Splunk.SPLK-3001.v2025-12-15.q104

Exam Code:	SPLK-3001
Exam Name:	Splunk Enterprise Security Certified Admin Exam
Certification Provider:	Splunk
Free Question Number:	104
Version:	v2025-12-15
# of views:	172
# of Questions views:	1040
https://www.exam-tests.com/SPLK-3001-exam/Splunk.SPLK-3001.v2025-12-15.q104.html	

NEW QUESTION: 1
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_reviewer
B. ess_user
C. ess_analyst
D. ess_admin
Answer: C (LEAVE A REPLY)

NEW QUESTION: 2
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: (SHOW ANSWER)
Explanation/Reference:
https://docs.splunk.com/Documentation/ES/6.4.1/Admin/Manageinternallookups

NEW QUESTION: 3
Which of the following are data models used by ES? (Choose all that apply.)
A. Web
B. Anomalies
C. Authentication
D. Network Traffic
Answer: B (LEAVE A REPLY)

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

NEW QUESTION: 4
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 (LEAVE A REPLY)
Explanation
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, the administrator would take the following steps:
On the Splunk Enterprise Security menu bar, click Configure > Content > Content Management.
Filter the content by Type: Correlation Search and select the correlation search that you want to add the Nslookup action to.
Click Edit and go to the Notable tab.
Under Recommended Actions, click Add New Action and select Nslookup from the drop-down menu.
Enter the required fields for the Nslookup action, such as the host field, the DNS server, and the output index.
Click Save to save the changes to the correlation search.
The Nslookup action will now appear as an option in the notable event's action menu on the Incident Review dashboard. References = Set up Adaptive Response actions in Splunk Enterprise Security Included adaptive response actions with Splunk Enterprise Security

NEW QUESTION: 5
Where should an ES search head be installed?
A. On a Splunk server running Splunk DB Connect.
B. On any Splunk server.
C. On a Splunk server with top level visibility.
D. On a server with a new install of Splunk.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 6
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 (LEAVE A REPLY)
Reference:
https://docs.splunk.com/Documentation/ES/6.1.0/User/Triagenotableevents

NEW QUESTION: 7
If a username does not match the 'identity' column in the identities list, which column is checked next?
A. Email.
B. Combination of Last Name, First Name.
C. Nickname
D. IP address.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 8
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: C,D (LEAVE A REPLY)
Explanation
Correlation searches are scheduled searches that run in Splunk Enterprise Security to detect security incidents or other notable events. They can consume a lot of resources and affect the overall search performance. To improve the search performance, you can do the following actions:
Reduce the frequency (schedule) of lower-priority correlation searches. This will reduce the number of searches that run concurrently and free up some resources for other searches. You can edit the schedule of a correlation search in the Content Management page of Splunk Enterprise Security. See Edit a correlation search in Splunk Enterprise Security for more details.
Add notable event suppressions for correlation searches with high numbers of false positives. This will prevent the correlation search from generating notable events that are not relevant or actionable, and reduce the load on the Notable Event Framework. You can add suppression rules for a correlation search in the Content Management page of Splunk Enterprise Security. See Suppress notable events in Splunk Enterprise Security for more details.

The other two actions are not recommended, because they can have negative effects on the search performance or the security posture. Disabling indexed real-time search can cause some dashboards and panels to not display data correctly, and increasing the priority of all correlation searches can cause resource contention and degrade the performance of other searches. See Optimize Splunk Enterprise for peak performance and How search types affect Splunk Enterprise performance for more information. References = Edit a correlation search in Splunk Enterprise Security Suppress notable events in Splunk Enterprise Security Optimize Splunk Enterprise for peak performance How search types affect Splunk Enterprise performance

NEW QUESTION: 9
Which component normalizes events?
A. SA-CIM.
B. SA-Notable.
C. ES application.
D. Technology add-on.
Answer: A (LEAVE A REPLY)
Reference:
https://docs.splunk.com/Documentation/CIM/4.15.0/User/UsetheCIMtonormalizedataatsearchtime

NEW QUESTION: 10
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 (LEAVE A REPLY)
Explanation
The argument to the | tstats command that restricts the search to summarized data only is summariesonly=t.
Summarized data is the data that is generated by the data model acceleration process, which creates summary indexes (TSIDX files) for the data models. By using summariesonly=t, the tstats command will only search the summary indexes, which can improve the performance and efficiency of the search. However, this also means that the search will not return any events that are not covered by the data model acceleration, such as events outside the acceleration time range or events that do not match the data model constraints12. References = 1:
tstats - Splunk Documentation - summariesonly. 2: Managing data models in Enterprise Security - Splunk Lantern - Indexes allow list.
Fun (or Less Agony) with Splunk Tstats | Deductiv

NEW QUESTION: 11
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 (LEAVE A REPLY)
Explanation

NEW QUESTION: 12
Where is detailed information about identities stored?
A. The User Activity index.
B. The Access Anomalies collection.
C. The Identity Lookup CSV file.
D. The Identity Investigator index.
Answer: (SHOW ANSWER)

