Vendor: Splunk

Exam Code:SPLK-3001

Exam Name: Splunk Enterprise Security Certified Admin

Version: Demo

QUESTION 1

A customer site is experiencing poor performance. The UI response time is high and searches take a very long time to run. Some operations time out and there are errors in the scheduler logs, indicating too many concurrent searches are being started. 6 total correlation searches are scheduled and they have already been tuned to weed out false positives.

Which of the following options is most likely to help performance?

A. Change the search heads to do local indexing of summary searches.

B. Add heavy forwarders between the universal forwarders and indexers so inputs can be parsed before indexing.

C. Increase memory and CPUs on the search head(s) and add additional indexers.

D. If indexed realtime search is enabled, disable it for the notable index.

Correct Answer: C

QUESTION 2

Glass tables can display static images and text, the results of ad-hoc searches, and which of the following objects?

A. Lookup searches.

B. Summarized data.

C. Security metrics.

D. Metrics store searches.

Correct Answer: C

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

---

QUESTION 3

Analysts have requested the ability to capture and analyze network traffic data. The administrator has researched the documentation and, based on this research, has decided to integrate the Splunk App for Stream with ES.

Which dashboards will now be supported so analysts can view and analyze network Stream data?

A. Endpoint dashboards.

B. User Intelligence dashboards.

C. Protocol Intelligence dashboards.

D. Web Intelligence dashboards.

Correct Answer: C

QUESTION 4

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.

Correct Answer: D

Reference: https://www.splunk.com/en_us/products/premium-solutions/splunk-enterprise-security/ features.html

---

QUESTION 5

"10.22.63.159", "websvr4", and "00:26:08:18: CF:1D" would be matched against what in ES?

A. A user.

B. A device.

C. An asset.

D. An identity.

Correct Answer: B

QUESTION 6

What tools does the Risk Analysis dashboard provide?

A. High risk threats.

B. Notable event domains displayed by risk score.

C. A display of the highest risk assets and identities.

D. Key indicators showing the highest probability correlation searches in the environment.

Correct Answer: C

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

---

QUESTION 7

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.

Correct Answer: C

QUESTION 8

What do threat gen searches produce?

A. Threat Intel in KV Store collections.

B. Threat correlation searches.

C. Threat notables in the notable index.

D. Events in the threat_activity index.

Correct Answer: D

https://docs.splunk.com/Documentation/ES/6.4.1/Admin/Createthreatmatchspecs

---

QUESTION 9

When installing Enterprise Security, what should be done after installing the add-ons necessary for normalizing data?

A. Configure the add-ons according to their README or documentation.

B. Disable the add-ons until they are ready to be used, then enable the add-ons.

C. Nothing, there are no additional steps for add-ons.

D. Configure the add-ons via the Content Management dashboard.

Correct Answer: A

QUESTION 10

How is it possible to specify an alternate location for accelerated storage?

A. Configure storage optimization settings for the index.

B. Update the Home Path setting in indexes, conf

C. Use the tstatsHomePath setting in props, conf

D. Use the tstatsHomePath Setting in indexes, conf

Correct Answer: C

QUESTION 11

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

A. DA

B. SA

C. TA

D. App-

Correct Answer: C

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

QUESTION 12

Adaptive response action history is stored in which index?

A. cim_modactions

B. modular_history

C. cim_adaptiveactions

D. modular_action_history

Correct Answer: A

Reference: https://docs.splunk.com/Documentation/ES/6.1.0/Install/Indexes