SPLK-3001 Q&As

Splunk Enterprise Security Certified Admin

Pass Splunk SPLK-3001 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.geekcert.com/splk-3001.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Splunk Official Exam Center

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

QUESTION 1

What is an example of an ES asset?

A. MAC address

B. User name

C. Server

D. People

Correct Answer: A

QUESTION 2

What feature of Enterprise Security downloads threat intelligence data from a web server?

A. Threat Service Manager

B. Threat Download Manager

C. Threat Intelligence Parser

D. Therat Intelligence Enforcement

Correct Answer: B

"The Threat Intelligence Framework provides a modular input (Threat Intelligence Downloads) that handles the majority of configurations typically needed for downloading intelligence files and data. To access this modular input, you simply need to create a stanza in your Inputs.conf file called "threatlist"."

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

Which indexes are searched by default for CIM data models?

A. notable and default

B. summary and notable

C. _internal and summary

D. All indexes

Correct Answer: D

Reference: https://answers.splunk.com/answers/600354/indexes-searched-by-cim-data-models.html

QUESTION 5

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.