

IT 认证电子书



质 量 更 高 服 务 更 好

半年免费升级服务

<http://www.itrenzheng.com>

Exam : SPLK-2003

**Title : Splunk SOAR Certified
Automation Developer
Exam**

Version : DEMO

1. 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

2. 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

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 `sudo 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

4. 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

5. 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 severity or status.

Answer: A