Options:

A- superuser, administrator
B- phantomcreate. phantomedit

C- phantomsearch, phantomdelete
D- admin,user

Answer:

A

Explanation:

When configuring Splunk Phantom to integrate with an external Splunk Enterprise instance, it is typically required to have user accounts with sufficient privileges to access data and perform necessary actions. The roles of 'superuser' and 'administrator' in Splunk provide the broad set of permissions needed for such integration, enabling comprehensive access to data, management capabilities, and the execution of searches or actions that Phantom may require as part of its automated playbooks or investigations.

Question 4

Question Type: MultipleChoice

A user wants to use their Splunk Cloud instance as the external Splunk instance for Phantom. What ports need to be opened on the Splunk Cloud instance to facilitate this? Assume default ports are in use.

Options:

A- TCP 8088 and TCP 8099.
B- TCP 80 and TCP 443.
C- Splunk Cloud is not supported.
D- TCP 8080 and TCP 8191.

Answer:

B

Explanation:

To integrate Splunk Phantom with a Splunk Cloud instance, network communication over certain ports is necessary. The default ports for web traffic are TCP 80 for HTTP and TCP 443 for HTTPS. Since Splunk Cloud instances are accessed over the internet, ensuring that these ports are open

is essential for Phantom to communicate with Splunk Cloud for various operations, such as running searches, sending data, and receiving results. It is important to note that TCP 8088 is typically used by Splunk's HTTP Event Collector (HEC), which may also be relevant depending on the integration specifics.

Question 5

Question Type: MultipleChoice

Which option best is the complete list of the types of backups that are supported by Phantom?

Options:

A- Full backups.
B- Full, delta, and incremental backups.
C- Full and incremental backups.
D- Full and delta backups.

Answer:

C

Explanation:

Splunk Phantom supports different types of backups to safeguard data. Full backups create a complete copy of the current state of the system, while incremental backups only save the changes made since the last backup. This approach allows for efficient use of storage space and faster backups after the initial full backup. Delta backups, which would save changes since the last full or incremental backup, are not a standard part of Phantom's backup capabilities according to available documentation. Therefore, the complete list of backups supported by Phantom would be Full and Incremental backups.

Question 6

Question Type: MultipleChoice

Under Asset Ingestion Settings, how many labels must be applied when configuring an asset?

Options:

A- Labels are not configured under Asset Ingestion Settings.
B- One.
C- One or more.
D- Zero or more.

Answer:

D

Explanation:

Under Asset Ingestion Settings in Splunk SOAR, when configuring an asset, the number of labels that must be applied can be zero or more. Labels are optional and are used to categorize data and control access. They are not a requirement under Asset Ingestion Settings, but they can be used to enhance organization and filtering if chosen.