EndExam

QUESTION & ANSWER

Accurate study guides, High passing rate!

We offer free update service for one year!

http://www.endexam.com

Exam : SPLK-3001

Title : Splunk Enterprise Security Certified Admin

Version : DEMO

1.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
Explanation:
Reference: https://dev.splunk.com/enterprise/docs/developapps/enterprisesecurity/datamodelsusedbyes/

2.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.
Answer: C
Explanation:
Reference: https://docs.splunk.com/Documentation/CIM/4.15.0/User/UsetheCIMtonormalizeOSSECdata

3.A site has a single existing search head which hosts a mix of both CIM and non-CIM compliant applications. All of the applications are mission-critical. The customer wants to carefully control cost, but wants good ES performance.
What is the best practice for installing ES?
A. Install ES on the existing search head.
B. Add a new search head and install ES on it.
C. Increase the number of CPUs and amount of memory on the search head, then install ES.
D. Delete the non-CIM-compliant apps from the search head, then install ES.
Answer: B
Explanation:
Reference: https://www.splunk.com/pdfs/technical-briefs/splunk-validated-architectures.pdf

4.What are adaptive responses triggered by?
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

5.When investigating, what is the best way to store a newly-found IOC?
A. Paste it into Notepad.
B. Click the “Add IOC” button.
C. Click the “Add Artifact” button.
D. Add it in a text note to the investigation.
Answer: C