Splunk

Exam Questions SPLK-2003

Splunk Phantom Certified Admin

NEW QUESTION 1
What is the default log level for system health debug logs?

A. INFO
B. WARN
C. ERROR
D. DEBUG

Answer: A

Explanation:
The default log level for system health debug logs in Splunk SOAR is typically set to INFO. This log level provides a balance between verbosity and relevance, offering insights into the operational status of the system without the detailed granularity of DEBUG or the limited scope of WARN and ERROR levels.
The default log level for system health debug logs is INFO. This means that only informational messages and higher severity messages (such as WARN, ERROR, or CRITICAL) are written to the log files. You can adjust the logging level for each daemon running in Splunk SOAR to help debug or troubleshoot issues. For more details, see Configure the logging levels for Splunk SOAR (On-premises) daemons.

NEW QUESTION 2
Why does SOAR use wildcards within artifact data paths?

A. To make playbooks more specific.
B. To make playbooks filter out nulls.
C. To make data access in playbooks easier.
D. To make decision execution in playbooks run faster.

Answer: C

Explanation:
Wildcards are used within artifact data paths in Splunk SOAR playbooks to simplify the process of accessing data. They allow playbooks to reference dynamic or variable data structures without needing to specify exact paths, which can vary between artifacts. This flexibility makes it easier to write playbooks that work across different events and scenarios, without hard-coding data paths.
SOAR uses wildcards within artifact data paths to make data access in playbooks easier. A data path is a way of specifying the location of a piece of data within an artifact. For example, artifact.cef.sourceAddress is a data path that refers to the source address field of the artifact. A wildcard is a special character that can match any value or subfield within a data path. For example, artifact.*.cef.sourceAddress is a data path that uses a wildcard to match any field name before the cef subfield. This allows the playbook to access the source address data regardless of the field name, which can vary depending on the app or source that generated the artifact. Therefore, option C is the correct answer, as it explains why SOAR uses wildcards within artifact data paths. Option A is incorrect, because wildcards do not make playbooks more specific, but more flexible and adaptable. Option B is incorrect, because wildcards do not make playbooks filter out nulls, but match any value or subfield. Option D is incorrect, because wildcards do not make decision execution in playbooks run faster, but make data access in playbooks easier.
1: Understanding datapaths in Administer Splunk SOAR (Cloud)

NEW QUESTION 3
Which of the following are the steps required to complete a full backup of a Splunk Phantom deployment' Assume the commands are executed from /opt/phantom/bin and that no other backups have been made.

A. On the command line enter: rode sudo python ibackup.pyc --setup, then audo phenv python ibackup.pyc --backup.
B. On the command line enter: sudo phenv python ibackup.pyc --backup —backup-type full, then sudo phenv python ibackup.pyc --setup.
C. Within the UI: Select from the main menu Administration > System Health > Backup.
D. Within the UI: Select from the main menu Administration > Product Settings > Backup.

Answer: B

Explanation:
The correct answer is B because the steps required to complete a full backup of a Splunk Phantom deployment are to first run the --backup --backup-type full command and then run the --setup command. The --backup command creates a backup file in the /opt/phantom/backup directory. The --backup-type full option specifies that the backup file includes all the data and configuration files of the Phantom server.
The --setup command creates a configuration file that contains the encryption key and other information needed to restore the backup file. See Splunk SOAR Certified Automation Developer Track for more details.
Performing a full backup of a Splunk Phantom deployment involves using the command-line interface, primarily because Phantom's architecture and data management processes are designed to be managed at the server level for comprehensive backup and recovery. The correct sequence involves initiating a full backup first using the --backup --backup- type full option to ensure all configurations, data, and necessary components are included in the backup. Following the completion of the backup, the --setup option might be used to configure or verify the backup settings, although typically, the setup would precede backup operations in practical scenarios. This process ensures that all aspects of the Phantom deployment are preserved, including configurations, playbooks, cases, and other data, which is crucial for disaster recovery and system migration.

NEW QUESTION 4
After a successful POST to a Phantom REST endpoint to create a new object what result is returned?

