PassQueen
a.k.a dumpsqueen.com

# Splunk SOAR Certified Automation Developer Exam

## Splunk SPLK-2003

**Version Demo**

**Total Demo Questions: 14**

**Total Premium Questions: 141**

**Buy Premium PDF**

https://passqueen.com

support@passqueen.com

# Topic Break Down

| Topic | No. of Questions |
|---|---|
| Topic 1, Planning and Installation | 13 |
| Topic 2, Administration | 39 |
| Topic 3, Data Management | 19 |
| Topic 4, Automation | 70 |
| Total | 141 |

QUESTION NO: 1

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: A**

**Explanation:**

Use Django queries; use curl to create a container and add artifacts to it; remove temporary lists. This correctly combines common administrative and integration tasks supported by Splunk Phantom (now Splunk SOAR) REST interfaces. The REST API is designed for programmatic interaction with SOAR objects, so an external client such as `curl` can submit a container representing a case or event and then submit one or more artifacts containing the associated observables and details. This is a standard integration pattern for sending data from security products into SOAR for investigation and automation.

The REST app also exposes endpoints and capabilities used to inspect or work with platform data through Django-oriented queries, which is useful when retrieving object information in the underlying SOAR application context. Temporary lists are platform objects that can be managed programmatically; removing lists that are no longer needed is therefore an appropriate REST-app administration task. Together, these activities reflect API-based data ingestion, querying, and object lifecycle management rather than playbook-canvas authoring. Splunk's REST API documentation describes API access and object operations, including creating and managing containers and artifacts. See the Splunk SOAR REST API documentation and the documentation for REST containers and artifacts.

**QUESTION NO: 2**

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:**

"CIM fields are mapped to CEF fields and a container is created on the SOAR server." is correct because the Splunk App for SOAR Export bridges Splunk search results and Splunk SOAR's event-ingestion model. The app uses field mappings to translate normalized Splunk Common Information Model (CIM) data into Common Event Format (CEF) fields that SOAR can use when creating artifacts. CEF provides a consistent artifact-field structure for values such as source and destination addresses, hashes, file names, URLs, users, and other investigation data. The resulting exported event is represented in SOAR as a container, which serves as the case-like record that groups the associated artifacts and provides the context in which playbooks, analysts, and automation operate. This processing occurs through the integration with the SOAR instance, so the container is created on the SOAR server rather than in Splunk. CIM normalization is central to making search-result fields predictable for mappings, while the SOAR container-and-artifact model is central to organizing data for investigation and response. See Splunk's Common Information Model overview and the Splunk SOAR Container API documentation for the relevant data-model and container concepts.

**QUESTION NO: 3**

Why is it good playbook design to create smaller and more focused playbooks? (select all that apply)

**A.** Reduces amount of playbook data stored in each repo.

**B.** Reduce large complex playbooks which become difficult to maintain.

**C.** Encourages code reuse in a more compartmentalized form.

**D.** To avoid duplication of code across multiple playbooks.

**ANSWER: B C D**

**Explanation:**

“Reduce large complex playbooks which become difficult to maintain,” “Encourages code reuse in a more compartmentalized form,” and “To avoid duplication of code across multiple playbooks” are all sound playbook-design principles for Splunk SOAR. A focused playbook has a clearly bounded responsibility, such as enriching an indicator, creating a ticket, or handling a specific remediation task. This makes its logic easier to understand, test, troubleshoot, and safely update as integrations, APIs, or operational procedures change.

Smaller playbooks can also be composed into broader automation workflows. A reusable child playbook can encapsulate common actions and be invoked wherever that capability is needed, rather than requiring the same action blocks and custom code to be recreated in each workflow. Centralizing shared logic reduces duplicated implementation and helps ensure that a correction or enhancement is consistently applied for every workflow that uses it. This modular approach supports maintainable automation as the SOAR deployment grows and as teams add more playbooks and integrations. Splunk’s playbook documentation describes creating and managing playbooks, while its automation guidance emphasizes structuring automation around reusable playbook logic. See the Splunk SOAR playbooks documentation and Playbook Editor documentation.

## QUESTION NO: 4

What users are included in a new installation of SOAR?

**A.** The admin and automation users are included by default.

**B.** The admin, power, and user users are included by default.

**C.** Only the admin user is included by default.

**D.** No users are included by default.

**ANSWER: A**

**Explanation:**

The admin and automation users are included by default. A new Splunk SOAR installation provides an administrative account for initial configuration and administration, as well as the special automation account used by the platform to execute automated actions and playbooks. The administrative account is the interactive account used to access and configure the SOAR environment. In current Splunk SOAR on-premises documentation, the initial local administrative username is identified as `soar_local_admin`; deployments upgraded from older releases can retain an `admin` account with the Administrator role. Thus, the wording “admin” in this question reflects the administrative default account convention used in the exam context. The automation account is distinct from a human administrator account: it is assigned the Automation role and enables SOAR to run playbooks and app actions with the access needed for orchestration. These two accounts support the separate needs of initial platform management and noninteractive automated execution immediately after installation. Splunk documents the initial local credentials and related installation defaults in its default credentials documentation, and describes user roles, including the Automation role, in the Splunk SOAR roles documentation.

