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

Which of the following lookup types in Enterprise Security contains information about known hostile IP addresses?

A. Security domains.

B. Threat intel.

C. Assets.

D. Domains.

Correct Answer: B

Reference: https://docs.splunk.com/Documentation/ES/6.4.1/Admin/Manageinternallookups

QUESTION 2

Which of the following steps will make the Threat Activity dashboard the default landing page in ES?

A. From the Edit Navigation page, drag and drop the Threat Activity view to the top of the page.

B. From the Preferences menu for the user, select Enterprise Security as the default application.

C. From the Edit Navigation page, click the \\'Set this as the default view" checkmark for Threat Activity.

D. Edit the Threat Activity view settings and checkmark the Default View option.

Correct Answer: C

QUESTION 3

Where is the Add-On Builder available from?

A. GitHub

B. SplunkBase

C. www.splunk.com

D. The ES installation package

Correct Answer: B

Reference: https://docs.splunk.com/Documentation/AddonBuilder/3.0.1/UserGuide/Installation

QUESTION 4

The Add-On Builder creates Splunk Apps that start with what?

A. DA

B. SA

C. TA

D. App-

Correct Answer: C

Reference: https://dev.splunk.com/enterprise/docs/developapps/enterprisesecurity/abouttheessolution/

QUESTION 5

Which component normalizes events?

A. SA-CIM.

B. SA-Notable.

C. ES application.

D. Technology add-on.

Correct Answer: A

Reference: https://docs.splunk.com/Documentation/CIM/4.15.0/User/UsetheCIMtonormalizedataatsearchtime