NEW QUESTION: 13
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: (SHOW ANSWER)
Explanation
According to the Splunk Enterprise Security documentation, threat gen searches are searches that generate synthetic events in the threat activity index to simulate security threats. Threat gen searches are useful for testing and validating the correlation searches, notable events, and adaptive response actions in Splunk Enterprise Security. Threat gen searches produce events in the threat activity index, which is a dedicated index for storing the synthetic events. The events in the threat activity index have the sourcetype of threatgen and the tag of threat. You can use the Threat Activity dashboard to view and analyze the events in the threat activity index. See Threat gen searches for more details.
The other options are not correct, because threat gen searches do not produce them. Threat gen searches do not produce threat intel in KV Store collections, which are key-value pairs of data that store and manage threat intelligence in Splunk Enterprise Security. Threat gen searches do not produce threat correlation searches, which are searches that correlate events with threat intelligence and generate notable events in Splunk Enterprise Security. Threat gen searches do not produce threat notables in the notable index, which are alerts or tasks that indicate potential security incidents or threats in Splunk Enterprise Security. Therefore, the correct answer is D. Events in the threat activity index. References = Threat gen searches. Upping the Auditing Game for Correlation Searches Within ... - Splunk

NEW QUESTION: 14
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: C (LEAVE A REPLY)
Explanation
The role that should be assigned to a security team member who will be taking ownership of notable events in the incident review dashboard is the ess_analyst role. The ess_analyst role is a predefined role in Splunk Enterprise Security that grants the user the ability to view, edit, comment, and change the status and owner of notable events. The ess_analyst role also allows the user to access the dashboards, reports, and searches related to security analysis and investigation12. References = 1: Overview of roles and capabilities in Splunk Enterprise Security - Splunk Documentation - ess_analyst role. 2: Incident Review - Splunk Documentation - Triage notable events on the Incident Review dashboard.

NEW QUESTION: 15
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 (LEAVE A REPLY)

NEW QUESTION: 16
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 (LEAVE A REPLY)
Explanation/Reference: https://www.splunk.com/en_us/products/premium-solutions/splunk-enterprise-security/features.html

NEW QUESTION: 17
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: A (LEAVE A REPLY)
Explanation
According to the Splunk Enterprise Security documentation, the Status Configuration window allows you to customize the status values and transitions for notable events. You can define which roles can change the status of a notable event from one value to another, and which roles can view the notable events with a specific status. To restrict the users with the ess_user role from being able to change the status of Resolved notable events to closed, you need to do the following steps:
On the Enterprise Security menu bar, select Configure > Incident Management > Status Configuration.
In the Status Configuration window, select the Resolved status from the list of values.
In the Status Transitions section, find the row for the closed status and click the Edit icon.
In the Edit Status Transition dialog box, remove the ess_user role from the Roles field and click Save.
Click Save Changes to apply the changes to the Status Configuration window.
This will prevent the users with the ess_user role from changing the status of any notable event from Resolved to closed. They will still be able to change the status of other notable events to closed, if they have the permission to do so. Therefore, the correct answer is A. From the Status Configuration window select the Resolved status. Remove ess_user from the status transitions for the closed status. References = Customize status values and transitions for notable events.

NEW QUESTION: 18
At what point in the ES installation process should Splunk_TA_ForIndexes.spl be deployed to the indexers?
A. After installing ES on the search head(s) and running the distributed configuration management tool.
B. Splunk_TA_ForIndexers.spl is only installed on indexer cluster sites using the cluster master and the splunk apply cluster-bundle command.
C. When adding apps to the deployment server.
D. Splunk_TA_ForIndexers.spl is installed first.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 19
Which of the following ES features would a security analyst use while investigating a network anomaly notable?
A. Key indicator search.
B. Protocol intelligence dashboard.
C. Correlation editor.
D. Threat download dashboard.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 20
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: (SHOW ANSWER)
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

NEW QUESTION: 21
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: (SHOW ANSWER)

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

NEW QUESTION: 22
When using distributed configuration management to create the Splunk_TA_ForIndexerspackage, 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 (LEAVE A REPLY)
Explanation/Reference:
https://docs.splunk.com/Documentation/ES/6.4.1/Install/InstallTechnologyAdd-ons

NEW QUESTION: 23
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 (LEAVE A REPLY)
Explanation
Data models are the primary source of data for Enterprise Security dashboards. Data models provide a structured and consistent way of defining and retrieving data from indexes. Data models accelerate searches by using prebuilt summaries of the data. Data models also enable the use of the tstats command, which can perform statistical analysis on the data model summaries. Data models are mapped to the Common Information Model (CIM), which provides a common language for describing data across domains and technologies. References = About data models Use the Common Information Model in Splunk Web

NEW QUESTION: 24
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 (LEAVE A REPLY)
Explanation
According to the Splunk Enterprise Security documentation, only users with the ess_admin role or the Manage All Investigations capability can delete an investigation. The investigation owner

and collaborators can edit the investigation, but not delete it. Therefore, the correct answer is A. ess_admin users only.
References = Manage investigations in Splunk Enterprise Security

NEW QUESTION: 25
What kind of value is in the red box in this picture?
A. An event priority.
B. A source ranking.
C. An IP address rating.
D. A risk score.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 26
Which of the following actions would not reduce the number of false positives from a correlation search?
A. Removing throttling fields.
B. Increasing threshold sensitivity.
C. Increasing the throttling window.
D. Reducing the severity.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 27
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 (LEAVE A REPLY)
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"."

