SPLK-3001$^{\text{Q\&As}}$

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

QUESTION 1

Which of the following is an adaptive action that is configured by default for ES?

A. Create notable event

B. Create new correlation search

C. Create investigation

D. Create new asset

Correct Answer: A

QUESTION 2

What feature of Enterprise Security downloads threat intelligence data from a web server?

A. Threat Service Manager

B. Threat Download Manager

C. Threat Intelligence Parser

D. Therat Intelligence Enforcement

Correct Answer: B

"The Threat Intelligence Framework provides a modular input (Threat Intelligence Downloads) that handles the majority of configurations typically needed for downloading intelligence files and data. To access this modular input, you simply need to create a stanza in your Inputs.conf file called "threatlist"."

QUESTION 3

Which of the following is a Web Intelligence dashboard?

A. Network Center

B. Endpoint Center

C. HTTP Category Analysis

D. stream :http Protocol dashboard

Correct Answer: C

QUESTION 4

Following the Installation of ES, an admin configured Leers with the ?s_uso r 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. From the Status Configuration window select the Resolved status. Remove ess_user from the status transitions for the closed status.

B. From the Status Configuration windows select the closed status. Remove ess_use r from the status transitions for the Resolved status.

C. In Enterprise Security, give the ess_user role the own Notable Events permission.

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

Correct Answer: B

QUESTION 5

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