

## SPLK-3001 Dumps

### Splunk Enterprise Security Certified Admin Exam

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



#### NEW QUESTION 1

Which of the following are examples of sources for events in the endpoint security domain dashboards?

- A. REST API invocations.
- B. Investigation final results status.
- C. Workstations, notebooks, and point-of-sale systems.
- D. Lifecycle auditing of incidents, from assignment to resolution.

**Answer:** D

**Explanation:**

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

#### NEW QUESTION 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>

#### NEW QUESTION 3

What does the risk framework add to an object (user, server or other type) to indicate increased risk?

- A. An urgency.
- B. A risk profile.
- C. An aggregation.
- D. A numeric score.

**Answer:** C

**Explanation:**

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

#### NEW QUESTION 4

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/Accelerateddatamodels>

#### NEW QUESTION 5

Which argument to the | tstats command restricts the search to summarized data only?

- A. summaries=t
- B. summaries=all
- C. summariesonly=t
- D. summariesonly=all

**Answer:** C

**Explanation:**

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

#### NEW QUESTION 6

Which of the following is a risk of using the Auto Deployment feature of Distributed Configuration Management to distribute indexes.conf?

- A. Indexes might crash.
- B. Indexes might be processing.
- C. Indexes might not be reachable.
- D. Indexes have different settings.

**Answer:** A

**Explanation:**

Reference: <https://docs.splunk.com/Documentation/Splunk/8.0.2/Admin/Indexesconf>

**NEW QUESTION 7**

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 8**

Which correlation search feature is used to throttle the creation of notable events?

- A. Schedule priority.
- B. Window interval.
- C. Window duration.
- D. Schedule windows.

**Answer: C**

**Explanation:**

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

**NEW QUESTION 9**

Both “Recommended Actions” and “Adaptive Response Actions” use adaptive response. How do they differ?

- A. Recommended Actions show a textual description to an analyst, Adaptive Response Actions show them encoded.
- B. Recommended Actions show a list of Adaptive Responses to an analyst, Adaptive Response Actions run them automatically.
- C. Recommended Actions show a list of Adaptive Responses that have already been run, Adaptive Response Actions run them automatically.
- D. Recommended Actions show a list of Adaptive Responses to an analyst, Adaptive Response Actions run manually with analyst intervention.

**Answer: D**

**Explanation:**

Reference: <https://docs.splunk.com/Documentation/ES/latest/Admin/Configureadaptiveresponse>

**NEW QUESTION 10**

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**

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

Additional Fields	Value
HTTP Method	GET
Source	10.98.27.195 <b>500</b>
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 11**

If a username does not match the 'identity' column in the identities list, which column is checked next?

- A. Email.
- B. Nickname
- C. IP address.
- D. Combination of Last Name, First Name.

**Answer: C**

**NEW QUESTION 13**

Which of the following features can the Add-on Builder configure in a new add-on?

- A. Expire data.
- B. Normalize data.
- C. Summarize data.
- D. Translate data.

**Answer: B**

**Explanation:**

Reference: <https://docs.splunk.com/Documentation/AddonBuilder/3.0.1/UserGuide/Overview>

**NEW QUESTION 14**

What is the maximum recommended volume of indexing per day, per indexer, for a non-cloud (on-prem) ES deployment?

- A. 50 GB
- B. 100 GB
- C. 300 GB
- D. 500 MB

**Answer: B**

**Explanation:**

Reference: <https://docs.splunk.com/Documentation/ITSI/4.4.2/Install/Plan>

**NEW QUESTION 17**

Which settings indicated that the correlation search will be executed as new events are indexed?

- A. Always-On
- B. Real-Time
- C. Scheduled
- D. Continuous

**Answer: C**

**Explanation:**

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

**NEW QUESTION 19**

Which data model populated the panels on the Risk Analysis dashboard?

- A. Risk
- B. Audit
- C. Domain analysis
- D. Threat intelligence

**Answer: A**

**Explanation:**

Reference: [https://docs.splunk.com/Documentation/ES/6.1.0/User/RiskAnalysis#Dashboard\\_panels](https://docs.splunk.com/Documentation/ES/6.1.0/User/RiskAnalysis#Dashboard_panels)

**NEW QUESTION 23**

When ES content is exported, an app with a .spl extension is automatically created. What is the best practice when exporting and importing updates to ES content?

- A. Use new app names each time content is exported.
- B. Do not use the .spl extension when naming an export.
- C. Always include existing and new content for each export.
- D. Either use new app names or always include both existing and new content.

**Answer: A**

**NEW QUESTION 27**

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 28**

What is the default schedule for accelerating ES Datamodels?

- A. 1 minute
- B. 5 minutes
- C. 15 minutes
- D. 1 hour

**Answer:** B

**Explanation:**

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

**NEW QUESTION 33**

.....

## 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>