NEW QUESTION: 28
What kind of value is in the red box in this picture?
A. A risk score.
B. A source ranking.
C. An event priority.
D. An IP address rating.
Answer: D (LEAVE A REPLY)

Explanation
The value in the red box is an IP address rating. This is a numerical value that represents the risk associated with an IP address. The higher the value, the higher the risk. This value is calculated based on the number of security events associated with the IP address, the severity of those events, and the time since the last event.
References:
Administering Splunk Enterprise Security
Splunk Enterprise security Admin
IP Intelligence

NEW QUESTION: 29
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: (SHOW ANSWER)
Explanation/Reference: https://docs.splunk.com/Documentation/ES/6.1.0/Admin/Customizemenubar#Restore_the_default_navigation

NEW QUESTION: 30
How is it possible to navigate to the ES graphical Navigation Bar editor?
A. Configure -> Navigation Menu
B. Settings -> User Interface -> Navigation Menus -> Click on "default" next to SplunkEnterpriseSecuritySuite
C. Settings -> User Interface -> Navigation -> Click on "Enterprise Security"
D. Configure -> General -> Navigation
Answer: D (LEAVE A REPLY)

NEW QUESTION: 31
Which data model populated the panels on the Risk Analysis dashboard?
A. Risk
B. Audit
C. Domain analysis
D. Threat intelligence
Answer: A (LEAVE A REPLY)
Reference:
https://docs.splunk.com/Documentation/ES/6.1.0/User/RiskAnalysis#Dashboard_panels

NEW QUESTION: 32
What are the steps to add a new column to the Notable Event table in the Incident Review dashboard?
A. Configure -> Incident Management -> Incident Review Settings -> Table Attributes
B. Configure -> Incident Management -> Notable Event Statuses
C. Configure -> Content Management -> Type: Correlation Search
D. Configure -> Incident Management -> Incident Review Settings -> Event Management
Answer: D (LEAVE A REPLY)

NEW QUESTION: 33
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: C (LEAVE A REPLY)
Explanation
A correlation search is a scheduled search that runs periodically to detect patterns of interest in the data and generate notable events or other actions when the search conditions are met. A correlation search can generate false positives, which are notable events that do not represent a real security incident or threat. False positives can create noise and reduce the efficiency and accuracy of the security analysis. To reduce false positives from a correlation search, you can modify the correlation schedule and sensitivity for your site. The correlation schedule determines how often the correlation search runs and over what time range. The sensitivity determines the threshold or limit for the search conditions to trigger a notable event. By adjusting the correlation schedule and sensitivity, you can fine-tune the correlation search to match your environment and data sources, and avoid generating notable events for normal or benign activities. You can modify the correlation schedule and sensitivity for a correlation search using the Content Management page in Splunk Enterprise Security. References = Modify the correlation schedule

and sensitivity for your site Correlation search overview for Splunk Enterprise Security Dealing with Security False Positives in Splunk (Enterprise Security ...2
Upping the Auditing Game for Correlation Searches Within ... - Splunk

NEW QUESTION: 34
Which of the following are data models used by ES? (Choose all that apply)
A. Anomalies
B. Authentication
C. Network Traffic
D. Web
Answer: B,C,D (LEAVE A REPLY)

NEW QUESTION: 35
What is the default schedule for accelerating ES Datamodels?
A. 1 minute
B. 5 minutes
C. 15 minutes
D. 1 hour
Answer: (SHOW ANSWER)
Explanation
According to the Splunk Enterprise Security documentation, the default schedule for accelerating ES data models is every 5 minutes. This means that the data model acceleration searches run every 5 minutes to summarize the newly indexed data and store the results in the tsidx files. The 5-minute schedule is recommended for most use cases, as it provides a balance between search performance and resource consumption. However, you can change the schedule of a data model acceleration search in the Content Management page of Splunk Enterprise Security, if needed. See Configure data models for Splunk Enterprise Security for more details. References = Configure data models for Splunk Enterprise Security.

NEW QUESTION: 36
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: B (LEAVE A REPLY)
Explanation
Removing throttling fields would not reduce the number of false positives from a correlation search. Throttling fields are the fields that are used to group events and suppress duplicate alerts. For example, if you use src and dest as throttling fields, then the correlation search will

only generate one alert per unique pair of src and dest values within the throttling window. This can help reduce the number of false positives by avoiding repeated alerts for the same issue. Removing throttling fields would increase the number of alerts generated by the correlation search, which could include more false positives. The other actions could help reduce the number of false positives by making the correlation search less sensitive or less frequent. Reducing the severity would lower the priority of the alerts and make them less visible. Increasing the throttling window would increase the time interval between alerts for the same issue. Increasing threshold sensitivity would make the correlation search more selective and require more evidence to trigger an alert. References = Configure correlation searches in Splunk Enterprise Security Optimizing correlation searches in Enterprise Security

