



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.pass4itsure.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 are the steps to add a new column to the Notable Event table in the Incident Review dashboard?

- A. Configure -> Incident Management -> Notable Event Statuses
- B. Configure -> Content Management -> Type: Correlation Search
- C. Configure -> Incident Management -> Incident Review Settings -> Event Management
- D. Configure -> Incident Management -> Incident Review Settings -> Table Attributes

Correct Answer: D

Reference: <https://docs.splunk.com/Documentation/ES/6.1.0/Admin/Customizenotables>

QUESTION 2

The option to create a Short ID for a notable event is located where?

- A. The Additional Fields.
- B. The Event Details.
- C. The Contributing Events.
- D. The Description.

Correct Answer: B

<https://docs.splunk.com/Documentation/ES/6.4.1/User/Takeactiononanotableevent>

QUESTION 3

When creating custom correlation searches, what format is used to embed field values in the title, description, and drill-down fields of a notable event?

- A. \$fieldname\$
- B. "fieldname"
- C. %fieldname%
- D. _fieldname_

Correct Answer: A

Reference: <https://docs.splunk.com/Documentation/ITSI/4.4.2/Configure/Createcorrelationsearch>



QUESTION 4

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 5

Which of the following features can the Add-on Builder configure in a new add-on?

- A. Expire data.
- B. Normalize data.
- C. Summarize data.
- D. Translate data.

Correct Answer: B

Reference: <https://docs.splunk.com/Documentation/AddonBuilder/3.0.1/UserGuide/Overview>

[Latest SPLK-3001 Dumps](#)

[SPLK-3001 PDF Dumps](#)

[SPLK-3001 Braindumps](#)