A. The new object ID.
B. The new object name.
C. The full CEF name.
D. The PostGres UUID.

Answer: A

Explanation:
The correct answer is A because after a successful POST to a Phantom REST endpoint to create a new object, the result returned is the new object ID. The object ID is a unique identifier for each object in Phantom, such as a container, an artifact, an action, or a playbook. The object ID can be used to retrieve, update, or delete the object using the Phantom REST API. The answer B is incorrect because after a successful POST to a Phantom REST endpoint to create a new

object, the result returned is not the new object name, which is a human-readable name for the object. The object name can be used to search for the object using the Phantom web interface. The answer C is incorrect because after a successful POST to a Phantom REST endpoint to create a new object, the result returned is not the full CEF name, which is a standard format for event data. The full CEF name can be used to access the CEF fields of an artifact using the Phantom REST API. The answer D is incorrect because after a successful POST to a Phantom REST endpoint to create a new object, the result returned is not the PostGres UUID, which is a unique identifier for each row in a PostGres database. The PostGres UUID is not exposed to the Phantom REST API. Reference: Splunk SOAR REST API Guide, page 17. When a POST request is made to a Phantom REST endpoint to create a new object, such as an event, artifact, or container, the typical response includes the ID of the newly created object. This ID is a unique identifier that can be used to reference the object within the system for future operations, such as updating, querying, or deleting the object. The response does not usually include the full name or other specific details of the object, as the ID is the most important piece of information needed immediately after creation for reference purposes.

NEW QUESTION 5
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 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 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.

NEW QUESTION 6
Which of the following describes the use of labels m Phantom?

A. Labels determine the service level agreement (SLA) for a container.
B. Labels control the default seventy, ownership, and sensitivity for the container.
C. Labels control which apps are allowed to execute actions on the container.
D. Labels determine which playbook(s) are executed when a container is created.

Answer: D

Explanation:
In Splunk Phantom, labels are used to categorize containers and trigger specific automated responses. When a container is created, labels can be assigned to it based on the nature of the event, type of incident, or other criteria. These labels are then matched against playbooks, which have label conditions defined within them. When the conditions are met, the corresponding playbooks are automatically executed. Labels do not directly control service level agreements, default severity, ownership, sensitivity, or app execution permissions.

NEW QUESTION 7
A filter block with only one condition configured which states: artifact.*.cef .sourceAddress !- , would permit which of the following data to pass forward to the next block?

A. Null IP addresses
B. Non-null IP addresses
C. Non-null destinationAddresses
D. Null values

Answer: B

Explanation:
A filter block with only one condition configured which states: artifact.*.cef.sourceAddress !- , would permit only non-null IP addresses to pass forward to the next block. The !- operator means “is not null”. The other options are not valid because they either include null values or other fields than sourceAddress. See Filter block for more details. A filter block in Splunk SOAR that is configured with the condition artifact.*.cef.sourceAddress != (assuming the intention was to use "!=" to denote 'not equal to') is designed to allow data that has non-null sourceAddress values to pass through to subsequent blocks. This means that any artifact data within the container that includes a sourceAddress field with a defined value (i.e., an actual IP address) will be permitted to move forward in the playbook. The filter effectively screens out any artifacts that do not have a source address specified, focusing the playbook's actions on those artifacts that contain valid IP address information in the sourceAddress field.

NEW QUESTION 8
Which of the following is a step when configuring event forwarding from Splunk to Phantom?

A. Map CIM to CEF fields.
B. Create a Splunk alert that uses the event_forward.py script to send events to Phantom.
C. Map CEF to CIM fields.
D. Create a saved search that generates the JSON for the new container on Phantom.

Answer: B

Explanation:

A step when configuring event forwarding from Splunk to Phantom is to create a Splunk alert that uses the event_forward.py script to send events to Phantom. This script will convert the Splunk events to CEF format and send them to Phantom as containers. The other options are not valid steps for event forwarding. See Forwarding events from Splunk to Phantom for more details.
Configuring event forwarding from Splunk to Phantom typically involves creating a Splunk alert that leverages a script (like event_forward.py) to automatically send triggered event data to Phantom. This setup enables Splunk to act as a detection mechanism that, upon identifying notable events based on predefined criteria, forwards these events to Phantom for further orchestration, automation, and response actions. This integration streamlines the process of incident management by connecting Splunk's powerful data analysis capabilities with Phantom's orchestration and automation framework.

NEW QUESTION 9
What are the components of the I2A2 design methodology?

