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.leads4pass.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

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 2

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 3

How does ES know local customer domain names so it can detect internal vs. external emails?

A. Web and email domain names are set in General -> General Configuration.

B. ES uses the User Activity index and applies machine learning to determine internal and external domains.

C. The Corporate Web and Email Domain Lookups are edited during initial configuration.

D. ES extracts local email and web domains automatically from SMTP and HTTP logs.

Correct Answer: C

QUESTION 4

What is an example of an ES asset?

A. MAC address

B. User name

C. Server

D. People

Correct Answer: A

QUESTION 5

Following the installation of ES, an admin configured users with the ess_user role the ability to close notable events.

How would the admin restrict these users from being able to change the status of Resolved notable events to Closed?

A. In Enterprise Security, give the ess_user role the Own Notable Events permission.

B. From the Status Configuration window select the Closed status. Remove ess_user from the status transitions for the Resolved status.

C. From the Status Configuration window select the Resolved status. Remove ess_user from the status transitions for the Closed status.

D. From Splunk Access Controls, select the ess_user role and remove the edit_notable_events capability.

Correct Answer: C