SPLK-2003 Q&As

Splunk SOAR Certified Automation Developer

Pass Splunk SPLK-2003 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass4itsure.com/splk-2003.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Splunk Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

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

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.

Correct Answer: D

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

What are indicators?

A. Action result items that determine the flow of execution in a playbook.

B. Action results that may appear in multiple containers.

C. Artifact values that can appear in multiple containers.

D. Artifact values with special security significance.

Correct Answer: D

Indicators within the context of Splunk SOAR refer to artifact values that have special security significance. These are typically derived from the data within artifacts and are identified as having particular importance in the analysis and investigation of security incidents. Indicators might include items such as IP addresses, domain names, file hashes, or other data points that can be used to detect, correlate, and respond to security threats. Recognizing and managing indicators effectively is key to leveraging SOAR for enhanced threat intelligence, incident response, and security operations efficiency.

QUESTION 3

What metrics can be seen from the System Health Display? (select all that apply)

A. Playbook Usage

B. Memory Usage

C. Disk Usage

D. Load Average

Correct Answer: BCD

System Health Display is a dashboard that shows the status and performance of the SOAR processes and components, such as the automation service, the playbook daemon, the DECIDED process, and the REST API. Some of the metrics

that can be seen from the System Health Display are:

?emory Usage: The percentage of memory used by the system and the processes. ?isk Usage: The percentage of disk space used by the system and the processes. ?oad Average: The average number of processes in the run queue or

waiting for disk I/O over a period of time.

Therefore, options B, C, and D are the correct answers, as they are the metrics that can be seen from the System Health Display. Option A is incorrect, because Playbook Usage is not a metric that can be seen from the System Health

Display, but rather a metric that can be seen from the Playbook Usage dashboard, which shows the number of playbooks and actions run over a period of time.

Web search results from search_web(query="Splunk SOAR Automation Developer System Health Display")

The System Health Display in Splunk SOAR provides several metrics to help monitor and manage the health of the system. These typically include:

B: Memory Usage - This metric shows the amount of memory being used by the SOAR platform, which is important for ensuring that the system does not exceed available resources.

C: Disk Usage - This metric indicates the amount of storage space being utilized, which is crucial for maintaining adequate storage resources and for planning capacity.

D: Load Average - This metric provides an indication of the overall load on the system over a period of time, which helps in understanding the system\\'s performance and in identifying potential bottlenecks or issues. Playbook Usage is generally not a metric displayed on the System Health page; instead, it\\'s more related to the usage analytics of playbooks rather than system health metrics.

QUESTION 4

What does a user need to do to have a container with an event from Splunk use context- aware actions designed for notable events?

A. Include the notable event\\'s event_id field and set the artifacts label to aplunk notable event id.

B. Rename the event_id field from the notable event to splunkNotableEventId.

C. Include the event_id field in the search results and add a CEF definition to Phantom for event_id, datatype splunk notable event id.

D. Add a custom field to the container named event_id and set the custom field\\'s data type to splunk notable event id.

Correct Answer: C

For a container in Splunk SOAR to utilize context-aware actions designed for notable events from Splunk, it is crucial to ensure that the notable event\\'s unique identifier (event_id) is included in the search results pulled into SOAR. Moreover, by adding a Common Event Format (CEF) definition for the event_id field within Phantom, and setting its data

type to something that denotes it as a Splunk notable event ID, SOAR can recognize and appropriately handle these identifiers. This setup facilitates the correct mapping and processing of notable event data within SOAR, enabling the execution of context-aware actions that are specifically tailored to the characteristics of Splunk notable events.

QUESTION 5

What are the differences between cases and events?

A. Case: potential threats. Events: identified as a specific kind of problem and need a structured approach.

B. Cases: only include high-level incident artifacts. Events: only include low-level incident artifacts.

C. Cases: contain a collection of containers. Events: contain potential threats.

D. Cases: incidents with a known violation and a plan for correction. Events: occurrences in the system that may require a response.

Correct Answer: D

Cases and events are two types of containers in Phantom. Cases are incidents with a known violation and a plan for correction, such as a malware infection, a phishing attack, or a data breach. Events are occurrences in the system that may require a response, such as an alert, a log entry, or an email. Cases and events can contain both high-level and low-level incident artifacts, such as IP addresses, URLs, files, or users. Cases do not contain a collection of containers, but rather a collection of artifacts, tasks, notes, and comments. Events are not necessarily potential threats, but rather indicators of potential threats. In the context of Splunk Phantom, cases and events serve different purposes. Cases are structured to manage and respond to incidents with known violations and typically have a plan for correction. They often involve a coordinated response and may include various artifacts, notes, tasks, and evidence that need to be managed collectively. Events, on the other hand, are occurrences or alerts within the system that may require a response. They can be considered as individual pieces of information or incidents that may be part of a larger case. Events are the building blocks that can be aggregated into cases if they are related and require a consolidated approach to incident response and investigation.