A. Inputs, Interactions, Actions, Apps
B. Inputs, Interactions, Actions, Artifacts
C. Inputs, Interactions, Apps, Artifacts
D. Inputs, Interactions, Actions, Assets

Answer: B

Explanation:
I2A2 design methodology is a framework for designing playbooks that consists of four components:
•Inputs: The data that is required for the playbook to run, such as artifacts, parameters, or custom fields.
•Interactions: The blocks that allow the playbook to communicate with users or other systems, such as prompts, comments, or emails.
•Actions: The blocks that execute the core logic of the playbook, such as app actions, filters, decisions, or utilities.
•Artifacts: The data that is generated or modified by the playbook, such as new artifacts, container fields, or notes.
The I2A2 design methodology helps you to plan, structure, and test your playbooks in a modular and efficient way. Therefore, option B is the correct answer, as it lists the correct components of the I2A2 design methodology. Option A is incorrect, because apps are not a component of the I2A2 design methodology, but a source of actions that can be used in the playbook. Option C is incorrect, for the same reason as option A. Option D is incorrect, because assets are not a component of the I2A2 design methodology, but a configuration of app credentials that can be used in the playbook.
1: Use a playbook design methodology in Administer Splunk SOAR (Cloud)
The I2A2 design methodology is an approach used in Splunk SOAR to structure and design playbooks. The acronym stands for Inputs, Interactions, Actions, and Artifacts. This methodology guides the creation of playbooks by focusing on these four key components, ensuring that all necessary aspects of an automated response are considered and effectively implemented within the platform.

NEW QUESTION 10
Which is the primary system requirement that should be increased with heavy usage of the file vault?

A. Amount of memory.
B. Number of processors.
C. Amount of storage.
D. Bandwidth of network.

Answer: C

Explanation:
The primary system requirement that should be increased with heavy usage of the file vault is the amount of storage. The file vault is a secure repository for storing files on Phantom. The more files are stored, the more storage space is needed. The other options are not directly related to the file vault usage. See [File vault] for more information. Heavy usage of the file vault in Splunk SOAR necessitates an increase in the amount of storage available. The file vault is used to securely store files associated with cases, such as malware samples, logs, and other artifacts relevant to an investigation. As the volume of files and the size of stored data grow, ensuring sufficient storage capacity becomes critical to maintain performance and ensure that all necessary data is retained for analysis and evidence.

NEW QUESTION 10
How can an individual asset action be manually started?

A. With the > action button in the analyst queue page.
B. By executing a playbook in the Playbooks section.
C. With the > action button in the Investigation page.
D. With the > asset button in the asset configuration section.

Answer: C

Explanation:
An individual asset action can be manually started with the > action button in the Investigation page. This allows the user to select an asset and an action to perform on it. The other options are not valid ways to start an asset action manually. See Performing asset actions for more information. Individual asset actions in Splunk SOAR can be manually initiated from the Investigation page of a container. The "> action" button on this page allows users to execute specific actions associated with assets directly, enabling on- the-fly operations on artifacts or indicators within a container. This feature is particularly useful for ad-hoc analysis and actions, allowing analysts to respond to or investigate specific aspects of an incident without the need for a full playbook.

NEW QUESTION 12
When the Splunk App for SOAR Export executes a Splunk search, which activities are completed?

A. CEF fields are mapped to CIM flelds and a container is created on the SOAR server.
B. CIM fields are mapped to CEF fields and a container is created on the SOAR server.
C. CEF fields are mapped to CIM and a container is created on the Splunk server.
D. CIM fields are mapped to CEF and a container is created on the Splunk server.

Answer: B

Explanation:

When the Splunk App for SOAR Export executes a Splunk search, it typically involves mapping Common Information Model (CIM) fields from Splunk to the Common Event Format (CEF) used by SOAR, after which a container is created on the SOAR server to house the related artifacts and information. This process allows for the integration of data between Splunk, which uses CIM for data normalization, and Splunk SOAR, which uses CEF as its data format for incidents and events.
Splunk App for SOAR Export is responsible for sending data from your Splunk Enterprise or Splunk Cloud instances to Splunk SOAR. The Splunk App for SOAR Export acts as a translation service between the Splunk platform and Splunk SOAR by performing the following tasks:
•Mapping fields from Splunk platform alerts, such as saved searches and data models, to CEF fields.
•Translating CIM fields from Splunk Enterprise Security (ES) notable events to CEF fields.
•Forwarding events in CEF format to Splunk SOAR, which are stored as artifacts. Therefore, option B is the correct answer, as it states the activities that are completed when the Splunk App for SOAR Export executes a Splunk search. Option A is incorrect, because CEF fields are not mapped to CIM fields, but the other way around. Option C is incorrect, because a container is not created on the Splunk server, but on the SOAR server. Option D is incorrect, because a container is not created on the Splunk server, but on the SOAR server.
1: Web search results from search_web(query="Splunk SOAR Automation Developer Splunk App for SOAR Export")

NEW QUESTION 15
On a multi-tenant Phantom server, what is the default tenant's ID?

