



Vendor: Splunk

Exam Code: SPLK-2003

Exam Name: Splunk SOAR Certified Automation Developer

Version: DEMO

QUESTION 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: C

QUESTION 2

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 3

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

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

Answer: D

QUESTION 4

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 5

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 6

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 all restricted playbooks that Tilters for runRole - "Admin".
- B. Add a tag with restricted access to the restricted playbooks.
- C. Make sure the Execute Playbook capability is removed from all roles except admin.
- D. Place restricted playbooks in a second source repository that has restricted access.

Answer: A

QUESTION 7

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: D

QUESTION 8

What is enabled if the Logging option for a playbook's settings is enabled?

- A. More detailed logging information is available in the Investigation page.
- B. All modifications to the playbook will be written to the audit log.
- C. More detailed information is available in the debug window.
- D. The playbook will write detailed execution information into the spawn.log.

Answer: D

QUESTION 9

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.

Answer: C

Thank You for Trying Our Product

Lead2pass Certification Exam Features:

- ★ More than **99,900** Satisfied Customers Worldwide.
- ★ Average **99.9%** Success Rate.
- ★ **Free Update** to match latest and real exam scenarios.
- ★ **Instant Download** Access! No Setup required.
- ★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.
- ★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.
- ★ **100%** Guaranteed Success or **100%** Money Back Guarantee.
- ★ **Fast**, helpful support **24x7**.



View list of all certification exams: <http://www.lead2pass.com/all-products.html>



Microsoft



ORACLE



CITRIX



JUNIPER
NETWORKS



EMC²
where information lives

10% Discount Coupon Code: ASTR14