Actual exam question from Splunk's SPLK-3001

Question #: 1

Topic #: 1

[All SPLK-3001 Questions]

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

A. DA-

B. SA-

C. TA-

D. App-

Show Suggested Answer

Actual exam question from Splunk's SPLK-3001

Question #: 2

Topic #: 1

[All SPLK-3001 Questions]

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.

Show Suggested Answer

Actual exam question from Splunk's SPLK-3001

Question #: 3

Topic #: 1

[All SPLK-3001 Questions]

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. ɹ€fieldnameɹ€

C. %fieldname%

D. _fieldname_

Show Suggested Answer

Actual exam question from Splunk's SPLK-3001

Question #: 4

Topic #: 1

[All SPLK-3001 Questions]

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

Show Suggested Answer

Actual exam question from Splunk's SPLK-3001

Question #: 5

Topic #: 1

[All SPLK-3001 Questions]

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

Show Suggested Answer

Actual exam question from Splunk's SPLK-3001

Question #: 6

Topic #: 1

[All SPLK-3001 Questions]

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.

Show Suggested Answer

Actual exam question from Splunk's SPLK-3001

Question #: 7

Topic #: 1

[All SPLK-3001 Questions]

What role should be assigned to a security team member who will be taking ownership of notable events in the incident review dashboard?

A. ess_user

B. ess_admin

C. ess_analyst

D. ess_reviewer

Show Suggested Answer

Actual exam question from Splunk's SPLK-3001

Question #: 8

Topic #: 1

[All SPLK-3001 Questions]

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

Show Suggested Answer

Actual exam question from Splunk's SPLK-3001

Question #: 9

Topic #: 1

[All SPLK-3001 Questions]

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.

Show Suggested Answer

Actual exam question from Splunk's SPLK-3001

Question #: 10

Topic #: 1

[All SPLK-3001 Questions]

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

Show Suggested Answer

Actual exam question from Splunk's SPLK-3001

Question #: 11

Topic #: 1

[All SPLK-3001 Questions]

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

A. thawedPath

B. tstatsHomePath

C. summaryHomePath

D. warmToColdScript

Show Suggested Answer

Actual exam question from Splunk's SPLK-3001

Question #: 12

Topic #: 1

[All SPLK-3001 Questions]

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.

Show Suggested Answer

Actual exam question from Splunk's SPLK-3001

Question #: 13

Topic #: 1

[All SPLK-3001 Questions]

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

Show Suggested Answer

Actual exam question from Splunk's SPLK-3001

Question #: 14

Topic #: 1

[All SPLK-3001 Questions]

When investigating, what is the best way to store a newly-found IOC?

A. Paste it into Notepad.

B. Click the ɹ€Add IOCɹ€ button.

C. Click the ɹ€Add Artifactɹ€ button.

D. Add it in a text note to the investigation.

Show Suggested Answer

Actual exam question from Splunk's SPLK-3001

Question #: 15

Topic #: 1

[All SPLK-3001 Questions]

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

A. Configure -> Correlation Searches -> Select Status ɹ€Enabledɹ€

B. Settings -> Searches, Reports, and Alerts -> Filter by Name of ɹ€Correlationɹ€

C. Configure -> Content Management -> Select Type ɹ€Correlationɹ€ and Status ɹ€Enabledɹ€

D. Settings -> Searches, Reports, and Alerts -> Select App of ɹ€SplunkEnterpriseSecuritySuiteɹ€ and filter by ɹ€-Ruleɹ€

Show Suggested Answer

Actual exam question from Splunk's SPLK-3001

Question #: 16

Topic #: 1

[All SPLK-3001 Questions]

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

A. Indexers might crash.

B. Indexers might be processing.

C. Indexers might not be reachable.

D. Indexers have different settings.

Show Suggested Answer

Actual exam question from Splunk's SPLK-3001

Question #: 17

Topic #: 1

[All SPLK-3001 Questions]

Which of the following are data models used by ES? (Choose all that apply.)

A. Web

B. Anomalies

C. Authentication

D. Network Traffic

Show Suggested Answer

Actual exam question from Splunk's SPLK-3001

Question #: 18

Topic #: 1

[All SPLK-3001 Questions]

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.

Show Suggested Answer

Actual exam question from Splunk's SPLK-3001

Question #: 19

Topic #: 1

[All SPLK-3001 Questions]

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

A. Schedule priority.

B. Window interval.

C. Window duration.

D. Schedule window.

Show Suggested Answer

Actual exam question from Splunk's SPLK-3001

Question #: 20

Topic #: 1

[All SPLK-3001 Questions]

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 Resposes to an analyst, Adaptive Response Actions run manually with analyst intervention.

Show Suggested Answer

Actual exam question from Splunk's SPLK-3001

Question #: 21

Topic #: 1

[All SPLK-3001 Questions]

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.

Show Suggested Answer

Actual exam question from Splunk's SPLK-3001

Question #: 22

Topic #: 1

[All SPLK-3001 Questions]

`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.