A. Default
B. 1
C. *

Answer: C

Explanation:
The correct answer is C because the default tenant’s ID is 1. The tenant ID is a unique identifier for each tenant on a multi-tenant Phantom server. The default tenant is the tenant that is created when Phantom is installed and contains all the existing data and assets. The default tenant’s ID is always 1 and cannot be changed. Other tenants have IDs that are assigned sequentially starting from 2. See Splunk SOAR Documentation for more details. In a multi-tenant Splunk SOAR environment, the default tenant is typically assigned an ID of 1. This ID is system-generated and is used to uniquely identify the default tenant within the SOAR database and system configurations. The default tenant serves as the primary operational environment before any additional tenants are configured, and its ID is crucial for database operations, API calls, and internal reference within the SOAR platform. Understanding and correctly using tenant IDs is essential for managing resources, permissions, and data access in a multi-tenant SOAR setup.

NEW QUESTION 17
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. Synchronous execution has not been configured.
B. The first playbook is performing poorly.
C. The sleep option for the second playbook is not set to a long enough interval.
D. Incorrect join configuration on the second playbook.

Answer: A

Explanation:
In Splunk SOAR, playbooks can execute actions either synchronously (waiting for one action to complete before starting the next) or asynchronously (allowing actions to run concurrently). If a playbook starts executing before the previous one has completed, it indicates that synchronous execution has not been properly configured between these playbooks. This is crucial when the output of one playbook is a dependency for the subsequent playbook. Options B, C, and D do not directly address the observed behavior of concurrent playbook execution, making option A the most accurate explanation for why the second playbook starts before the completion of the first.
synchronous execution is a feature of the SOAR automation engine that allows you to control the order of execution of playbook blocks. Synchronous execution ensures that a playbook block waits for the completion of the previous block before starting its execution. Synchronous execution can be enabled or disabled for each playbook block in the playbook editor, by toggling the Synchronous Execution switch in the block settings. Therefore, option A is the correct answer, as it states the cause of the behavior where the second playbook starts executing before the first one completes. Option B is incorrect, because the first playbook performing poorly is not the cause of the behavior, but rather a possible consequence of the behavior. Option C is incorrect, because the sleep option for the second playbook is not the cause of the behavior, but rather a workaround that can be used to delay the execution of the second playbook. Option D is incorrect, because the join configuration on the second playbook is not the cause of the behavior, but rather a way of merging multiple paths of execution into one.
1: Web search results from search_web(query="Splunk SOAR Automation Developer synchronous execution")

NEW QUESTION 22
Which of the following is an asset ingestion setting in SOAR?

A. Polling Interval
B. Tag
C. File format
D. Operating system

Answer: A

Explanation:
The asset ingestion setting 'Polling Interval' within Splunk SOAR determines how frequently the SOAR platform will poll an asset to ingest data. This setting is crucial for assets that are configured to pull in data from external sources at regular intervals. Adjusting the polling interval allows administrators to balance the need for timely data against network and system resource considerations.
An asset ingestion setting is a configuration option that allows you to specify how often SOAR should poll an asset for new data. Data ingestion settings are available for assets such as QRadar, Splunk, and IMAP. To configure ingestion settings for an asset, you need to navigate to the Asset Configuration page, select the Ingest Settings tab, and edit the Polling Interval field. The Polling Interval is the number of seconds between each poll request that SOAR sends to the asset. Therefore, option A is the correct answer, as it is the only option that is an asset ingestion setting in SOAR. Option B is incorrect, because Tag is not an asset ingestion setting, but a way of labeling an asset for easier identification and filtering. Option C is incorrect, because File format is not an asset ingestion setting, but a way of specifying the format of the data that is ingested from an asset. Option D is incorrect, because Operating system is not an asset ingestion setting, but a way of identifying the type of system that an asset runs on.
1: Configure ingest settings for a Splunk SOAR (On-premises) asset

NEW QUESTION 27
When configuring a Splunk asset for SOAR to connect to a Splunk Cloud instance, the user discovers that they need to be able to run two different on_poll searches. How is this possible?

A. Install a second Splunk app and configure the query in the second app.
B. Configure the second query in the Splunk App for SOAR Export.
C. Enter the two queries in the asset as comma separated values.
D. Configure a second Splunk asset with the second query.

