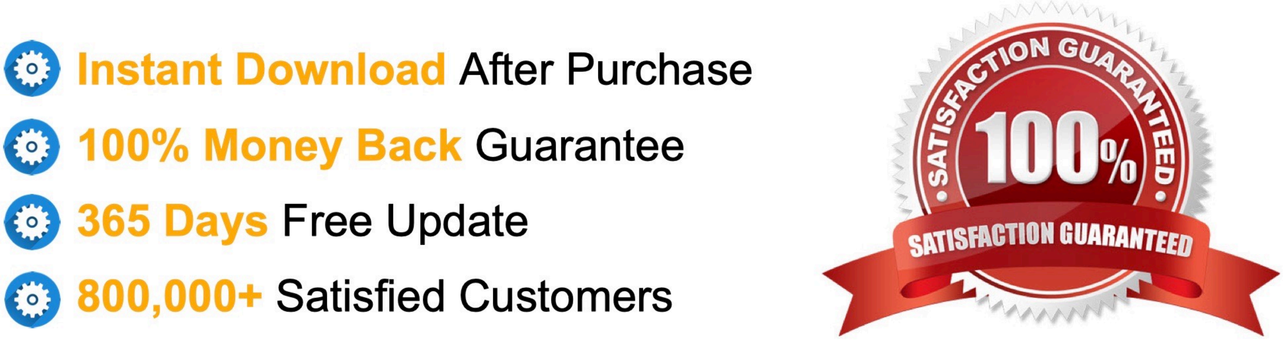
SPLK-3001 Q&As

Splunk Enterprise Security Certified Admin


Instant Download After Purchase
100% Money Back Guarantee
365 Days Free Update
800,000+ Satisfied Customers
SATISFACTION GUARANTEED
100%
SATISFACTION GUARANTEED

QUESTION 1

What is the maximum recommended volume of indexing per day, per indexer, for a non-cloud (on-prem) ES deployment?

A. 50 GB

B. 100 GB

C. 300 GB

D. 500 MB

Correct Answer: B

Reference: https://docs.splunk.com/Documentation/ITSI/4.4.2/Install/Plan

QUESTION 2

Which of the following are examples of sources for events in the endpoint security domain dashboards?

A. REST API invocations.

B. Investigation final results status.

C. Workstations, notebooks, and point-of-sale systems.

D. Lifecycle auditing of incidents, from assignment to resolution.

Correct Answer: C

Reference: https://docs.splunk.com/Documentation/ES/6.1.0/User/EndpointProtectionDomaindashboards

QUESTION 3

Adaptive response action history is stored in which index?

A. cim_modactions

B. modular_history

C. cim_adaptiveactions

D. modular_action_history

Correct Answer: A

Reference: https://docs.splunk.com/Documentation/ES/6.1.0/Install/Indexes

QUESTION 4

When ES content is exported, an app with a .spl extension is automatically created. What is the best practice when exporting and importing updates to ES content?

A. Use new app names each time content is exported.

B. Do not use the .spl extension when naming an export.

C. Always include existing and new content for each export.

D. Either use new app names or always include both existing and new content.

Correct Answer: D

Either use new app names each time (which could be difficult to manage) or make sure you always include all content (old and new) each time you export.

QUESTION 5

Both "Recommended Actions" and "Adaptive Response Actions" use adaptive response.

How do they differ?

A. Recommended Actions show a textual description to an analyst, Adaptive Response Actions show them encoded.

B. Recommended Actions show a list of Adaptive Responses to an analyst, Adaptive Response Actions run them automatically.

C. Recommended Actions show a list of Adaptive Responses that have already been run, Adaptive Response Actions run them automatically.

D. Recommended Actions show a list of Adaptive Resposes to an analyst, Adaptive Response Actions run manually with analyst intervention.

Correct Answer: D

Reference: https://docs.splunk.com/Documentation/ES/latest/Admin/Configureadaptiveresponse

SPLK-3001 VCE Dumps SPLK-3001 Study Guide SPLK-3001 Braindumps