Splunk.SPLK-3001.by.Ena.65q

Number: SPLK-3001
Passing Score: 800
Time Limit: 120
File Version: 4.0

Exam Code: SPLK-3001
Exam Name: Splunk Enterprise Security Certified Admin

Exam A

QUESTION 1
Which of the following is an adaptive action that is configured by default for ES?

A. Create notable event
B. Create new correlation search
C. Create investigation
D. Create new asset

Correct Answer: A
Section:

QUESTION 2
Which of the following are the default ports that must be configured for Splunk Enterprise Security to function?

A. SplunkWeb (8068), Splunk Management (8089), KV Store (8000)
B. SplunkWeb (8390), Splunk Management (8323), KV Store (8672)
C. SplunkWeb (8000), Splunk Management (8089), KV Store (8191)
D. SplunkWeb (8043), Splunk Management (8088), KV Store (8191)

Correct Answer: C
Section:
Explanation:
https://docs.splunk.com/Documentation/Splunk/8.1.2/Security/SecureSplunkonyournetwork

QUESTION 3
A customer site is experiencing poor performance. The UI response time is high and searches take a very long time to run. Some operations time out and there are errors in the scheduler logs, indicating too many concurrent searches are being started. 6 total correlation searches are scheduled and they have already been tuned to weed out false positives.
Which of the following options is most likely to help performance?

A. Change the search heads to do local indexing of summary searches.
B. Add heavy forwarders between the universal forwarders and indexers so inputs can be parsed before indexing.
C. Increase memory and CPUs on the search head(s) and add additional indexers.
D. If indexed realtime search is enabled, disable it for the notable index.

Correct Answer: C
Section:

QUESTION 4
What should be used to map a non-standard field name to a CIM field name?

A. Field alias.
B. Search time extraction.

C. Tag.
D. Eventtype.

Correct Answer: A
Section:

QUESTION 5
Which of the following lookup types in Enterprise Security contains information about known hostile IP addresses?

A. Security domains.
B. Threat intel.
C. Assets.
D. Domains.

Correct Answer: B
Section:
Explanation:
Reference: https://docs.splunk.com/Documentation/ES/6.4.1/Admin/Manageinternallookups

QUESTION 6
Which tool Is used to update indexers In E5?

A. Index Updater
B. Distributed Configuration Management
C. indexes.conf
D. Splunk_TA_ForIndexeres. spl

Correct Answer: B
Section:

QUESTION 7
Which of the following actions may be necessary before installing ES?

A. Redirect distributed search connections.
B. Purge KV Store.
C. Add additional indexers.
D. Add additional forwarders.

Correct Answer: C
Section:

QUESTION 8
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.

Correct Answer: C
Section:
Explanation:
Reference:
https://docs.splunk.com/Documentation/ES/6.1.0/User/EndpointProtectionDomaindashboards

QUESTION 9
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_

Correct Answer: A
Section:
Explanation:
Reference: https://docs.splunk.com/Documentation/ITSI/4.4.2/Configure/Createcorrelationsearch

QUESTION 10
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

Correct Answer: B
Section:
Explanation:
"The Threat Intelligence Framework provides a modular input (Threat Intelligence Downloads) that handles the majority of configurations typically needed for downloading intelligence files & data. To access this modular input, you simply need to create a stanza in your Inputs.conf file called “threatlist”."

QUESTION 11
The Remote Access panel within the User Activity dashboard is not populating with the most recent hour of dat a. What data model should be checked for potential errors such as skipped searches?

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

Correct Answer: D
Section:
Explanation:
Reference: https://answers.splunk.com/answers/565482/how-to-resolve-skipped-scheduledsearches.html

QUESTION 12
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.

Correct Answer: C
Section:
Explanation:
Reference:
https://docs.splunk.com/Documentation/CIM/4.15.0/User/UsetheCIMtonormalizeOSSECdata

QUESTION 13
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

Correct Answer: B
Section:
Explanation:
Reference: https://docs.splunk.com/Documentation/ES/6.1.0/User/Triagenotableevents

QUESTION 14
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

Correct Answer: B
Section:
Explanation:
Reference: https://docs.splunk.com/Documentation/ES/6.1.0/User/Howurgencyisassigned

QUESTION 15
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.