NEW QUESTION: 37
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. 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.
B. Add the dashboard to a custom add-in app and install it to ES using the Content Manager.
C. Add links on the ES home page to the new dashboard.
D. Set the dashboard permissions to allow access by es_analysts and use the navigation editor to add it to the menu.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 38
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 -> Next Steps -> Nslookup
B. Configure -> Content Management -> Type: Correlation Search -> Notable -> Nslookup
C. Configure -> Content Management -> Type: Correlation Search -> Notable -> Recommended Actions -> Nslookup
D. Configure -> Type: Correlation Search -> Notable -> Recommended Actions -> Nslookup
Answer: C (LEAVE A REPLY)

NEW QUESTION: 39
Which of the following actions can improve overall search performance?
A. Add notable event suppressions for correlation searches with high numbers of false positives.
B. Increase priority of all correlation searches.
C. Reduce the frequency (schedule) of lower-priority correlation searches.
D. Disable indexed real-time search.

Answer: A,C (LEAVE A REPLY)

NEW QUESTION: 40
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. Extracting Fields.
C. Normalization to Customer Standard.
D. Normalization to the Splunk Common Information Model.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 41
What does the summariesonly=true option do for a correlation search?
A. Searches summary indexes only.
B. Searches only accelerated data.
C. Uses a default summary time range.
D. Forwards summary indexes to the indexing tier.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 42
Where is it possible to export content, such as correlation searches, from ES?
A. Settings Menu -> ES -> Export
B. Content exporter
C. Configure -> Content Management
D. Export content dashboard
Answer: C (LEAVE A REPLY)

NEW QUESTION: 43
What do threat gen searches produce?
A. Threat Intel in KV Store collections.
B. Threat correlation searches.
C. Events in the threat_activity index.
D. Threat notables in the notable index.
Answer: (SHOW ANSWER)

NEW QUESTION: 44
Which correlation search feature is used to throttle the creation of notable events?
A. Window interval.
B. Schedule windows.
C. Window duration.
D. Schedule priority.

Answer: (SHOW ANSWER)

NEW QUESTION: 45
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: (SHOW ANSWER)
Explanation
The way to navigate to the list of currently-enabled ES correlation searches is to use the Content Management page in Splunk Enterprise Security. The Content Management page allows you to view, enable, disable, and edit the content items that are included in Splunk Enterprise Security, such as correlation searches, dashboards, reports, and lookups. To access the Content Management page, you need to select Configure > Content > Content Management from the Splunk ES menu bar. Then, you can filter the content items by Type and Status to view only the correlation searches that are enabled. You can also use other filters, such as App, Domain, or Owner, to further refine your view12. References = 1: Content Management - Splunk Documentation - View content items. 2: Content Management - Splunk Documentation - Enable or disable content items.

NEW QUESTION: 46
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: (SHOW ANSWER)
Explanation
A correlation search that is set to run in real-time mode will be executed as new events are indexed. Real-time mode means that the search continuously runs over a rolling window of time, such as the last 15 minutes or the last hour. Real-time searches can detect patterns and anomalies in near real-time and trigger adaptive response actions accordingly. However, real-time searches are more resource-intensive than scheduled searches and may impact the overall performance of the system. Therefore, Splunk Enterprise Security uses indexed real-time searches by default for some correlation searches, which are more efficient than non-indexed real-time searches. You can change the search mode of a correlation search from real-time to scheduled or vice versa from the Content Management page. See Configure correlation

searches in Splunk Enterprise Security1 for more details. The other options, A, C, and D, are not correct. Always-On is not a valid search mode for correlation searches. Scheduled mode means that the search runs at a specified interval, such as every 5 minutes or every hour. Continuous mode is a deprecated search mode that is no longer supported by Splunk Enterprise Security. References = Configure correlation searches in Splunk Enterprise Security

NEW QUESTION: 47
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 (LEAVE A REPLY)
Reference:
https://docs.splunk.com/Documentation/AddonBuilder/3.0.1/UserGuide/Overview

NEW QUESTION: 48
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 (LEAVE A REPLY)
Explanation/Reference:
https://docs.splunk.com/Documentation/ES/6.1.0/User/EndpointProtectionDomaindashboards

NEW QUESTION: 49
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 (LEAVE A REPLY)
Explanation/Reference: https://answers.splunk.com/answers/565482/how-to-resolve-skipped-scheduled-searches.html

NEW QUESTION: 50
When ES content is exported, an app with a .splextension is automatically created.
What is the best practice when exporting and importing updates to ES content?
A. Do not use the .splextension when naming an export.
B. Either use new app names or always include both existing and new content.
C. Use new app names each time content is exported.
D. Always include existing and new content for each export.
Answer: (SHOW ANSWER)

NEW QUESTION: 51
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: (SHOW ANSWER)
Explanation/Reference: https://answers.splunk.com/answers/790783/anti-tampering-features-to-protect-splunk-logs- the.html

NEW QUESTION: 52
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: C (LEAVE A REPLY)
Explanation
According to the Splunk Enterprise Security documentation, the recommended way to install ES is on a server with a new install of Splunk. This is because ES requires a dedicated search head that is not shared with other apps or users. Installing ES on a server with a new install of Splunk ensures that there are no conflicts or performance issues with other apps or configurations. If you want to install ES on an existing search head, you need to follow some additional steps,

such as redirecting distributed search connections, purging KV Store, and backing up existing data. See Install Splunk Enterprise Security for more details. Therefore, the correct answer is C. On a server with a new install of Splunk. References = Install Splunk Enterprise Security.

