DUMPSARENA

Splunk Enterprise Security Certified Admin Exam

Splunk SPLK-3001

Version Demo

Total Demo Questions: 7

Total Premium Questions: 97

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

QUESTION NO: 1

Which of the following ES features would a security analyst use while investigating a network anomaly notable?

A. Correlation editor.

B. Key indicator search.

C. Threat download dashboard.

D. Protocol intelligence dashboard.

ANSWER: D

QUESTION NO: 2

Which of the following are data models used by ES? (Choose all that apply)

A. Web

B. Anomalies

C. Authentication

D. Network Traffic

ANSWER: A C D

QUESTION NO: 3

Which two fields combine to create the Urgency of a notable event?

A. Priority and Severity.

B. Priority and Criticality.

C. Criticality and Severity.

D. Precedence and Time.

ANSWER: A

QUESTION NO: 4

Which column in the Asset or Identity list is combined with event security to make a notable event's urgency?

A. VIP

B. Priority

C. Importance

D. Criticality

ANSWER: B

QUESTION NO: 5

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 NO: 6

Which of the following threat intelligence types can ES download? (Choose all that apply)

A. Text

B. STIX/TAXII

C. VulnScanSPL

D. SplunkEnterpriseThreatGenerator

ANSWER: A B

QUESTION NO: 7

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

ANSWER: B