ExamsIndex
Practice Materials & Tests

DEMO VERSION

Splunk

SPLK-3001 Exam

Splunk Enterprise Security Certified Admin Exam

Exam Latest Version: 9.0

Question 1. (Multi Select)

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

A: Web
B: Anomalies
C: Authentication
D: Network Traffic

Correct Answer: A, C, D

Question 2. (Single Select)

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

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

Correct Answer: C

Question 3. (Single Select)

In order to include an eventtype in a data model node, what is the next step after extracting the correct fields?

A: Save the settings.

B: Apply the correct tags.
C: Run the correct search.
D: Visit the CIM dashboard.

Correct Answer: C

Question 4. (Single Select)

What role should be assigned to a security team member who will be taking ownership of notable events in the incident review dashboard?

A: ess_user
B: ess_admin
C: ess_analyst
D: ess_reviewer

Correct Answer: B

Question 5. (Single Select)

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

Correct Answer: B

ExamsIndex

Demo PDF Complete

Your SPLK-3001 Demo (5 Questions)

Get the Complete Version

Full Questions with Detailed Explanations

Interactive Web-Based Exams Available

To get 30% off, use Coupon Code: NEWYEAR30

https://examsindex.com/exam/splk-3001