NEW QUESTION: 53
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.
Answer: D (LEAVE A REPLY)
Explanation/Reference:
https://docs.splunk.com/Documentation/ES/6.4.1/Install/Planyourdatainputs

NEW QUESTION: 54
Which of the following are examples of sources for events in the endpoint security domain dashboards?
A. Lifecycle auditing of incidents, from assignment to resolution.
B. REST API invocations.
C. Investigation final results status.
D. Workstations, notebooks, and point-of-sale systems.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 55
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: (SHOW ANSWER)
Explanation/Reference:

NEW QUESTION: 56
Which of the following is an adaptive action that is configured by default for ES?
A. Create notable event
B. Create investigation
C. Create new asset
D. Create new correlation search
Answer: D (LEAVE A REPLY)

NEW QUESTION: 57
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. Increase memory and CPUs on the search head(s) and add additional indexers.
B. Add heavy forwarders between the universal forwarders and indexers so inputs can be parsed before indexing.
C. Change the search heads to do local indexing of summary searches.
D. If indexed realtime search is enabled, disable it for the notable index.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 58
To which of the following should the ES application be uploaded?
A. The KV Store.
B. The dedicated forwarder.
C. The indexer.
D. The search head.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 59
What kind of value is in the red box in this picture?
A. An event priority.
B. An IP address rating.
C. A risk score.
D. A source ranking.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 60
Which of the following are the default ports that must be configured for Splunk Enterprise Security to function?
A. SplunkWeb (8000), Splunk Management (8089), KV Store (8191)
B. SplunkWeb (8088), Splunk Management (8089), KV Store (8000)
C. SplunkWeb (8043), Splunk Management (8088), KV Store (8191)
D. SplunkWeb (8386), Splunk Management (8926), KV Store (8106)
Answer: (SHOW ANSWER)
Explanation/Reference:
https://docs.splunk.com/Documentation/Splunk/8.1.2/Security/SecureSplunkonyournetwork

NEW QUESTION: 61

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 (LEAVE A REPLY)
Reference:
https://docs.splunk.com/Documentation/ES/6.1.0/Admin/Customizemenubar#Restore_the_default_navigation

NEW QUESTION: 62
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 (LEAVE A REPLY)
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

NEW QUESTION: 63
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 (LEAVE A REPLY)
Reference:
https://docs.splunk.com/Documentation/ITSI/4.4.2/Install/Plan

NEW QUESTION: 64
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. Either use new app names or always include both existing and new content.
D. Always include existing and new content for each export.
Answer: C (LEAVE A REPLY)
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.

NEW QUESTION: 65
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. User Intelligence
C. Threat Intelligence
Section: (none)
Explanation
D. Protocol Analysis
Answer: (SHOW ANSWER)

NEW QUESTION: 66
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. Delete the non-CIM-compliant apps from the search head, then install ES.
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. Install ES on the existing search head.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 67
Which data model populated the panels on the Risk Analysis dashboard?

A. Risk
B. Audit
C. Domain analysis
D. Threat intelligence
Answer: A (LEAVE A REPLY)
Explanation
The Risk Analysis dashboard uses the Risk data model to populate the panels. The Risk data model is a data model that contains information about the risk scores and risk modifiers of various objects, such as systems, users, hashes, and network artifacts. The Risk data model accelerates these fields for the Risk Analysis and Incident Review dashboards. The Risk data model also handles case insensitive asset and identity correlation, allowing risk modifiers that are applied to system or user name variants to be correctly attributed to the same risk_object1. The other options, B, C, and D, are not correct. The Audit data model contains information about audit events, such as user logins, password changes, and system access. The Domain Analysis data model contains information about the domains that are visited by the systems in the network. The Threat Intelligence data model contains information about the threat intelligence sources, indicators, and matches. References = Risk Analysis dashboard Risk data model Risk Analysis framework

NEW QUESTION: 68
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: (SHOW ANSWER)
Explanation/Reference:
https://docs.splunk.com/Documentation/ES/6.1.0/Install/InstallEnterpriseSecurity

NEW QUESTION: 69
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: D (LEAVE A REPLY)
Explanation
Detailed information about identities, such as user names, email addresses, phone numbers, and roles, is stored in the Identity Lookup CSV file in Splunk Enterprise Security. The Identity Lookup CSV file is a lookup file that contains the identity data that is collected and extracted from various data sources, such as Active Directory, LDAP, or custom identity lists. The Identity

Lookup CSV file is used to enrich events with identity information and generate notable events based on identity correlation searches. You can view and manage the Identity Lookup CSV file using the Asset and Identity Management page in Splunk Enterprise Security.
References =
Manage assets and identities in Splunk Enterprise Security
Identity Lookup CSV file

NEW QUESTION: 70
Adaptive response action history is stored in which index?
A. modular_history
B. cim_modactions
C. modular_action_history
D. cim_adaptiveactions
Answer: B (LEAVE A REPLY)

