

SPLK-3001 Dumps

Splunk Enterprise Security Certified Admin Exam

<https://www.certleader.com/SPLK-3001-dumps.html>



NEW QUESTION 1

Which setting is used in indexes.conf to specify alternate locations for accelerated storage?

- A. thawedPath
- B. tstatsHomePath
- C. summaryHomePath
- D. warmToColdScript

Answer: B

Explanation:

Reference: <https://docs.splunk.com/Documentation/Splunk/8.0.2/Knowledge/Acceleratedatamodels>

NEW QUESTION 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: B

Explanation:

Reference: <https://dev.splunk.com/enterprise/docs/developapps/enterprisesecurity/datamodelsusedbyes/>

NEW QUESTION 3

At what point in the ES installation process should Splunk_TA_ForIndexers.spl be deployed to the indexers?

- A. When adding apps to the deployment server.
- B. Splunk_TA_ForIndexers.spl is installed first.
- C. After installing ES on the search head(s) and running the distributed configuration management tool.
- D. Splunk_TA_ForIndexers.spl is only installed on indexer cluster sites using the cluster master and the splunk apply cluster-bundle command.

Answer: B

Explanation:

Reference: <https://docs.splunk.com/Documentation/ES/6.1.0/Install/InstallTechnologyAdd-ons>

NEW QUESTION 4

What does the Security Posture dashboard display?

- A. Active investigations and their status.
- B. A high-level overview of notable events.
- C. Current threats being tracked by the SOC.
- D. A display of the status of security tools.

Answer: B

Explanation:

The Security Posture dashboard is designed to provide high-level insight into the notable events across all domains of your deployment, suitable for display in a Security Operations Center (SOC). This dashboard shows all events from the past 24 hours, along with the trends over the past 24 hours, and provides real-time event information and updates.

Reference: <https://docs.splunk.com/Documentation/ES/6.1.0/User/SecurityPosturedashboard>

NEW 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.

Answer: B

NEW QUESTION 6

How should an administrator add a new lookup through the ES app?

- A. Upload the lookup file in Settings -> Lookups -> Lookup Definitions
- B. Upload the lookup file in Settings -> Lookups -> Lookup table files
- C. Add the lookup file to /etc/apps/SplunkEnterpriseSecuritySuite/lookups
- D. Upload the lookup file using Configure -> Content Management -> Create New Content -> Managed Lookup

Answer: D

Explanation:

Reference: <https://docs.splunk.com/Documentation/ES/6.1.0/Admin/Createlookups>

NEW QUESTION 7

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.

Answer: C

Explanation:

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

NEW QUESTION 8

Which of the following actions would not reduce the number of false positives from a correlation search?

- A. Reducing the severity.
- B. Removing throttling fields.
- C. Increasing the throttling window.
- D. Increasing threshold sensitivity.

Answer: A

NEW QUESTION 9

Which of the following would allow an add-on to be automatically imported into Splunk Enterprise Security?

- A. A prefix of CIM_
- B. A suffix of .spl
- C. A prefix of TECH_
- D. A prefix of Splunk_TA_

Answer: D

Explanation:

Reference: <https://dev.splunk.com/enterprise/docs/developapps/enterprisesecurity/planintegrations/>

NEW QUESTION 10

How is notable event urgency calculated?

- A. Asset priority and threat weight.
- B. Alert severity found by the correlation search.
- C. Asset or identity risk and severity found by the correlation search.
- D. Severity set by the correlation search and priority assigned to the associated asset or identity.

Answer: D

Explanation:

Reference: <https://docs.splunk.com/Documentation/ES/6.1.0/User/Howurgencyisassigned>

NEW QUESTION 10

What kind of value is in the red box in this picture?

Additional Fields	Value
HTTP Method	GET
Source	10.98.27.195 500
Source Expected	false
Source PCI Domain	untrust
Source Requires Antivirus	false
Source Should Time Synchronize	false
Source Should Update	false
Tag	modaction_result

- A. A risk score.
- B. A source ranking.
- C. An event priority.
- D. An IP address rating.

Answer: C

Explanation:

Reference: <https://docs.splunk.com/Documentation/Splunk/8.0.2/Data/FormateventsforHTTPEventCollector>

NEW QUESTION 15

Where is it possible to export content, such as correlation searches, from ES?

- A. Content exporter
- B. Configure -> Content Management
- C. Export content dashboard
- D. Settings Menu -> ES -> Export

Answer: B

Explanation:

Reference: <https://docs.splunk.com/Documentation/ES/6.1.0/Admin/Export>

NEW QUESTION 18

Which component normalizes events?

- A. SA-CIM.
- B. SA-Notable.
- C. ES application.
- D. Technology add-on.

Answer: A

Explanation:

Reference: <https://docs.splunk.com/Documentation/CIM/4.15.0/User/UsetheCIMtonormalizedataatsearchtime>

NEW QUESTION 20

.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your SPLK-3001 Exam with Our Prep Materials Via below:

<https://www.certleader.com/SPLK-3001-dumps.html>