QUESTION 6

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

A. The end block.

B. The start block.

C. The filter block.

D. The next block.

Correct Answer: A

In Splunk SOAR (formerly Phantom), when a playbook is running and it encounters a filter block, if no data matches the filter conditions specified, the playbook will proceed to the end block. The end block signifies the completion of the playbook\\'s execution path that was contingent on the filter conditions being met. If the filter conditions are not met, and there are no alternative paths specified, the playbook recognizes this as the logical conclusion of that particular execution flow.

QUESTION 7

Which of the following will show all artifacts that have the term results in a filePath CEF value?

A. .../rest/artifact?_filter_cef_filePath_icontain=\\'\\'results\\'\\'

B. ...rest/artifacts/filePath=\\'\\'%results%\\'\\'

C. .../result/artifacts/cef/filePath= \\'%results%\\'\\'

D. .../result/artifact?_query_cef_filepath_icontains=\\'\\'results

Correct Answer: A

The correct answer is A because the _filter parameter is used to filter the results based on a field value, and the icontain operator is used to perform a case- insensitive substring match. The filePath field is part of the Common Event Format (CEF) standard, and the cef_ prefix is used to access CEF fields in the REST API. The answer B is incorrect because it uses the wrong syntax for the REST API. The answer C is incorrect because it uses the wrong endpoint (result instead of artifact) and the wrong syntax for the REST API. The answer D is incorrect because it uses the wrong syntax for the REST API and the wrong spelling for the icontains operator. Reference: Splunk SOAR REST API Guide, page 18. To query and display all artifacts that contain the term "results" in a filePath CEF (Common Event Format) value, using the REST API endpoint with a filter parameter is effective. The filter _filter_cef_filePath_icontain="results" is applied to search within the artifact data for filePath fields that contain the term "results", disregarding case sensitivity. This method allows users to precisely locate and work with artifacts that meet specific criteria, aiding in the investigation and analysis processes within Splunk SOAR.

QUESTION 8

Is it possible to import external Python libraries such as the time module?

A. No.

B. No, but this can be changed by setting the proper permissions.

C. Yes, in the global block.

D. Yes. from a drop-down menu.

Correct Answer: C

In Splunk SOAR, it is possible to import external Python libraries, such as the time module, within the scope of a playbook\\'s global code block. The global block allows users to define custom Python code, including imports of standard Python libraries that are included in the Phantom platform\\'s Python environment. This capability enables the extension of playbooks\\' functionality with additional Python logic, making playbooks more powerful and versatile in their operations.

QUESTION 9

Which of the following are the default ports that must be configured on Splunk to allow connections from Phantom?

A. SplunkWeb (8088), SplunkD (8089), HTTP Collector (8000)

B. SplunkWeb (8089), SplunkD (8088), HTTP Collector (8000)

C. SplunkWeb (8421), SplunkD (8061), HTTP Collector (8798)

D. SplunkWeb (8000), SplunkD (8089), HTTP Collector (8088)

Correct Answer: D

The correct answer is D because the default ports that must be configured on Splunk to allow connections from Phantom are SplunkWeb (8000), SplunkD (8089), and HTTP Collector (8088). SplunkWeb is the port used to access the Splunk web interface. SplunkD is the port used to communicate with the Splunk server. HTTP Collector is the port used to send data to Splunk using the HTTP Event Collector (HEC). These ports must be configured on Splunk and Phantom to enable the integration between the two products. See Splunk SOAR Documentation for more details. To allow connections from Splunk Phantom to Splunk, certain default ports need to be open and properly configured. The default ports include SplunkWeb (8000) for web access, SplunkD (8089) for Splunk\\'s management port, and the HTTP Event Collector (HEC) on port 8088, which is used for ingesting data into Splunk. These ports are essential for the communication between Splunk Phantom and Splunk, facilitating data exchange, search capabilities, and the integration of various functionalities between the two platforms.

QUESTION 10

How can more than one user perform tasks in a workbook?

