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

To observe what network services are in use in a network\\'s activity overall, which of the following dashboards in Enterprise Security will contain the most relevant data?

A. Intrusion Center

B. Protocol Analysis

C. User Intelligence

D. Threat Intelligence

Correct Answer: B

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

QUESTION 2

Which of the following is part of tuning correlation searches for a new ES installation?

A. Configuring correlation notable event index.

B. Configuring correlation permissions.

C. Configuring correlation adaptive responses.

D. Configuring correlation result storage.

Correct Answer: A

QUESTION 3

An administrator is asked to configure an "Nslookup" adaptive response action, so that it appears as a selectable option in the notable event\\'s action menu when an analyst is working in the Incident Review dashboard. What steps would the administrator take to configure this option?

A. Configure -> Content Management -> Type: Correlation Search -> Notable -> Nslookup

B. Configure -> Type: Correlation Search -> Notable -> Recommended Actions -> Nslookup

C. Configure -> Content Management -> Type: Correlation Search -> Notable -> Next Steps -> Nslookup

D. Configure -> Content Management -> Type: Correlation Search -> Notable -> Recommended Actions > Nslookup

Correct Answer: D

QUESTION 4

Enterprise Security\\'s dashboards primarily pull data from what type of knowledge object?

A. Tstats

B. KV Store

C. Data models

D. Dynamic lookups

Correct Answer: C

Reference: https://docs.splunk.com/Splexicon:Knowledgeobject

QUESTION 5

What should be used to map a non-standard field name to a CIM field name?

A. Field alias.

B. Search time extraction.

C. Tag.

D. Eventtype.

Correct Answer: A