ATMIC NETWORKS
YOUR GUIDE TO GLOBAL CERTIFIATION

"Please note that these files may not be up to date. However, the questions will help you understand the exam format and typical question patterns."

www.atmicnetworks .com

Warning: Keep connected with our support team for latest updates

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/

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: C

Explanation:

Reference:
https://docs.splunk.com/Documentation/ES/6.1.0/User/EndpointProtectionDomaindashboards

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: A

Explanation:

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

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. Therat Intelligence Enforcement

Answer: B

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: 5

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

Answer: D

Explanation:

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

Question: 6

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

Question: 7

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

Answer: B

Explanation:

Reference: https://docs.splunk.com/Documentation/ES/6.1.0/User/Triagenotableevents

Question: 8

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

Question: 9

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: D

Explanation:

Reference: https://docs.splunk.com/Documentation/ES/6.1.0/User/RiskScoring

Question: 10

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

Question: 11

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/Acceleratedatamodels

Question: 12

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

Question: 13

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/Acceleratedatamodels

Question: 14

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: C

Explanation:

Question: 15

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: C

Explanation:

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

Question: 16

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

Question: 17

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

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

Answer: A,C,D

Explanation:

Reference:
https://dev.splunk.com/enterprise/docs/developapps/enterprisesecurity/datamodelsusedbyes/

Question: 18

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: C

Explanation:

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

Question: 19

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

Question: 20

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.

Answer: D

Explanation:

Reference: https://docs.splunk.com/Documentation/ES/latest/Admin/Configureadaptiveresponse

Question: 21

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:

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: 22

“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

Explanation:

Question: 23

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

Question: 24

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

Question: 25

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

Explanation:

Question: 26

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

Explanation:

Question: 27

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: D

Explanation:

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

Question: 28

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: B

Explanation:

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

Question: 29

Adaptive response action history is stored in which index?

A. cim_modactions
B. modular_history
C. cim_adaptiveactions
D. modular_action_history

Answer: A

Explanation:

Reference: https://docs.splunk.com/Documentation/ES/6.1.0/Install/Indexes

Question: 30

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

Explanation:

Question: 31

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

Question: 32

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/

Question: 33

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/

Answer: C

Explanation:

Explanation:
The upgraded contents of the staging instance will be migrated back to the deployer and deployed to the search head cluster members. On the staging instance, copy $SPLUNK_HOME/etc/apps to $SPLUNK_HOME/etc/shcluster/apps on the deployer. 1. On the deployer, remove any deprecated apps or add-ons in $SPLUNK_HOME/etc/shcluster/apps that were removed during the upgrade on staging. Confirm by reviewing the ES upgrade report generated on staging, or by examining the apps moved into $SPLUNK_HOME/etc/disabled-apps on staging

Question: 34

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

Question: 35

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

Additional Fields	Value
HTTP Method	GET
Source	1098.27.195
Source Expected	false
Source PCI Domain	unttust
Source Requires Antivirus	false
Source Should Time Synchronize	false
Source Should Update	false
Tag	m oda cticn_res u lt

A. A risk score.
B. A source ranking.
C. An event priority.
D. An IP address rating.

Answer: A

Explanation:

Reference:
https://docs.splunk.com/Documentation/Splunk/8.0.2/Data/FormateventsforHTTPEventCollector

Question: 36

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

Question: 37

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

A. Text
B. STIX/TAXII
C. VulnScanSPL

D. SplunkEnterpriseThreatGenerator

Answer: AB

Explanation:

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

Question: 38

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

Question: 39

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

Question: 40

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

Question: 41

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: A

Explanation:

Question: 42

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

Question: 43

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

Answer: B

Explanation:

Reference: https://docs.splunk.com/Documentation/ITSI/4.4.2/Install/Plan

Question: 44

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: D

Explanation:

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

Question: 45

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

Question: 46

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

Question: 47

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

Question: 48

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 "Enterprise Security"
D. Settings -> User Interface -> Navigation Menus -> Click on "default" next to SplunkEnterpriseSecuritySuite

Answer: B

Explanation:

Reference: https://docs.splunk.com/Documentation/ES/6.1.0/Admin/Customizemenubar#Restore_the_default_navigation

Question: 49

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

Question: 50

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

Question: 51

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.

Answer: D

Explanation:

Either use new app names each time (which could be difficult to manage) or make sure you always include all content (old and new) each time you export.

Question: 52

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

Question: 53

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

Question: 54

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

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

Explanation:

Question: 56

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

Question: 57

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

Question: 58

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

Question: 59

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

Explanation:

Question: 60

What is the default schedule for accelerating ES Datamodels?

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

Answer: B

Explanation:

Question: 61

Which of the following is a Web Intelligence dashboard?

A. Network Center
B. Endpoint Center
C. HTTP Category Analysis
D. stream :http Protocol dashboard

Answer: C

Explanation:

Question: 62

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

Answer: A

Explanation:

Question: 63

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)

Answer: C

Explanation:

https://docs.splunk.com/Documentation/Splunk/8.1.2/Security/SecureSplunkonyournetwork

Question: 64

Which tool Is used to update indexers In E5?

