



Splunk

Exam Questions SPLK-3001

Splunk Enterprise Security Certified Admin Exam

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

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. Therat Intelligence Enforcement

Answer: B

NEW QUESTION 3

The Remote Access panel within the User Activity dashboard is not populating with the most recent hour of data. What data model should be checked for potential errors such as skipped searches?

- A. Web
- B. Risk
- C. Performance
- D. Authentication

Answer: A

Explanation:

Reference: <https://answers.splunk.com/answers/565482/how-to-resolve-skipped-scheduled-searches.html>

NEW QUESTION 4

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 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

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 7

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 8

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 9

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 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

“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 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 12

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 13

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/planintegrationes/>

NEW QUESTION 18

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 23

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 25

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 28

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 31

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 35

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 39

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

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 48

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 49

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.

Answer: C

Explanation:

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

NEW QUESTION 52

After installing Enterprise Security, the distributed configuration management tool can be used to create which app to configure indexers?

- A. Splunk_DS_ForIndexers.spl
- B. Splunk_ES_ForIndexers.spl
- C. Splunk_SA_ForIndexers.spl
- D. Splunk_TA_ForIndexers.spl

Answer: D

Explanation:

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

NEW QUESTION 55

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 58

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 63

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 64

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 66

.....

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](#)