ExamsNest

Your Ultimate Exam Preparation Hub

Vendor: Splunk

Code: SPLK-3001

Exam: Splunk Enterprise Security Certified Admin

https://www.examsnest.com/exam/splk-3001/

QUESTIONS & ANSWERS

DEMO VERSION

Version: 7.0

Question: 1

The Add-On Builder creates Splunk Apps that start with what?

A. DA-
B. SA-
C. TA-
D. App-

Answer: C

Explanation:

Reference:
https://dev.splunk.com/enterprise/docs/developapps/enterprisesecurity/abouttheessolution/

Question: 2

Which of the following are examples of sources for events in the endpoint security domain dashboards?

A. REST API invocations.
B. Investigation final results status.
C. Workstations, notebooks, and point-of-sale systems.
D. Lifecycle auditing of incidents, from assignment to resolution.

Answer: C

Explanation:

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

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_

Answer: A

Explanation:

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

Question: 4

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

Answer: B

Explanation:

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

Question: 5

The Remote Access panel within the User Activity dashboard is not populating with the most recent hour of dat
a. What data model should be checked for potential errors such as skipped searches?

A. Web
B. Risk
C. Performance
D. Authentication

Answer: D

Explanation:

Reference: https://answers.splunk.com/answers/565482/how-to-resolve-skipped-scheduled-searches

ExamsNest

Your Ultimate Exam Preparation Hub

Thank You for trying the PDF Demo

Vendor: Splunk

Code: SPLK-3001

Exam: Splunk Enterprise Security Certified Admin

https://www.examsnest.com/exam/splk-3001/

Use Coupon "**SAVE15**" for extra 15% discount on the purchase of Practice Test Software. Test your Exam preparation with actual exam questions.

Start Your Preparation