Show Suggested Answer

Actual exam question from Splunk's SPLK-3001

Question #: 23

Topic #: 1

[All SPLK-3001 Questions]

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

Show Suggested Answer

Actual exam question from Splunk's SPLK-3001

Question #: 24

Topic #: 1

[All SPLK-3001 Questions]

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.

Show Suggested Answer

Actual exam question from Splunk's SPLK-3001

Question #: 25

Topic #: 1

[All SPLK-3001 Questions]

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.

Show Suggested Answer

Actual exam question from Splunk's SPLK-3001

Question #: 26

Topic #: 1

[All SPLK-3001 Questions]

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

Show Suggested Answer

Actual exam question from Splunk's SPLK-3001

Question #: 27

Topic #: 1

[All SPLK-3001 Questions]

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

Show Suggested Answer

Actual exam question from Splunk's SPLK-3001

Question #: 28

Topic #: 1

[All SPLK-3001 Questions]

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

Show Suggested Answer

Actual exam question from Splunk's SPLK-3001

Question #: 29

Topic #: 1

[All SPLK-3001 Questions]

Adaptive response action history is stored in which index?

A. cim_modactions

B. modular_history

C. cim_adaptiveactions

D. modular_action_history

Show Suggested Answer

Actual exam question from Splunk's SPLK-3001

Question #: 30

Topic #: 1

[All SPLK-3001 Questions]

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.

Show Suggested Answer

Actual exam question from Splunk's SPLK-3001

Question #: 31

Topic #: 1

[All SPLK-3001 Questions]

Where is the Add-On Builder available from?

A. GitHub

B. SplunkBase

C. www.splunk.com

D. The ES installation package

Show Suggested Answer

Actual exam question from Splunk's SPLK-3001

Question #: 32

Topic #: 1

[All SPLK-3001 Questions]

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_

Show Suggested Answer

Actual exam question from Splunk's SPLK-3001

Question #: 33

Topic #: 1

[All SPLK-3001 Questions]

ES apps and add-ons from $SPLUNK_HOME/etc/apps should be copied from the staging instance to what location on the cluster deployer instance?

A. $SPLUNK_HOME/etc/master-apps/

B. $SPLUNK_HOME/etc/system/local/

C. $SPLUNK_HOME/etc/shcluster/apps

D. $SPLUNK_HOME/var/run/searchpeers/

Show Suggested Answer

Actual exam question from Splunk's SPLK-3001

Question #: 34

Topic #: 1

[All SPLK-3001 Questions]

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.

Show Suggested Answer

Actual exam question from Splunk's SPLK-3001

Question #: 35

Topic #: 1

[All SPLK-3001 Questions]

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.

Show Suggested Answer

Actual exam question from Splunk's SPLK-3001

Question #: 36

Topic #: 1

[All SPLK-3001 Questions]

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

Show Suggested Answer

Actual exam question from Splunk's SPLK-3001

Question #: 37

Topic #: 1

[All SPLK-3001 Questions]

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

A. Text

B. STIX/TAXII

C. VulnScanSPL

D. SplunkEnterpriseThreatGenerator

Show Suggested Answer

Actual exam question from Splunk's SPLK-3001

Question #: 38

Topic #: 1

[All SPLK-3001 Questions]

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.

Show Suggested Answer

Actual exam question from Splunk's SPLK-3001

Question #: 39

Topic #: 1

[All SPLK-3001 Questions]

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

A. Tstats

B. KV Store

C. Data models

D. Dynamic lookups

Show Suggested Answer

Actual exam question from Splunk's SPLK-3001

Question #: 40

Topic #: 1

[All SPLK-3001 Questions]

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.

Show Suggested Answer

Actual exam question from Splunk's SPLK-3001

Question #: 41

Topic #: 1

[All SPLK-3001 Questions]

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.

Show Suggested Answer

Actual exam question from Splunk's SPLK-3001

Question #: 42

Topic #: 1

[All SPLK-3001 Questions]

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.

Show Suggested Answer

Actual exam question from Splunk's SPLK-3001

Question #: 43

Topic #: 1

[All SPLK-3001 Questions]

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

Show Suggested Answer

Actual exam question from Splunk's SPLK-3001

Question #: 44

Topic #: 1

[All SPLK-3001 Questions]

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.

Show Suggested Answer

Actual exam question from Splunk's SPLK-3001

Question #: 45

Topic #: 1

[All SPLK-3001 Questions]

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

A. Always-On

B. Real-Time

C. Scheduled

D. Continuous

Show Suggested Answer

Actual exam question from Splunk's SPLK-3001

Question #: 46

Topic #: 1

[All SPLK-3001 Questions]

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

Show Suggested Answer

Actual exam question from Splunk's SPLK-3001

Question #: 47

Topic #: 1

[All SPLK-3001 Questions]

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

A. Risk

B. Audit

C. Domain analysis

D. Threat intelligence

Show Suggested Answer

Actual exam question from Splunk's SPLK-3001

Question #: 48

Topic #: 1

[All SPLK-3001 Questions]

How is it possible to navigate to the ES graphical Navigation Bar editor?

