

Splunk

Exam Questions SPLK-3001

Splunk Enterprise Security Certified Admin Exam



NEW QUESTION 1

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 2

Which indexes are searched by default for CIM data models?

- A. notable and default
- B. summary and notable
- C. _internal and summary
- D. All indexes

Answer: D

Explanation:

Reference: <https://answers.splunk.com/answers/600354/indexes-searched-by-cim-data-models.html>

NEW QUESTION 3

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 4

Which of the following is a way to test for a property normalized data model?

- A. Use Audit -> Normalization Audit and check the Errors panel.
- B. Run a | datamodel search, compare results to the CIM documentation for the datamodel.
- C. Run a | loadjob search, look at tag values and compare them to known tags based on the encoding.
- D. Run a | datamodel search and compare the results to the list of data models in the ES normalization guide.

Answer: B

Explanation:

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

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

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: B

NEW QUESTION 7

How is it possible to navigate to the list of currently-enabled ES correlation searches?

- A. Configure -> Correlation Searches -> Select Status “Enabled”
- B. Settings -> Searches, Reports, and Alerts -> Filter by Name of “Correlation”
- C. Configure -> Content Management -> Select Type “Correlation” and Status “Enabled”
- D. Settings -> Searches, Reports, and Alerts -> Select App of “SplunkEnterpriseSecuritySuite” and filter by “-Rule”

Answer: A

Explanation:

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

NEW QUESTION 8

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 9

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 10

At what point in the ES installation process should Splunk_TA_ForIndexes.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 10

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 11

Which of the following is a key feature of a glass table?

- A. Rigidity.
- B. Customization.
- C. Interactive investigations.
- D. Strong data for later retrieval.

Answer: B

NEW QUESTION 16

What are the steps to add a new column to the Notable Event table in the Incident Review dashboard?

- A. Configure -> Incident Management -> Notable Event Statuses
- B. Configure -> Content Management -> Type: Correlation Search
- C. Configure -> Incident Management -> Incident Review Settings -> Event Management
- D. Configure -> Incident Management -> Incident Review Settings -> Table Attributes

Answer: C

Explanation:

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

NEW QUESTION 20

To observe what network services are in use in a network's activity overall, which of the following dashboards in Enterprise Security will contain the most relevant data?

- A. Intrusion Center
- B. Protocol Analysis
- C. User Intelligence
- D. Threat Intelligence

Answer: A

Explanation:

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

NEW QUESTION 24

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 29

Where is the Add-On Builder available from?

- A. GitHub
- B. SplunkBase
- C. www.splunk.com
- D. The ES installation package

Answer: B

Explanation:

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

NEW QUESTION 33

Which of the following threat intelligence types can ES download? (Choose all that apply)

- A. Text
- B. STIX/TAXII
- C. VulnScanSPL
- D. SplunkEnterpriseThreatGenerator

Answer: B

Explanation:

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

NEW QUESTION 35

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>

NEW QUESTION 40

Enterprise Security's dashboards primarily pull data from what type of knowledge object?

- A. Tstats
- B. KV Store
- C. Data models
- D. Dynamic lookups

Answer: C

Explanation:

Reference: <https://docs.splunk.com/Splexicon:Knowledgeobject>

NEW QUESTION 42

To which of the following should the ES application be uploaded?

- A. The indexer.
- B. The KV Store.
- C. The search head.
- D. The dedicated forwarder.

Answer: C

Explanation:

Reference: <https://docs.splunk.com/Documentation/ES/6.1.0/Install/InstallEnterpriseSecuritySHC>

NEW QUESTION 44

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 47

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 50

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 54

Where are attachments to investigations stored?

- A. KV Store
- B. notable index
- C. attachments.csv lookup
- D. <splunk_home>/etc/apps/SA-Investigations/default/ui/views/attachments

Answer: A

Explanation:

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

NEW QUESTION 58

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

NEW QUESTION 60

Who can delete an investigation?

- A. ess_admin users only.
- B. The investigation owner only.
- C. The investigation owner and ess-admin.
- D. The investigation owner and collaborators.

Answer: A

Explanation:

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

NEW QUESTION 63

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.

Answer: D

Explanation:

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

NEW QUESTION 65

An administrator wants to ensure that none of the ES indexed data could be compromised through tampering. What feature would satisfy this requirement?

- A. Index consistency.
- B. Data integrity control.
- C. Indexer acknowledgement.
- D. Index access permissions.

Answer: B

Explanation:

Reference: <https://answers.splunk.com/answers/790783/anti-tampering-features-to-protect-splunk-logs-the.html>

NEW QUESTION 66

What is the first step when preparing to install ES?

- A. Install ES.
- B. Determine the data sources used.
- C. Determine the hardware required.
- D. Determine the size and scope of installation.

Answer: D

NEW QUESTION 67

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

SPLK-3001 Practice Exam Features:

- * SPLK-3001 Questions and Answers Updated Frequently
- * SPLK-3001 Practice Questions Verified by Expert Senior Certified Staff
- * SPLK-3001 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * SPLK-3001 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The SPLK-3001 Practice Test Here](#)