Correct Answer: D
Section:
Explanation:
Reference: https://docs.splunk.com/Documentation/ES/6.1.0/User/RiskScoring

QUESTION 16
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

Correct Answer: D
Section:
Explanation:
Reference: https://answers.splunk.com/answers/600354/indexes-searched-by-cim-datamodels.html

QUESTION 17
Which setting is used in indexes.conf to specify alternate locations for accelerated storage?

A. thawedPath
B. tstatsHomePath
C. summaryHomePath
D. warmToColdScript

Correct Answer: B
Section:
Explanation:
Reference:
https://docs.splunk.com/Documentation/Splunk/8.0.2/Knowledge/Acceleratedatamodels

QUESTION 18
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.

Correct Answer: B
Section:
Explanation:
Reference:
https://docs.splunk.com/Documentation/CIM/4.15.0/User/UsetheCIMtonormalizedataatsearchtime

QUESTION 19
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

Correct Answer: C
Section:
Explanation:
Reference:
https://docs.splunk.com/Documentation/Splunk/8.0.2/Knowledge/Acceleratedatamodels

QUESTION 20
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.

Correct Answer: C
Section:

QUESTION 21
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”

Correct Answer: C
Section:
Explanation:
Reference: https://docs.splunk.com/Documentation/ES/6.1.0/Admin/Listcorrelationsearches

QUESTION 22
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.

Correct Answer: A
Section:
Explanation:

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

QUESTION 23
Which of the following are data models used by ES? (Choose all that apply)

A. Web
B. Anomalies
C. Authentication
D. Network Traffic

Correct Answer: A, C, D
Section:
Explanation:
Reference:
https://dev.splunk.com/enterprise/docs/developapps/enterprisesecurity/datamodelsusedbyes/

QUESTION 24
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.

Correct Answer: C
Section:
Explanation:
Reference: https://docs.splunk.com/Documentation/ES/6.1.0/Install/InstallTechnologyAdd-ons

QUESTION 25
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.

Correct Answer: C
Section:
Explanation:
Reference: https://docs.splunk.com/Documentation/ES/6.1.0/Admin/Configurecorrelationsearches

QUESTION 26
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.

Correct Answer: D
Section:
Explanation:
Reference: https://docs.splunk.com/Documentation/ES/latest/Admin/Configureadaptiveresponse

QUESTION 27
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.

Correct Answer: B
Section:
Explanation:
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
Reference: https://docs.splunk.com/Documentation/ES/6.1.0/User/SecurityPosturedashboard

QUESTION 28
"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.

Correct Answer: B
Section:

QUESTION 29
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

Correct Answer: D
Section:
Explanation:
Reference: https://docs.splunk.com/Documentation/ES/6.1.0/Admin/Createlookups

QUESTION 30
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.

Correct Answer: C
Section:
Explanation:
Reference: https://docs.splunk.com/Documentation/ES/6.1.0/User/CreateGlassTable

QUESTION 31
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.

Correct Answer: B
Section:

QUESTION 32
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

Correct Answer: D
Section:

QUESTION 33
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

Correct Answer: D
Section:
Explanation:

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

QUESTION 34
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.

Correct Answer: B
Section:
Explanation:
Reference: https://docs.splunk.com/Documentation/ES/6.1.0/User/Howurgencyisassigned

QUESTION 35
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.

Correct Answer: A
Section:

QUESTION 36
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.

Correct Answer: D
Section:
Explanation:
Reference: https://www.splunk.com/en_us/products/premium-solutions/splunk-enterprisesecurity/features.html

QUESTION 37
Which component normalizes events?

A. SA-CIM.
B. SA-Notable.
C. ES application.
D. Technology add-on.

Correct Answer: A
Section:
Explanation:
Reference:
https://docs.splunk.com/Documentation/CIM/4.15.0/User/UsetheCIMtonormalizedataatsearchtime

QUESTION 38
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.

Correct Answer: B
Section:
Explanation:
Reference: https://answers.splunk.com/answers/790783/anti-tampering-features-to-protect-splunklogs-the.html

QUESTION 39
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.