Answer: C

Explanation:
In Splunk SOAR, if a user needs to run two different on_poll searches for a Splunk Cloud instance, the way to achieve this is to configure a second Splunk asset specifically for the second query. Each asset can be configured with its own on_poll search, allowing multiple searches to be run at their respective intervals. This method provides flexibility and ensures that each search can be managed and configured individually.
The correct way to run two different on_poll searches from a Splunk Cloud instance to Splunk SOAR is to configure a second Splunk asset with the second query. Each Splunk asset in Splunk SOAR can only have one query for the on_poll event, which defines which events to pull in and when to pull them in1. Therefore, if you need to run two different queries, you need to create two separate Splunk assets and configure them with the respective queries. The other options are either not possible or not effective for this purpose. For example:
•Installing a second Splunk app in Splunk SOAR will not help, as the app is just a container for the actions and assets, not the source of the data2.
•Configuring the second query in the Splunk App for SOAR Export will not work, as this app is used to forward events from the Splunk platform to Splunk SOAR, not to pull them in3.
•Entering the two queries in the asset as comma separated values will not work, as the asset will only accept one valid query for the on_poll event1.

NEW QUESTION 29
What is the default embedded search engine used by Phantom?

A. Embedded Splunk search engine.
B. Embedded Phantom search engine.
C. Embedded Elastic search engine.
D. Embedded Django search engine.

Answer: B

Explanation:
Splunk SOAR (formerly Phantom) utilizes its own embedded search engine for querying and analyzing data within the platform. This search engine is specifically designed to cater to the unique data structures and use cases of security automation and orchestration, including searching through containers, artifacts, actions, and more. While Splunk SOAR can integrate with external Splunk instances for enhanced data analysis and search capabilities, the platform's primary, out-of-the-box search functionality is provided
by its embedded Phantom search engine.

NEW QUESTION 31
Which of the following can be edited or deleted in the Investigation page?

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

Answer: B

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. Therefore, option B is the correct answer, as it is the only option that can be edited or deleted in the Investigation page. Option A is incorrect, because action results are the outputs of the actions or playbooks that have been run on the event or case, and they cannot be edited or deleted in the Investigation page. Option C is incorrect, because approval records are the logs of the approval requests and responses that have been made for certain actions or playbooks, and they cannot be edited or deleted in the Investigation page. Option D is incorrect, because artifact values are the data that has been collected or generated by the event or case, and they cannot be edited or deleted in the Investigation page.
1: Start with Investigation in Splunk SOAR (Cloud)

NEW QUESTION 36
After enabling multi-tenancy, which of the Mowing is the first configuration step?

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.

NEW QUESTION 37
Which of the following is an advantage of using the Visual Playbook Editor?

A. Eliminates any need to use Python code.
B. The Visual Playbook Editor is the only way to generate user prompts.
C. Supports Python or Javascript.
D. Easier playbook maintenance.

Answer: D

Explanation:
Visual Playbook Editor is a feature of Splunk SOAR that allows you to create, edit, and implement automated playbooks using visual building blocks and execution flow lanes, without having to write code. The Visual Playbook Editor automatically generates the code for you, which you can view and edit in the Code Editor if needed. The Visual Playbook Editor also supports Python and Javascript as scripting languages for custom code blocks. One of the advantages of using the Visual Playbook Editor is that it makes playbook maintenance easier, as you can quickly modify, test, and debug your playbooks using the graphical interface. Therefore, option D is the correct answer, as it states an advantage of using the Visual Playbook Editor. Option A is incorrect, because using the Visual Playbook Editor does not eliminate the need to use Python code, but rather simplifies the process of creating and editing code. You can still add custom Python code to your playbooks using the custom function block or the Code Editor. Option B is incorrect, because the Visual Playbook Editor is not the only way to generate user prompts, but rather one of the ways. You can also generate user prompts using the classic playbook editor or the Code Editor. Option C is incorrect, because supporting Python or Javascript is not an advantage of using the Visual Playbook Editor, but rather a feature of Splunk SOAR in general. You can use Python or Javascript in any of the playbook editors, not just the Visual Playbook Editor. 1: Web search results from search_web(query="Splunk SOAR Automation Developer Visual Playbook Editor")

NEW QUESTION 42
What values can be applied when creating Custom CEF field?