A. Configure -> Navigation Menu

B. Configure -> General -> Navigation

C. Settings -> User Interface -> Navigation -> Click on ɹ€Enterprise Securityɹ€

D. Settings -> User Interface -> Navigation Menus -> Click on ɹ€defaultɹ€ next to SplunkEnterpriseSecuritySuite

Show Suggested Answer

Actual exam question from Splunk's SPLK-3001

Question #: 49

Topic #: 1

[All SPLK-3001 Questions]

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

Show Suggested Answer

Actual exam question from Splunk's SPLK-3001

Question #: 50

Topic #: 1

[All SPLK-3001 Questions]

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.

Show Suggested Answer

Actual exam question from Splunk's SPLK-3001

Question #: 51

Topic #: 1

[All SPLK-3001 Questions]

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.

Show Suggested Answer

Actual exam question from Splunk's SPLK-3001

Question #: 52

Topic #: 1

[All SPLK-3001 Questions]

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.

Show Suggested Answer

Actual exam question from Splunk's SPLK-3001

Question #: 53

Topic #: 1

[All SPLK-3001 Questions]

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

Show Suggested Answer

Actual exam question from Splunk's SPLK-3001

Question #: 54

Topic #: 1

[All SPLK-3001 Questions]

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.

Show Suggested Answer

Actual exam question from Splunk's SPLK-3001

Question #: 55

Topic #: 1

[All SPLK-3001 Questions]

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.

Show Suggested Answer

Actual exam question from Splunk's SPLK-3001

Question #: 56

Topic #: 1

[All SPLK-3001 Questions]

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.

Show Suggested Answer

Actual exam question from Splunk's SPLK-3001

Question #: 57

Topic #: 1

[All SPLK-3001 Questions]

Which component normalizes events?

A. SA-CIM.

B. SA-Notable.

C. ES application.

D. Technology add-on.

Show Suggested Answer

Actual exam question from Splunk's SPLK-3001

Question #: 58

Topic #: 1

[All SPLK-3001 Questions]

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.

Show Suggested Answer

Actual exam question from Splunk's SPLK-3001

Question #: 59

Topic #: 1

[All SPLK-3001 Questions]

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.

Show Suggested Answer

Actual exam question from Splunk's SPLK-3001

Question #: 60

Topic #: 1

[All SPLK-3001 Questions]

What is the default schedule for accelerating ES Datamodels?

A. 1 minute

B. 5 minutes

C. 15 minutes

D. 1 hour

Show Suggested Answer

Actual exam question from Splunk's SPLK-3001

Question #: 61

Topic #: 1

[All SPLK-3001 Questions]

Accelerated data requires approximately how many times the daily data volume of additional storage space per year?

A. 3.4

B. 5.7

C. 1.0

D. 2.5

Show Suggested Answer

Actual exam question from Splunk's SPLK-3001

Question #: 62

Topic #: 1

[All SPLK-3001 Questions]

When installing Enterprise Security, what should be done after installing the add-ons necessary for normalizing data?

A. Nothing, there are no additional steps for add-ons.

B. Configure the add-ons via the Content Management dashboard.

C. Disable the add-ons until they are ready to be used, then enable the add-ons.

D. Configure the add-ons according to their README or documentation.

Show Suggested Answer

Actual exam question from Splunk's SPLK-3001

Question #: 63

Topic #: 1

[All SPLK-3001 Questions]

What can be exported from ES using the Content Management page?

A. Only correlation searches, managed lookups, and glass tables.

B. Only correlation searches.

C. Any content type listed in the Content Management page.

D. Only correlation searches, glass tables, and workbench panels.

Show Suggested Answer

Actual exam question from Splunk's SPLK-3001

Question #: 64

Topic #: 1

[All SPLK-3001 Questions]

Where should an ES search head be installed?

A. On a Splunk server with top level visibility.

B. On any Splunk server.

C. On a server with a new install of Splunk.

D. On a Splunk server running Splunk DB Connect.

Show Suggested Answer

Actual exam question from Splunk's SPLK-3001

Question #: 65

Topic #: 1

[All SPLK-3001 Questions]

Following the installation of ES, an admin configured users with the ess_user role the ability to close notable events.

How would the admin restrict these users from being able to change the status of Resolved notable events to Closed?

A. In Enterprise Security, give the ess_user role the Own Notable Events permission.

B. From the Status Configuration window select the Closed status. Remove ess_user from the status transitions for the Resolved status.

C. From the Status Configuration window select the Resolved status. Remove ess_user from the status transitions for the Closed status.

D. From Splunk Access Controls, select the ess_user role and remove the edit_notable_events capability.

Show Suggested Answer

Actual exam question from Splunk's SPLK-3001

Question #: 66

Topic #: 1

[All SPLK-3001 Questions]

Which of the following actions may be necessary before installing ES?

A. Add additional indexers.

B. Redirect distributed search connections.

C. Purge KV Store.

D. Add additional forwarders.

Show Suggested Answer