## QUESTION NO: 5

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

**A.** The ability to run more complex reports on SOAR activities.

**B.** The ability to ingest Splunk notable events into SOAR.

**C.** The ability to automate Splunk searches within SOAR.

**D.** The ability to display results as Splunk dashboards within SOAR.

**ANSWER: A**

**Explanation:**

The ability to run more complex reports on SOAR activities is the benefit provided by configuring Splunk SOAR search to use an external Splunk server. This configuration sends SOAR data to a Splunk Enterprise or Splunk Cloud Platform deployment, where the data can be searched and analyzed with the full Splunk Search Processing Language and the broader reporting capabilities of that Splunk deployment. Administrators can use the external platform to investigate SOAR operational activity, correlate SOAR data with other indexed sources, schedule searches, and create reports or visualizations suited to operational and security analysis. In other words, the external-search configuration extends SOAR data analysis beyond the locally available SOAR search experience by making the data available to Splunk's mature search and reporting environment. This is especially useful when teams need to analyze larger volumes of SOAR event, audit, and activity data alongside information already held in their Splunk environment. Splunk documents the external Splunk search configuration and the forwarding of SOAR data for search in its Configure Splunk search guidance. Additional context on using Splunk SOAR data with Splunk search and the Splunk App for SOAR is available in the remote-search service documentation.

**QUESTION NO: 6**

Which of the following are tabs of an asset configuration?

**A.** Asset Name, Asset IP, Asset URL, Asset Nickname

**B.** Tags, Asset Name, Asset Date, Asset Order

**C.** App Name, App Order, App Expiry, App Version

**D.** Asset Info, Asset Settings, Approval Settings, Access Control

**ANSWER: D**

**Explanation:**

**Asset Info, Asset Settings, Approval Settings, Access Control** is correct because these are the functional sections used to configure and govern an asset in Splunk SOAR. Asset Info holds the asset's identifying and descriptive information, providing the core metadata administrators use to recognize the configured integration. Asset Settings contains the app-specific configuration values needed for the asset to communicate with its external service, such as connection details, authentication parameters, and other settings exposed by the app.

Approval Settings is part of asset administration because it defines how approval requirements apply when actions associated with that asset need authorization. This lets administrators apply operational controls to potentially sensitive actions without changing the playbook logic itself. Access Control provides the authorization layer for the asset, enabling administrators to manage which users or roles can view, use, or administer it. Together, these tabs separate identification, technical connectivity, approval governance, and permissions into clear administrative areas. This structure supports secure, maintainable integrations and is consistent with Splunk SOAR's asset-management model. Refer to the official Splunk SOAR on-premises documentation and Splunk's Splunk SOAR documentation portal for current asset administration guidance.

**QUESTION NO: 7**

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

**ANSWER: B C D**

**Explanation:**

The System Health Display provides administrators with operational measurements for the underlying Splunk SOAR deployment, helping them monitor whether the appliance or instance has sufficient system resources for normal platform operation. **Memory Usage** is displayed to show RAM consumption, which is important because SOAR services, automation workloads, and concurrent user activity all depend on available memory. **Disk Usage** is a health metric because SOAR requires usable storage for application data, logs, temporary files, and related operational components. Monitoring disk capacity helps administrators identify potential resource constraints before they disrupt platform services. **Load Average** is also available as an operating-system-level indication of workload demand over time. It helps an administrator assess whether the host is experiencing sustained processing or I/O pressure and supports investigation of general performance issues. Together, these measurements describe core host health rather than the functional activity of an individual playbook. Splunk SOAR documentation describes System Health as the location for monitoring platform and system status, while the administration documentation also covers the resource and deployment considerations that make these host-level measurements operationally important. See Splunk SOAR on-premises monitoring documentation and Splunk SOAR installation and system-requirements documentation.

## QUESTION NO: 8

Which of the following can be done with the System Health Display?

**A.** Create a temporary, edited version of a process and test the results.

**B.** Partially rewind processes, which is useful for debugging.

**C.** View a single column of status for SOAR processes. For metrics, click Details.

**D.** Reset DECIDED to reset playbook environments back to at-start conditions.

**ANSWER: C**

**Explanation:**

The System Health Display provides an at-a-glance operational view of Splunk SOAR processes. It presents the status of the relevant services in a single-column display, allowing an administrator to quickly identify whether each monitored process is healthy or requires attention. Selecting *Details* exposes the associated metrics, which supports investigation of process behavior and resource or performance conditions without leaving the health-monitoring interface. This makes “View a single column of status for SOAR processes. For metrics, click Details.” the correct description of what the System Health Display can do. This display is intended for monitoring the health and status of the SOAR platform’s internal processes and for drilling into the metrics behind their reported state. Administrators can use it as part of routine operational monitoring, particularly when validating that SOAR services are running normally after configuration changes, maintenance, or troubleshooting activity. Splunk’s SOAR documentation describes the administrative interfaces used to monitor platform status and system health; see the Splunk SOAR on-premises system-health monitoring documentation and the Splunk SOAR on-premises administration documentation.

## QUESTION NO: 9

Which of the following cannot be marked as evidence in a container?

**A.** Action result

**B.** Artifact

**C.** Note

**D.** Comment

**ANSWER: D**

**Explanation:**

**Comment** is correct because comments are collaboration entries rather than evidence objects in Splunk SOAR. Analysts use comments to communicate with one another, record informal updates, ask questions, and provide investigation context within a container. Although that discussion may be useful to the team, the platform does not support designating a comment itself as formal evidence.

In Splunk SOAR, evidence is intended to preserve investigation material that directly supports a case or its conclusions. When an analyst marks an eligible item as evidence, it is identified and collected in the container's evidence view, helping reviewers locate the material relied upon during the investigation. This workflow supports clear case documentation and makes it easier to distinguish preserved investigative information from ongoing team conversation. A comment remains available in the container's activity and discussion history, but it is not an evidence-markable item.

For details on managing containers and the evidence workflow, see the Splunk SOAR documentation on managing evidence and the Splunk SOAR documentation on containers.