Correct Answer: D
Section:

QUESTION 40
What is the default schedule for accelerating ES Datamodels?

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

Correct Answer: B
Section:

QUESTION 41
Which of the following is a Web Intelligence dashboard?

A. Network Center
B. Endpoint Center
C. HTTP Category Analysis

D. stream :http Protocol dashboard

Correct Answer: C
Section:

QUESTION 42
When using distributed configuration management to create the Splunk_TA_ForIndexers package, which three files can be included?

A. indexes.conf, props.conf, transforms.conf
B. web.conf, props.conf, transforms.conf
C. inputs.conf, props.conf, transforms.conf
D. eventtypes.conf, indexes.conf, tags.conf

Correct Answer: A
Section:
Explanation:
Reference: https://docs.splunk.com/Documentation/ES/6.4.1/Install/InstallTechnologyAdd-ons

QUESTION 43
Which of these Is a benefit of data normalization?

A. Reports run faster because normalized data models can be optimized for better performance.
B. Dashboards take longer to build.
C. Searches can be built no matter the specific source technology for a normalized data type.
D. Forwarder-based inputs are more efficient.

Correct Answer: A
Section:

QUESTION 44
Following the Installation of ES, an admin configured Leers with the ©ss_uso r 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. From the Status Configuration window select the Resolved status. Remove ess_user from the status transitions for the closed status.
B. From the Status Configuration windows select the closed status. Remove ess_use r from the status transitions for the Resolved status.
C. In Enterprise Security, give the ess_user role the own Notable Events permission.
D. From Splunk Access Controls, select the ess_user role and remove the edit_notabie_events capability.

Correct Answer: B
Section:

QUESTION 45
What is the bar across the bottom of any ES window?

A. The Investigator Workbench.
B. The Investigation Bar.
C. The Analyst Bar.

D. The Compliance Bar.

Correct Answer: B
Section:
Explanation:
Reference: https://docs.splunk.com/Documentation/ES/6.4.1/User/Startaninvestigation

QUESTION 46
Which lookup table does the Default Account Activity Detected correlation search use to flag known default accounts?

A. Administrative Identities
B. Local User Intel
C. Identities
D. Privileged Accounts

Correct Answer: C
Section:

QUESTION 47
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.

Correct Answer: B
Section:
Explanation:
Reference: https://docs.splunk.com/Documentation/ES/6.4.1/Admin/Export

QUESTION 48
A newly built custom dashboard needs to be available to a team of security analysts In ES. How is It possible to Integrate the new dashboard?

A. Add links on the ES home page to the new dashboard.
B. Create a new role Inherited from es_analyst, make the dashboard permissions read-only, and make this dashboard the default view for the new role.
C. Set the dashboard permissions to allow access by es_analysts and use the navigation editor to add it to the menu.
D. Add the dashboard to a custom add-in app and install it to ES using the Content Manager.

Correct Answer: C
Section:

QUESTION 49
Analysts have requested the ability to capture and analyze network traffic dat a. The administrator has researched the documentation and, based on this research, has decided to integrate the Splunk App for Stream with ES. Which dashboards will now be supported so analysts can view and analyze network Stream data?

A. Endpoint dashboards.

B. User Intelligence dashboards.
C. Protocol Intelligence dashboards.
D. Web Intelligence dashboards.

Correct Answer: C
Section:

QUESTION 50
Which of the following is a recommended pre-installation step?

A. Disable the default search app.
B. Configure search head forwarding.
C. Download the latest version of KV Store from MongoDBxom.
D. Install the latest Python distribution on the search head.

Correct Answer: B
Section:

QUESTION 51
Which feature contains scenarios that are useful during ES Implementation?

A. Use Case Library
B. Correlation Searches
C. Predictive Analytics
D. Adaptive Responses

Correct Answer: B
Section:
Explanation:
Reference: https://www.splunk.com/pdfs/professional-services/2019/splunk-enterprise-securityimplementation-success.pdf

QUESTION 52
The option to create a Short ID for a notable event is located where?

