



Splunk

SPLK-2003

Splunk SOAR Certified Automation Developer Exam

Questions & Answers PDF

For More Information:

<https://www.certswarrior.com/>

Features:

- 90 Days Free Updates
- 30 Days Money Back Guarantee
- Instant Download Once Purchased
- 24/7 Online Chat Support
- Its Latest Version

Latest Version: 6.0

Question: 1

What is the default embedded search engine used by Phantom?

- A. Embedded Splunk search engine.
- B. Embedded Phantom search engine.
- C. Embedded Elastic search engine.
- D. Embedded Django search engine.

Answer: C

Question: 2

A filter block with only one condition configured which states: `artifact.*.cef.sourceAddress !=` , would permit which of the following data to pass forward to the next block?

- A. Null IP addresses
- B. Non-null IP addresses
- C. Non-null destinationAddresses
- D. Null values

Answer: D

Question: 3

A user wants to get the playbook results for a single artifact. Which steps will accomplish the?

- A. Use the contextual menu from the artifact and select run playbook.
- B. Use the run playbook dialog and set the scope to the artifact.
- C. Create a new container including Just the artifact in question.
- D. Use the contextual menu from the artifact and select the actions.

Answer: C

Question: 4

What is the main purpose of using a customized workbook?

-
- A. Workbooks automatically implement a customized processing of events using Python code.
 - B. Workbooks guide user activity and coordination during event analysis and case operations.
 - C. Workbooks apply service level agreements (SLAs) to containers and monitor completion status on the ROI dashboard.
 - D. Workbooks may not be customized; only default workbooks are permitted within Phantom.

Answer: D

Question: 5

Which of the following is a step when configuring event forwarding from Splunk to Phantom?

- A. Map CIM to CEF fields.
- B. Create a Splunk alert that uses the event_forward.py script to send events to Phantom.
- C. Map CEF to CIM fields.
- D. Create a saved search that generates the JSON for the new container on Phantom.

Answer: C



CERTSWARRIOR

FULL PRODUCT INCLUDES:

Money Back Guarantee



Instant Download after Purchase



90 Days Free Updates



PDF Format Digital Download



24/7 Live Chat Support



Latest Syllabus Updates



For More Information – Visit link below:

<http://www.certswarrior.com>

Discount Coupon Code:

CERTSWARRIOR10

We Accept

PayPal