NEW QUESTION: 71
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. Modify the correlation schedule and sensitivity for your site.
B. Suppress notable events from that correlation search.
C. Change the correlation search's default status and severity.
D. Disable acceleration for the correlation search to reduce storage requirements.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 72
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 (LEAVE A REPLY)
Explanation/Reference:
https://docs.splunk.com/Documentation/ES/6.4.1/User/Takeactiononanotableevent

NEW QUESTION: 73
Which argument to the | tstats command restricts the search to summarized data only?
A. summariesonly=t
B. summaries=all
C. summariesonly=all

D. summaries=t
Answer: A (LEAVE A REPLY)

NEW QUESTION: 74
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 (LEAVE A REPLY)
Explanation
According to the Splunk Enterprise Security documentation, the way to make the Threat Activity dashboard the default landing page in ES is to use the Edit Navigation page and click the 'Set this as the default view' checkmark for Threat Activity. The Edit Navigation page allows you to customize the menu bar of ES and add links to custom dashboards, reports, or other views. You can also set the default view for each app context, which determines the landing page when you open the app. To set the Threat Activity dashboard as the default view, you need to do the following steps:
On the Enterprise Security menu bar, select Configure > General > Navigation.
In the Edit Navigation page, select the Enterprise Security app context from the drop-down menu.
In the Navigation XML section, find the line that contains the view name 'threat_activity'.
Add the attribute default="true" to the line and remove the same attribute from any other line in the same app context.
Click Save Changes to apply the changes to the Edit Navigation page.
This will make the Threat Activity dashboard the default landing page when you open the Enterprise Security app. See Customize the navigation bar for more details.
The other options are not the correct ways to make the Threat Activity dashboard the default landing page in ES. Dragging and dropping the Threat Activity view to the top of the page will not change the default view, but only the order of the menu items. Selecting Enterprise Security as the default application will not change the default view within the app, but only the app that opens when you log in to Splunk. Editing the Threat Activity view settings will not change the default view, but only the title, description, permissions, and schedule of the dashboard.
Therefore, the correct answer is C. From the Edit Navigation page, click the 'Set this as the default view" checkmark for Threat Activity. References = Customize the navigation bar.

NEW QUESTION: 75
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: (SHOW ANSWER)
Explanation
According to the Splunk Enterprise Security Admin documentation, the minimum hardware requirements for a dedicated search head running ES are as follows: OS: 64 bit, RAM: 32 GB, CPU: 16 cores. These requirements are based on the assumption that the search head is not performing any other tasks besides running ES. The documentation also recommends having at least 500 GB of disk space for the search head.
References = Splunk Enterprise Security Admin documentation

NEW QUESTION: 76
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 (LEAVE A REPLY)
Explanation
When exporting and importing updates to ES content, you should follow the best practices described in the Splunk Enterprise Security Admin documentation1. One of the best practices is to avoid overwriting existing content on the destination system. To do this, you have two options: either use new app names each time you export content, or always include both existing and new content in each export. This way, you can preserve the original content and avoid conflicts or data loss. The other options, A, B, and C, are not correct. Using new app names each time content is exported is only one of the options, not the only one. Using the .spl extension when naming an export is not a problem, as it is the default extension for Splunk apps. Including only new content for each export is not a good practice, as it may overwrite existing content on the destination system.
References =
Export content from Splunk Enterprise Security as an app

NEW QUESTION: 77
At what point in the ES installation process should Splunk_TA_ForIndexes.spl be deployed to the indexers?
A. After installing ES on the search head(s) and running the distributed configuration management tool.
B. When adding apps to the deployment server.
C. Splunk_TA_ForIndexers.spl is only installed on indexer cluster sites using the cluster master and the splunk apply cluster-bundle command.
D. Splunk_TA_ForIndexers.spl is installed first.
Answer: (SHOW ANSWER)

NEW QUESTION: 78
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 (LEAVE A REPLY)
Explanation
The Threat Download Manager is a feature of Splunk Enterprise Security that downloads threat intelligence data from a web server. The Threat Download Manager is a modular input that runs on a schedule and fetches threat intelligence data from various sources, such as STIX/TAXII servers, RSS feeds, or custom URLs. The Threat Download Manager then passes the downloaded data to the Threat Intelligence Parser for further processing12. References = 1: Add threat intelligence to Splunk Enterprise Security - Splunk Documentation - Configure the threat intelligence sources included with Splunk Enterprise Security. 2: Using threat intelligence in Splunk Enterprise Security - Splunk Lantern - Where do I get threat intelligence?