A. The Additional Fields.
B. The Event Details.
C. The Contributing Events.
D. The Description.

Correct Answer: B
Section:
Explanation:
https://docs.splunk.com/Documentation/ES/6.4.1/User/Takeactiononanotableevent

QUESTION 53
After managing source types and extracting fields, which key step comes next In the Add-On Builder?

A. Validate and package
B. Configure data collection.
C. Create alert actions.
D. Map to data models.

Correct Answer: D
Section:

QUESTION 54
What is an example of an ES asset?

A. MAC address
B. User name
C. Server
D. People

Correct Answer: A
Section:

QUESTION 55
Which of the following steps will make the Threat Activity dashboard the default landing page in ES?

A. From the Edit Navigation page, drag and drop the Threat Activity view to the top of the page.
B. From the Preferences menu for the user, select Enterprise Security as the default application.
C. From the Edit Navigation page, click the 'Set this as the default view" checkmark for Threat Activity.
D. Edit the Threat Activity view settings and checkmark the Default View option.

Correct Answer: C
Section:

QUESTION 56
What do threat gen searches produce?

A. Threat Intel in KV Store collections.
B. Threat correlation searches.
C. Threat notables in the notable index.
D. Events in the threat_activity index.

Correct Answer: D
Section:
Explanation:
https://docs.splunk.com/Documentation/ES/6.4.1/Admin/Createthreatmatchspecs

QUESTION 57
Which of the following is part of tuning correlation searches for a new ES installation?

A. Configuring correlation notable event index.

B. Configuring correlation permissions.
C. Configuring correlation adaptive responses.
D. Configuring correlation result storage.

Correct Answer: A
Section:

QUESTION 58
A security manager has been working with the executive team en long-range security goals. A primary goal for the team Is to Improve managing user risk in the organization. Which of the following ES features can help identify users accessing inappropriate web sites?

A. Configuring the identities lookup with user details to enrich notable event Information for forensic analysis.
B. Make sure the Authentication data model contains up-to-date events and is properly accelerated.
C. Configuring user and website watchlists so the User Activity dashboard will highlight unwanted user actions.
D. Use the Access Anomalies dashboard to identify unusual protocols being used to access corporate sites.

Correct Answer: C
Section:

QUESTION 59
How is it possible to specify an alternate location for accelerated storage?

A. Configure storage optimization settings for the index.
B. Update the Home Path setting in indexes, conf
C. Use the tstatsHomePath setting in props, conf
D. Use the tstatsHomePath Setting in indexes, conf

Correct Answer: C
Section:

QUESTION 60
When installing Enterprise Security, what should be done after installing the add-ons necessary for normalizing data?

A. Configure the add-ons according to their README or documentation.
B. Disable the add-ons until they are ready to be used, then enable the add-ons.
C. Nothing, there are no additional steps for add-ons.
D. Configure the add-ons via the Content Management dashboard.

Correct Answer: A
Section:

QUESTION 61
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

Correct Answer: A
Section:
Explanation:
Reference: https://docs.splunk.com/Documentation/ES/6.4.1/Install/Datamodels

QUESTION 62
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.

Correct Answer: C
Section:
Explanation:
Reference:
https://docs.splunk.com/Documentation/ES/6.4.1/Admin/Export#:~:text=as%20an%20app-,Export%20content%20from%20Splunk%20Enterprise%20Security%20as,from%20the%20Content%20Management%20page.&text=You%20can%20export%20any%20type,%2C%20data%20models%2C%20and%20views.

QUESTION 63
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.

Correct Answer: C
Section:

QUESTION 64
A set of correlation searches are enabled at a new ES installation, and results are being monitored.
One of the correlation searches is generating many notable events which, when evaluated, are determined to be false positives.
What is a solution for this issue?

A. Suppress notable events from that correlation search.
B. Disable acceleration for the correlation search to reduce storage requirements.
C. Modify the correlation schedule and sensitivity for your site.
D. Change the correlation search's default status and severity.

Correct Answer: A
Section:

QUESTION 65

Where is detailed information about identities stored?

A. The Identity Investigator index.
B. The Access Anomalies collection.
C. The User Activity index.
D. The Identity Lookup CSV file.

Correct Answer: C
Section: