Free Questions for SPLK-3001 by actualtestdumps

Shared by Cervantes on 06-06-2022

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

After data is ingested, which data management step is essential to ensure raw data can be accelerated by a Data Model and used by ES?

Options:

A- Applying Tags.

B- Normalization to Customer Standard.

C- Normalization to the Splunk Common Information Model.

D- Extracting Fields.

Answer:

C

Question 2

Question Type: MultipleChoice

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

Options:

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.

Answer:

C

Question 3

Question Type: **MultipleChoice**

What are adaptive responses triggered by?

Options:

A- By correlation searches and users on the incident review dashboard.

B- By correlation searches and custom tech add-ons.

C- By correlation searches and users on the threat analysis dashboard.

D- By custom tech add-ons and users on the risk analysis dashboard.

Answer:

D

Question 4

Question Type: MultipleChoice

What is the main purpose of the Dashboard Requirements Matrix document?

Options:

A- Identifies on which data model(s) each dashboard depends.

B- Provides instructions for customizing each dashboard for local data models.

C- Identifies the searches used by the dashboards.

D- Identifies which data model(s) depend on each dashboard.

Answer:

D

Question 5

Question Type: **MultipleChoice**

What does the summariesonly=true option do for a correlation search?

Options:

A- Searches only accelerated data.

B- Forwards summary indexes to the indexing tier.

C- Uses a default summary time range.

D- Searches summary indexes only.

Answer:

A

Question 6

Question Type: MultipleChoice

Which columns in the Assets lookup are used to identify an asset in an event?

Options:

A- src, dvc, dest

B- cidr, port, netbios, saml

C- ip, mac, dns, nt_host

D- host, hostname, url, address

Answer:

C

Question 7

Question Type: MultipleChoice

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

Options:

A- Priority and Severity.

B- Priority and Criticality.

C- Criticality and Severity.

D- Precedence and Time.

Answer:

A

Question 8

Question Type: MultipleChoice

Where is detailed information about identities stored?

Options:

A- The Identity Investigator index.

B- The Access Anomalies collection.

C- The User Activity index.

D- The Identity Lookup CSV file.

Answer:

C

Question 9

Question Type: MultipleChoice

Which of the following lookup types in Enterprise Security contains information about known hostile IP addresses?

Options:

A- Security domains.

B- Threat intel.

C- Assets.

D- Domains.

Answer:

B

Question 10

Question Type: MultipleChoice

What should be used to map a non-standard field name to a CIM field name?

Options:

A- Field alias.

B- Search time extraction.

C- Tag.

D- Eventtype.

Answer:

A

20%
DISCOUNT