NEW QUESTION: 79
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 (LEAVE A REPLY)
Explanation

Splunk Enterprise Security knows the local customer domain names so it can detect internal vs. external emails by using the Corporate Web and Email Domain Lookups. These are lookup files that contain the list of domains that are considered internal or corporate for the organization. The Corporate Web and Email Domain Lookups are edited during the initial configuration of Splunk Enterprise Security, and they are used to enrich events with the tag=internal_web or tag=internal_email fields. These fields indicate whether the web or email activity is internal or external, and they are used by dashboards and correlation searches in Splunk Enterprise Security to monitor and analyze the web and email traffic. References = Corporate Web and Email Domain Lookups Configure web and email domains in Splunk Enterprise Security Detecting Typosquatting, Phishing, and Corporate Espionage ... - Splunk

NEW QUESTION: 80
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: D (LEAVE A REPLY)

NEW QUESTION: 81
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 (LEAVE A REPLY)
Explanation
To navigate to the ES graphical Navigation Bar editor, you need to click the Configure menu in the ES app bar, then select General, and then select Navigation. The Navigation page allows you to customize the navigation bar of the ES app by adding, removing, or reordering the menu items. You can also edit the labels, icons, and links of the menu items. You can use the graphical editor to drag and drop the menu items, or you can edit the navigation XML directly. For more information, see Customize the navigation bar in Splunk Enterprise Security1. The other options, A, C, and D, are not correct. There is no Navigation Menu option under the Configure menu. The Settings menu does not allow you to edit the navigation bar of the ES app. The Settings menu only allows you to edit the navigation menus of the Splunk platform, such as the app launcher and the user menu. References = Customize the navigation bar in Splunk Enterprise Security Design navigation graphs | Android Developers1
Design navigation graphs | Android Developers

NEW QUESTION: 82
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: (SHOW ANSWER)
Explanation/Reference:
https://docs.splunk.com/Documentation/ES/6.1.0/Admin/Customizenotables

NEW QUESTION: 83
Which of the following threat intelligence types can ES download? (Choose all that apply)
A. Text
B. STIX/TAXII
C. VulnScanSPL
D. SplunkEnterpriseThreatGenerator
Answer: B (LEAVE A REPLY)
Explanation/Reference:
https://docs.splunk.com/Documentation/ES/6.1.0/Admin/Downloadthreatfeed

NEW QUESTION: 84
The option to create a Short ID for a notable event is located where?
A. The Contributing Events.
B. The Event Details.
C. The Additional Fields.
D. The Description.
Answer: B (LEAVE A REPLY)
https://docs.splunk.com/Documentation/ES/6.4.1/User/Takeactiononanotableevent

NEW QUESTION: 85
Which of the following is a recommended pre-installation step?
A. Install the latest Python distribution on the search head.
B. Configure search head forwarding.
C. Disable the default search app.
D. Download the latest version of KV Store from MongoDB.com.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 86
Both "Recommended Actions" and "Adaptive Response Actions" use adaptive response. How do they differ?

A. Recommended Actions show a textual description to an analyst, Adaptive Response Actions show them encoded.
B. Recommended Actions show a list of Adaptive Responses to an analyst, Adaptive Response Actions run them automatically.
C. Recommended Actions show a list of Adaptive Responses that have already been run, Adaptive Response Actions run them automatically.
D. Recommended Actions show a list of Adaptive Responses to an analyst, Adaptive Response Actions run manually with analyst intervention.
Answer: B (LEAVE A REPLY)
Explanation
Recommended Actions show a list of Adaptive Responses to an analyst, which are possible actions that can be taken in response to a notable event. Adaptive Response Actions run automatically when a correlation search triggers a notable event, and can perform actions such as sending an email, adding a comment, or modifying a risk score. Recommended Actions are configured in the correlation search editor, while Adaptive Response Actions are configured in the alert actions manager. References = Included adaptive response actions with Splunk Enterprise Security Set up Adaptive Response actions in Splunk Enterprise Security Configure adaptive response actions for a correlation search in Splunk Enterprise Security

NEW QUESTION: 87
When investigating, what is the best way to store a newly-found IOC?
A. Add it in a text note to the investigation.
B. Click the "Add IOC" button.
C. Click the "Add Artifact" button.
D. Paste it into Notepad.
Answer: (SHOW ANSWER)

NEW QUESTION: 88
Which two fields combine to create the Urgency of a notable event?
A. Priority and Severity.
B. Priority and Criticality.
C. Precedence and Time.
D. Criticality and Severity.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 89
What is the default schedule for accelerating ES Datamodels?
A. 15 minutes
B. 1 minute
C. 5 minutes
D. 1 hour

Answer: C (LEAVE A REPLY)

NEW QUESTION: 90
If a username does not match the 'identity' column in the identities list, which column is checked next?
A. Email.
B. Nickname
C. Combination of Last Name, First Name.
D. IP address.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 91
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 (LEAVE A REPLY)
Explanation/Reference:
https://dev.splunk.com/enterprise/docs/developapps/enterprisesecurity/planintegrationes/

NEW QUESTION: 92
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 (LEAVE A REPLY)
Explanation
The urgency of a notable event is a value that indicates how important or urgent the event is for investigation and response. The urgency of a notable event is determined by two fields: the

priority and the severity. The priority is a value that is assigned to an asset or an identity based on how critical or valuable it is for the organization. The priority can be unknown, low, medium, high, or critical. The severity is a value that is assigned to a notable event based on how serious or harmful the event is for the security posture. The severity can be unknown, informational, low, medium, high, or critical. The urgency of a notable event is calculated by combining the priority and the severity values using a lookup table called urgency_lookup. The urgency can be informational, low, medium, high, or critical. You can use the urgency field to prioritize the investigation of notable events in Splunk Enterprise Security. References = How urgency is assigned to notable events in Splunk Enterprise Security Priority and severity in Splunk Enterprise Security