A. Any user in a role with write access to the case\\'s workbook can be assigned to tasks.

B. Add the required users to the authorized list for the container.

C. Any user with a role that has Perform Task enabled can execute tasks for workbooks.

D. The container owner can assign any authorized user to any task in a workbook.

Correct Answer: C

In Splunk SOAR, tasks within workbooks can be performed by any user whose role has the \\'Perform Task\\' capability enabled. This capability is assigned within the role configuration and allows users with the appropriate permissions to execute tasks. It is not limited to users with write access or the container owner; rather, it is based on the specific permissions granted to the role with which the user is associated.

QUESTION 11

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.

Correct Answer: B

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:

?apping fields from Splunk platform alerts, such as saved searches and data models, to CEF fields.

?ranslating CIM fields from Splunk Enterprise Security (ES) notable events to CEF fields. ?orwarding 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.

Web search results from search_web(query="Splunk SOAR Automation Developer Splunk App for SOAR Export")

QUESTION 12

Which app allows a user to send Splunk Enterprise Security notable events to Phantom?

A. Any of the integrated Splunk/Phantom Apps

B. Splunk App for Phantom Reporting.

C. Splunk App for Phantom.

D. Phantom App for Splunk.

Correct Answer: C

The Splunk App for Phantom is designed to facilitate the integration between Splunk Enterprise Security and Splunk SOAR (Phantom), enabling the seamless forwarding of notable events from Splunk to Phantom. This app allows users to leverage the analytical and data processing capabilities of Splunk ES and utilize Phantom for automated orchestration and response. The app typically includes mechanisms for specifying which notable events to send to Phantom, formatting the data appropriately, and ensuring secure communication between the two platforms. This integration is crucial for organizations looking to combine the strengths of Splunk\\'s SIEM capabilities with Phantom\\'s automation and orchestration features to enhance their security operations.

QUESTION 13

A user selects the New option under Sources on the menu. What will be displayed?

A. A list of new assets.

B. The New Data Ingestion wizard.

C. A list of new data sources.

D. A list of new events.

Correct Answer: B

Selecting the New option under Sources in the Splunk SOAR menu typically initiates the New Data Ingestion wizard. This wizard guides users through the process of configuring new data sources for ingestion into the SOAR platform. It is designed to streamline the setup of various data inputs, such as event logs, threat intelligence feeds, or notifications from other security tools, ensuring that SOAR can receive and process relevant security data efficiently. This feature is crucial for expanding SOAR\\'s monitoring and response capabilities by integrating diverse data sources. Options A, C, and D do not accurately describe what is displayed when the New option under Sources is selected, making option B the correct choice. New Data Ingestion wizard allows you to create a new data source for Splunk SOAR (On- premises) by selecting the type of data, the ingestion method, and the configuration options. The other options are incorrect because they do not match the description of the New option under Sources on the menu. For example, option A refers to a list of new assets, which is not related to data ingestion. Option C refers to a list of new data sources, which is not what the New option does. Option D refers to a list of new events, which is not the same as creating a new data source.

QUESTION 14

Without customizing container status within SOAR, what are the three types of status for a container?

A. New, Open, Resolved

B. Low, Medium, High

C. New, In Progress, Closed

D. Low, Medium, Critical

Correct Answer: C

In Splunk SOAR, without any customization, the three default statuses for a container are New, In Progress, and Closed. These statuses are designed to reflect the lifecycle of an incident or event within the platform, from its initial detection

and logging (New), through the investigation and response stages (In Progress), to its final resolution and closure (Closed). These statuses help in organizing and prioritizing incidents, tracking their progress, and ensuring a structured

workflow. Options A, B, and D do not accurately represent the default container statuses within SOAR, making option C the correct answer. containers are the top-level data structure that SOAR playbook APIs operate on. Containers can

have different statuses that indicate their state and progress in the SOAR workflow. Without customizing container status within SOAR, the three types of status for a container are:

New: The container has been created but not yet assigned or investigated.

In Progress: The container has been assigned and is being investigated or automated.

Closed: The container has been resolved or dismissed and no further action is required. Therefore, option C is the correct answer, as it lists the three types of status for a container without customizing container status within SOAR. Option A

is incorrect, because Resolved is not a type of status for a container without customizing container status within SOAR, but rather a custom status that can be defined by an administrator. Option B is incorrect, because Low, Medium, and High

are not types of status for a container, but rather types of severity that indicate the urgency or impact of a container. Option D is incorrect, for the same reason as option B.

Web search results from search_web(query="Splunk SOAR Automation Developer container status")

QUESTION 15

What values can be applied when creating Custom CEF field?

A. Name

B. Name, Data Type

C. Name, Value

D. Name, Data Type, Severity

Correct Answer: B

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.