A. Name
B. Name, Data Type
C. Name, Value
D. Name, Data Type, Severity

Answer: B

Explanation:
Custom CEF fields can be created with a name and a data type. The name must be unique and the data type must be one of the following: string, int, float, bool, or list. The severity is not a valid option for custom CEF fields. See Creating custom CEF fields for more details. When creating Custom Common Event Format (CEF) fields in Splunk SOAR (formerly Phantom), the essential values you need to specify are the "Name" of the field and the "Data Type." The "Name" is the identifier for the field, while the "Data Type" specifies the kind of data the field will hold, such as string, integer, IP address, etc. This combination allows for the structured and accurate representation of data within SOAR, ensuring that custom fields are compatible with the platform's data processing and analysis mechanisms.

NEW QUESTION 47
Within the 12A2 design methodology, which of the following most accurately describes the last step?

A. List of the apps used by the playbook.
B. List of the actions of the playbook design.
C. List of the outputs of the playbook design.
D. List of the data needed to run the playbook.

Answer: C

Explanation:
The correct answer is C because the last step of the 12A2 design methodology is to list the outputs of the playbook design. The outputs are the expected results or outcomes of the playbook execution, such as sending an email, creating a ticket, blocking an IP, etc. The outputs should be aligned with the objectives and goals of the playbook. See Splunk SOAR Certified Automation Developer for more details.
The 12A2 design methodology in the context of Splunk SOAR (formerly Phantom) refers to a structured approach to developing playbooks. The last step in this methodology focuses on defining the outputs of the playbook design. This step is crucial as it outlines what the expected results or actions the playbook should achieve upon its completion. These outputs can vary widely, from sending notifications, creating tickets, updating statuses, to generating reports. Defining the outputs is essential for understanding the playbook's impact on the security operation workflows and how it contributes to resolving security incidents or automating tasks.

NEW QUESTION 52
Which of the following queries would return all artifacts that contain a SHA1 file hash?

A. https://<PHANTOM_URL>/rest/artifact?_filter_cef_md5_insull=false
B. https://<PHANTOM_URL>/rest/artifact?_filter_cef_Shal_contains=""
C. https://<PHANTOM_URL>/rest/artifact?_filter_cef_shal_insull=False
D. https://<PHANTOM_URL>/rest/artifact?_filter_shal insull=False

Answer: C

Explanation:
To retrieve all artifacts containing a SHA1 file hash via the Splunk SOAR REST API, the appropriate query would filter for artifacts where the 'cef_sha1' field is not null, indicating that a SHA1 hash is present. The correct REST API call should use the filter parameter _filter_cef_shal isnull=False (assuming 'shal' is a typo and it

should be 'sha1'). This query parameter is used to filter out artifacts that do not have a SHA1 hash, thus returning only those that do.

NEW QUESTION 55
Phantom supports multiple user authentication methods such as LDAP and SAML2. What other user authentication method is supported?

A. SAML3
B. PIV/CAC
C. Biometrics
D. OpenID

Answer: B

Explanation:
Splunk SOAR supports multiple user authentication methods to ensure secure access to the platform. Apart from LDAP (Lightweight Directory Access Protocol) and SAML2 (Security Assertion Markup Language 2.0), SOAR also supports PIV (Personal Identity Verification) and CAC (Common Access Card) as authentication methods. These are particularly used in government and military organizations for secure and authenticated access to systems, providing a high level of security through physical tokens or cards that contain encrypted user credentials.

NEW QUESTION 58
Which of the following roles is appropriate for a Splunk SOAR account that will only be used to execute automated tasks?

A. Non-Human
B. Automation
C. Automation Engineer
D. Service Account

Answer: A

Explanation:
In Splunk SOAR, the 'Non-Human' role is appropriate for accounts that are used exclusively to execute automated tasks. This role is designed for service accounts that interact with the SOAR platform programmatically rather than through a human user. It ensures that the account has the necessary permissions to perform automated actions while restricting access that would be unnecessary or inappropriate for a non-human entity.

NEW QUESTION 61
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 Django queries; use curl to create a container and add artifacts to it; add action blocks.
D. Use SQL queries; use curl to create a container and add artifacts to it; remove temporary lists.

Answer: C

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 65
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.

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.

NEW QUESTION 66
Splunk user account(s) with which roles must be created to configure Phantom with an external Splunk Enterprise instance?

A. superuser, administrator
B. phantomcreat
C. phantomedit
D. phantomsearch, phantomdelete
E. 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.

NEW QUESTION 68
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

SPLK-2003 Practice Exam Features:

* SPLK-2003 Questions and Answers Updated Frequently

* SPLK-2003 Practice Questions Verified by Expert Senior Certified Staff

* SPLK-2003 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* SPLK-2003 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year