NEW QUESTION: 93
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. Protocol Analysis
B. Intrusion Center
C. User Intelligence
D. Threat Intelligence
Answer: (SHOW ANSWER)

NEW QUESTION: 94
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: (SHOW ANSWER)
Explanation
Explanation/Reference:
https://docs.splunk.com/Documentation/ES/6.1.0/Admin/Customizenotables

NEW QUESTION: 95
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 (LEAVE A REPLY)

Explanation/Reference:

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

NEW QUESTION: 96

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 (LEAVE A REPLY)

Explanation/Reference: https://www.splunk.com/pdfs/technical-briefs/splunk-validated-architectures.pdf

NEW QUESTION: 97

Where should an ES search head be installed?

A. On a Splunk server with top level visibility.

B. On a Splunk server running Splunk DB Connect.

C. On any Splunk server.

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

Answer: D (LEAVE A REPLY)

NEW QUESTION: 98

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 (LEAVE A REPLY)

Explanation

According to the Splunk Enterprise Security documentation, the default ports that must be configured for Splunk Enterprise Security to function are the following:

SplunkWeb (8000): This port provides the socket for Splunk Web, the web interface for Splunk Enterprise Security. It allows you to access the dashboards, reports, alerts, and other features of Splunk Enterprise Security from your browser. You can change this port in the web.conf file or by using the splunk set web-port command.

Splunk Management (8089): This port is used to communicate with the splunkd daemon, the main process that runs Splunk Enterprise Security. Splunk Web talks to splunkd on this port, as does the command line interface, and any distributed connections from other servers. This port also provides the REST API endpoint for Splunk Enterprise Security. You can change this port in the server.conf file or by using the splunk set splunkd-port command.
KV Store (8191): This port is used by the KV Store, a MongoDB-based service that stores key-value pairs of data for Splunk Enterprise Security. The KV Store is used to store and manage data for various features of Splunk Enterprise Security, such as asset and identity correlation, threat intelligence, adaptive response, and investigations. You can change this port in the server.conf file.
Therefore, the correct answer is C. SplunkWeb (8000), Splunk Management (8089), KV Store (8191).
References =
Change default values
KV Store overview

NEW QUESTION: 99
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: (SHOW ANSWER)
Explanation
The correct answer is B. Normalize data. The Add-on Builder can configure a new add-on to normalize data by mapping the data fields to the Common Information Model (CIM). The CIM provides a common language for describing data across domains and technologies. Normalizing data enables the data to be used by other Splunk apps, such as Splunk Enterprise Security and Splunk IT Service Intelligence. The Add-on Builder can also configure other features in a new add-on, such as collecting data from various sources, extracting fields from the data, creating alert actions and adaptive response actions, and testing and validating the add-on.
However, the Add-on Builder cannot configure an add-on to expire data, summarize data, or translate data.
These are not features of the Add-on Builder. References =
Splunk Add-on Builder
[Use the Common Information Model in Splunk Web]

NEW QUESTION: 100
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: (SHOW ANSWER)
Explanation
When investigating an incident in Splunk Enterprise Security, the best way to store a newly-found IOC (indicator of compromise) is to click the "Add Artifact" button. This button allows you to add an artifact to the current investigation from any dashboard or search result. An artifact is a piece of machine data that indicates risk, such as an IP address, a domain name, a file hash, or a user name. By adding an artifact to the investigation, you can enrich the context of the incident, track the artifact across multiple data sources, and share the artifact with other analysts. You can also use the artifact to create a threat intelligence indicator, which can be used to detect and alert on future threats12. References = 1: Add artifacts to an investigation - Splunk Documentation. 2: About investigations in Splunk Enterprise Security - Splunk Documentation.

NEW QUESTION: 101
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 (LEAVE A REPLY)
Reference:
the.html

NEW QUESTION: 102
How is it possible to navigate to the list of currently-enabled ES correlation searches?
A. Configure -> Content Management -> Select Type "Correlation" and Status "Enabled"
B. Configure -> Correlation Searches -> Select Status "Enabled"
C. Settings -> Searches, Reports, and Alerts -> Select App of "SplunkEnterpriseSecuritySuite" and filter by "- Rule"
D. Settings -> Searches, Reports, and Alerts -> Filter by Name of "Correlation"
Answer: A (LEAVE A REPLY)

NEW QUESTION: 103
What kind of value is in the red box in this picture?
A. A risk score.
B. A source ranking.
C. An event priority.
D. An IP address rating.

Answer: (SHOW ANSWER)
Reference:
https://docs.splunk.com/Documentation/Splunk/8.0.2/Data/FormateventsforHTTPEventCollector

NEW QUESTION: 104
What are adaptive responses triggered by?
A. By correlation searches and custom tech add-ons.
B. By custom tech add-ons and users on the risk analysis dashboard.
C. By correlation searches and users on the incident review dashboard.
D. By correlation searches and users on the threat analysis dashboard.
Answer: (SHOW ANSWER)