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

Answer: B

Explanation:

Question: 65

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.

Answer: C

Explanation:

Question: 66

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

Answer: A

Explanation:

Reference: https://docs.splunk.com/Documentation/ES/6.4.1/Install/InstallTechnologyAdd-ons

Question: 67

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.

Answer: A

Explanation:

Question: 68

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.

Answer: B

Explanation:

Question: 69

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.

Answer: B

Explanation:

Reference: https://docs.splunk.com/Documentation/ES/6.4.1/User/Startaninvestigation

Question: 70

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

Answer: C

Explanation:

Question: 71

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.

Answer: B

Explanation:

Reference: https://docs.splunk.com/Documentation/ES/6.4.1/Admin/Export

Question: 72

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.

Answer: C

Explanation:

Question: 73

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.

Answer: C

Explanation:

Question: 74

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.

Answer: B

Explanation:

Question: 75

Which feature contains scenarios that are useful during ES Implementation?

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

Answer: B

Explanation:

Reference: https://www.splunk.com/pdfs/professional-services/2019/splunk-enterprise-security-implementation-success.pdf

Question: 76

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.

Answer: B

Explanation:

https://docs.splunk.com/Documentation/ES/6.4.1/User/Takeactiononanotableevent

Question: 77

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.

Answer: D

Explanation:

Question: 78

What is an example of an ES asset?

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

Answer: A

Explanation:

Question: 79

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.

Answer: C

Explanation:

Question: 80

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.

Answer: D

Explanation:

https://docs.splunk.com/Documentation/ES/6.4.1/Admin/Createthreatmatchspecs

Question: 81

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.

Answer: A

Explanation:

Question: 82

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.

Answer: C

Explanation:

Question: 83

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

Answer: C

Explanation:

Question: 84

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.

Answer: A

Explanation:

Question: 85

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

Answer: A

Explanation:

Reference: https://docs.splunk.com/Documentation/ES/6.4.1/Install/Datamodels

Question: 86

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.

Answer: C

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: 87

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.

Answer: C

Explanation:

Question: 88

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.

Answer: C

Explanation:

Question: 89

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.

Answer: A

Explanation:

Question: 90

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.

Answer: B

Explanation:

Reference: https://docs.splunk.com/Documentation/ES/6.4.1/Admin/Manageinternallookups

Question: 91

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.

Answer: A

Explanation:

Question: 92

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.

Answer: C

Explanation:

Question: 93

Which two fields combine to create the Urgency of a notable event?

A. Priority and Severity.
B. Priority and Criticality.
C. Criticality and Severity.
D. Precedence and Time.

Answer: A

Explanation:

Reference: https://docs.splunk.com/Documentation/ES/6.4.1/User/Howurgencyisassigned

Question: 94

Which columns in the Assets lookup are used to identify an asset in an event?

A. src, dvc, dest
B. cidr, port, netbios, saml
C. ip, mac, dns, nt_host
D. host, hostname, url, address

Answer: C

Explanation:

Reference: https://docs.splunk.com/Documentation/ES/6.4.1/Admin/Formatassetoridentitylist

Question: 95

What does the summariesonly=true option do for a correlation search?

A. Searches only accelerated data.
B. Forwards summary indexes to the indexing tier.
C. Uses a default summary time range.
D. Searches summary indexes only.

Answer: A

Explanation:

Reference: https://community.splunk.com/t5/Splunk-Enterprise-Security/Why-do-correlation-searches-in- Enterprise-Security-not-use-quot/m-p/262622

Question: 96

What is the main purpose of the Dashboard Requirements Matrix document?

A. Identifies on which data model(s) each dashboard depends.
B. Provides instructions for customizing each dashboard for local data models.
C. Identifies the searches used by the dashboards.
D. Identifies which data model(s) depend on each dashboard.

Answer: D

Question: 97

What are adaptive responses triggered by?

A. By correlation searches and users on the incident review dashboard.
B. By correlation searches and custom tech add-ons.
C. By correlation searches and users on the threat analysis dashboard.

D. By custom tech add-ons and users on the risk analysis dashboard.

Answer: D

Explanation:

Question: 98

How does ES know local customer domain names so it can detect internal vs. external emails?

A. Web and email domain names are set in General -> General Configuration.
B. ES uses the User Activity index and applies machine learning to determine internal and external domains.
C. The Corporate Web and Email Domain Lookups are edited during initial configuration.
D. ES extracts local email and web domains automatically from SMTP and HTTP logs.

Answer: C

Explanation:

Question: 99

After data is ingested, which data management step is essential to ensure raw data can be accelerated by a Data Model and used by ES?

A. Applying Tags.
B. Normalization to Customer Standard.
C. Normalization to the Splunk Common Information Model.
D. Extracting Fields.

Answer: C