Up-to-date Questions and Answers from authentic resources to improve knowledge and pass the exam at very first attempt. ----- Guaranteed.

KILL EXAMS

SPLK-2003 MCQs
SPLK-2003 TestPrep
SPLK-2003 Study Guide
SPLK-2003 Practice Test
SPLK-2003 Exam Questions

PASS

Splunk

SPLK-2003

Splunk SOAR Certified Automation Developer

Question: 145

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

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

Question: 146

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: D

Question: 147

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 âbackup-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

Question: 148

An active playbook can be configured to operate on all containers that share which attribute?

A. Artifact
B. Label
C. Tag
D. Severity

Answer: B

Question: 149

Which of the following applies to filter blocks?

A. Can select which blocks have access to container data.
B. Can select assets by tenant, approver, or app.

C. Can be used to select data for use by other blocks.
D. Can select containers by seventy or status.

Answer: A

Question: 150

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: A

Question: 151

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?

A. Use the py-postgresq1 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: A

Question: 152

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

Question: 153

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)

Answer: D

Question: 154

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

A. New, In Progress, Closed
B. Low, Medium, High
C. Mew, Open, Resolved
D. Low, Medium, Critical

Answer: A

Question: 155

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

A. superuser, administrator
B. phantomcreate. phantomedit
C. phantomsearch, phantomdelete
D. admin,user

Answer: A

Question: 156

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: A

Question: 157

During a second test of a playbook, a user receives an error that states: 'an empty parameters list was passed to phantom.act()." What does this indicate?

A. The container has artifacts not parameters.
B. The playbook is using an incorrect container.
C. The playbook debugger's scope is set to new.
D. The playbook debugger's scope is set to all.

Answer: A

Question: 158

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.

Answer: D

Question: 159

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: B

Question: 160

When configuring a Splunk asset for Phantom to connect to a SplunkC loud instance, the user discovers that they need to be able to run two different on_poll searches.

How is this possible

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

Answer: A

Question: 161

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

A. 0
B. Default
C. 1
D. *

Answer: D

Question: 162

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.

Answer: C

Question: 163

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.

Answer: A

Question: 164

Some of the playbooks on the Phantom server should only be executed by members of the admin role.

How can this rule be applied?

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: A

KILLEXAMS.COM

Killexams.com is a leading online platform specializing in high-quality certification exam preparation. Offering a robust suite of tools, including MCQs, practice tests, and advanced test engines, Killexams.com empowers candidates to excel in their certification exams. Discover the key features that make Killexams.com the go-to choice for exam success.

Exam Questions:

Killexams.com provides exam questions that are experienced in test centers. These questions are updated regularly to ensure they are up-to-date and relevant to the latest exam syllabus. By studying these questions, candidates can familiarize themselves with the content and format of the real exam.

Exam MCQs:

Killexams.com offers exam MCQs in PDF format. These questions contain a comprehensive collection of questions and answers that cover the exam topics. By using these MCQs, candidate can enhance their knowledge and improve their chances of success in the certification exam.

Practice Test:

Killexams.com provides practice test through their desktop test engine and online test engine. These practice tests simulate the real exam environment and help candidates assess their readiness for the actual exam. The practice test cover a wide range of questions and enable candidates to identify their strengths and weaknesses.

Guaranteed Success:

Killexams.com offers a success guarantee with the exam MCQs. Killexams claim that by using this materials, candidates will pass their exams on the first attempt or they will get refund for the purchase price. This guarantee provides assurance and confidence to individuals preparing for certification exam.

Updated Contents:

Killexams.com regularly updates its question bank of MCQs to ensure that they are current and reflect the latest changes in the exam syllabus. This helps candidates stay up-to-date with the exam content and increases their chances of success.