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.pass2lead.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 does the risk framework add to an object (user, server or other type) to indicate increased risk?

A. An urgency.

B. A risk profile.

C. An aggregation.

D. A numeric score.

Correct Answer: D

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

QUESTION 2

Which lookup table does the Default Account Activity Detected correlation search use to flag known default accounts?

A. Administrative Identities

B. Local User Intel

C. Identities

D. Privileged Accounts

Correct Answer: C

QUESTION 3

Analysts have requested the ability to capture and analyze network traffic data. The administrator has researched the documentation and, based on this research, has decided to integrate the Splunk App for Stream with ES.

Which dashboards will now be supported so analysts can view and analyze network Stream data?

A. Endpoint dashboards.

B. User Intelligence dashboards.

C. Protocol Intelligence dashboards.

D. Web Intelligence dashboards.

Correct Answer: C

QUESTION 4

Which of the following actions can improve overall search performance?

A. Disable indexed real-time search.

B. Increase priority of all correlation searches.

C. Reduce the frequency (schedule) of lower-priority correlation searches.

D. Add notable event suppressions for correlation searches with high numbers of false positives.

Correct Answer: A

QUESTION 5

If a username does not match the `identity\\' column in the identities list, which column is checked next?

A. Email.

B. Nickname

C. IP address.

D. Combination of Last Name, First Name.

Correct Answer: A