DUMPSARENA

Splunk SOAR Certified Automation Developer Exam

Splunk SPLK-2003

Version Demo

Total Demo Questions: 10

Total Premium Questions: 58

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

QUESTION NO: 1

Which of the following can the format block be used for?

A. To generate arrays for input into other functions.

B. To generate HTML or CSS content for output in email messages, user prompts, or comments.

C. To generate string parameters for automated action blocks.

D. To create text strings that merge state text with dynamic values for input or output.

ANSWER: D

QUESTION NO: 2

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 NO: 3

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 NO: 4

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 NO: 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

QUESTION NO: 6

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 NO: 7

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 NO: 8

When analyzing events a working on a case, significant items can be marked as evidence. Where can ail of a case's evidence items be viewed together?

A. Workbook page Evidence tab.

B. Evidence report.

C. Investigation page Evidence tab.

D. At the bottom of the Investigation page widget panel.

ANSWER: C

QUESTION NO: 9

When working with complex datapaths, which operator is used to access a sub-element inside another element?

A. !(pipe)

B. *(asterisk)

C. :(colon)

D. .(dot)

ANSWER: A

QUESTION NO: 10

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