

Splunk

Exam Questions SPLK-3001

Splunk Enterprise Security Certified Admin Exam



NEW QUESTION 1

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

- A. DA-
- B. SA-
- C. TA-
- D. App-

Answer: C

Explanation:

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

NEW QUESTION 2

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 3

When creating custom correlation searches, what format is used to embed field values in the title, description, and drill-down fields of a notable event?

- A. \$fieldname\$
- B. "fieldname"
- C. %fieldname%
- D. _fieldname_

Answer: C

Explanation:

Reference: <https://docs.splunk.com/Documentation/ITSI/4.4.2/Configure/Createcorrelationsearch>

NEW QUESTION 4

What feature of Enterprise Security downloads threat intelligence data from a web server?

- A. Threat Service Manager
- B. Threat Download Manager
- C. Threat Intelligence Parser
- D. Threat Intelligence Enforcement

Answer: B

NEW QUESTION 5

Which column in the Asset or Identity list is combined with event security to make a notable event's urgency?

- A. VIP
- B. Priority
- C. Importance
- D. Criticality

Answer: B

Explanation:

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

NEW QUESTION 6

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 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

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 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

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 10

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 12

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 15

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 19

An administrator is asked to configure an "Nslookup" adaptive response action, so that it appears as a selectable option in the notable event's action menu when an analyst is working in the Incident Review dashboard. What steps would the administrator take to configure this option?

- A. Configure -> Content Management -> Type: Correlation Search -> Notable -> Nslookup
- B. Configure -> Type: Correlation Search -> Notable -> Recommended Actions -> Nslookup
- C. Configure -> Content Management -> Type: Correlation Search -> Notable -> Next Steps -> Nslookup
- D. Configure -> Content Management -> Type: Correlation Search -> Notable -> Recommended Actions -> Nslookup

Answer: D

NEW QUESTION 22

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 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

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 31

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

- 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 34

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 37

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 39

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 41

ES needs to be installed on a search head with which of the following options?

- A. No other apps.
- B. Any other apps installed.
- C. All apps removed except for TA-*
- D. Only default built-in and CIM-compliant apps.

Answer: A

Explanation:

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

NEW QUESTION 44

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 47

An administrator is provisioning one search head prior to installing ES. What are the reference minimum requirements for OS, CPU, and RAM for that machine?

- A. OS: 32 bit, RAM: 16 MB, CPU: 12 cores

- B. OS: 64 bit, RAM: 32 MB, CPU: 12 cores
- C. OS: 64 bit, RAM: 12 MB, CPU: 16 cores
- D. OS: 64 bit, RAM: 32 MB, CPU: 16 cores

Answer: C

Explanation:

Reference: <https://docs.splunk.com/Documentation/Splunk/8.0.2/Capacity/Referencehardware>

NEW QUESTION 51

The Brute Force Access Behavior Detected correlation search is enabled, and is generating many false positives. Assuming the input data has already been validated. How can the correlation search be made less sensitive?

- A. Edit the search and modify the notable event status field to make the notable events less urgent.
- B. Edit the search, look for where or xswhere statements, and after the threshold value being compared to make it less common match.
- C. Edit the search, look for where or xswhere statements, and alter the threshold value being compared to make it a more common match.
- D. Modify the urgency table for this correlation search and add a new severity level to make notable events from this search less urgent.

Answer: B

Explanation:

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

NEW QUESTION 56

Which of the following actions can improve overall search performance?

- A. Disable indexed real-time search.
- B. Increase priority of all correlation searches.
- C. Reduce the frequency (schedule) of lower-priority correlation searches.
- D. Add notable event suppressions for correlation searches with high numbers of false positives.

Answer: A

NEW QUESTION 61

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 62

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 67

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 72

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 76

.....

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](#)