Splunk.SPLK-3001.v2022-08-26.q32

Exam Code:	SPLK-3001
Exam Name:	Splunk Enterprise Security Certified Admin Exam
Certification Provider:	Splunk
Free Question Number:	32
Version:	v2022-08-26
# of views:	457
# of Questions views:	2631
https://www.freecram.net/torrent/Splunk.SPLK-3001.v2022-08-26.q32.html	

NEW QUESTION: 1
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. Run the correct search.
C. Apply the correct tags.
D. Visit the CIM dashboard.
Answer: (SHOW ANSWER)

NEW QUESTION: 2
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/system/local/
B. $SPLUNK_HOME/var/run/searchpeers/
C. $SPLUNK_HOME/etc/shcluster/apps
D. $SPLUNK_HOME/etc/master-apps/
Answer: (SHOW ANSWER)
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: 3

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

NEW QUESTION: 4
Glass tables can display static images and text, the results of ad-hoc searches, and which of the following objects?
A. Metrics store searches.
B. Lookup searches.
C. Summarized data.
D. Security metrics.
Answer: (SHOW ANSWER)

NEW QUESTION: 5
Which of the following is a Web Intelligence dashboard?
A. stream :http Protocol dashboard
B. HTTP Category Analysis
C. Network Center
D. Endpoint Center
Answer: (SHOW ANSWER)

NEW QUESTION: 6
Where are attachments to investigations stored?
A. notable index
B. <splunk_home>/etc/apps/SA-Investigations/default/ui/views/attachments
C. attachments.csv lookup
D. KV Store
Answer: (SHOW ANSWER)

NEW QUESTION: 7
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 Resposes to an analyst, Adaptive Response Actions run manually with analyst intervention.

D. Recommended Actions show a list of Adaptive Responses that have already been run, Adaptive Response Actions run them automatically.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 8
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. Protocol Intelligence dashboards.
B. User Intelligence dashboards.
C. Endpoint dashboards.
D. Web Intelligence dashboards.
Answer: (SHOW ANSWER)

NEW QUESTION: 9
Where is detailed information about identities stored?
A. The Access Anomalies collection.
B. The User Activity index.
C. The Identity Lookup CSV file.
D. The Identity Investigator index.
Answer: (SHOW ANSWER)

NEW QUESTION: 10
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 -> Recommended Actions -> 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 -> Nslookup
Answer: (SHOW ANSWER)

NEW QUESTION: 11
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: (SHOW ANSWER)
https://docs.splunk.com/Documentation/ES/6.4.1/User/Takeactiononanotableevent

NEW QUESTION: 12
"10.22.63.159", "websvr4", and "00:26:08:18: CF:1D" would be matched against what in ES?
A. A user.
B. An identity.
C. An asset.
D. A device.
Answer: (SHOW ANSWER)

NEW QUESTION: 13
Which of the following is a key feature of a glass table?
A. Strong data for later retrieval.
B. Customization.
C. Rigidity.
D. Interactive investigations.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 14
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. If indexed realtime search is enabled, disable it for the notable index.
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. Increase memory and CPUs on the search head(s) and add additional indexers.
Answer: (SHOW ANSWER)

NEW QUESTION: 15
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 threat analysis dashboard.
D. By correlation searches and users on the incident review dashboard.
Answer: (SHOW ANSWER)

NEW QUESTION: 16
Which column in the Asset or Identity list is combined with event security to make a notable event's urgency?
A. VIP
B. Criticality
C. Importance
D. Priority
Answer: (SHOW ANSWER)

NEW QUESTION: 17
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: (SHOW ANSWER)

NEW QUESTION: 18
What is an example of an ES asset?
A. People
B. MAC address
C. Server
D. User name
Answer: (SHOW ANSWER)

NEW QUESTION: 19
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: (SHOW ANSWER)

NEW QUESTION: 20
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. Extracting Fields.
B. Normalization to the Splunk Common Information Model.
C. Normalization to Customer Standard.
D. Applying Tags.
Answer: (SHOW ANSWER)

NEW QUESTION: 21
What feature of Enterprise Security downloads threat intelligence data from a web server?
A. Threat Download Manager
B. Therat Intelligence Enforcement
C. Threat Intelligence Parser
D. Threat Service Manager
Answer: (SHOW ANSWER)
"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: 22
Which of the following is part of tuning correlation searches for a new ES installation?
A. Configuring correlation result storage.
B. Configuring correlation adaptive responses.
C. Configuring correlation notable event index.
D. Configuring correlation permissions.
Answer: (SHOW ANSWER)

NEW QUESTION: 23
How is it possible to specify an alternate location for accelerated storage?
A. Configure storage optimization settings for the index.
B. Use the tstatsHomePath Setting in indexes, conf
C. Update the Home Path setting in indexes, conf
D. Use the tstatsHomePath setting in props, conf
Answer: (SHOW ANSWER)

NEW QUESTION: 24
Which of the following is a recommended pre-installation step?
A. Download the latest version of KV Store from MongoDBxom.
B. Install the latest Python distribution on the search head.
C. Configure search head forwarding.
D. Disable the default search app.
Answer: (SHOW ANSWER)

NEW QUESTION: 25
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. Make sure the Authentication data model contains up-to-date events and is properly accelerated.
B. Configuring user and website watchlists so the User Activity dashboard will highlight unwanted user actions.
C. Configuring the identities lookup with user details to enrich notable event Information for forensic analysis.
D. Use the Access Anomalies dashboard to identify unusual protocols being used to access corporate sites.
Answer: (SHOW ANSWER)

NEW QUESTION: 26
ES needs to be installed on a search head with which of the following options?
A. Any other apps installed.
B. All apps removed except for TA-*.
C. Only default built-in and CIM-compliant apps.
D. No other apps.
Answer: (SHOW ANSWER)

NEW QUESTION: 27
What tools does the Risk Analysis dashboard provide?
A. Notable event domains displayed by risk score.
B. High risk threats.
C. A display of the highest risk assets and identities.
D. Key indicators showing the highest probability correlation searches in the environment.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 28
Which of the following are examples of sources for events in the endpoint security domain dashboards?

A. Investigation final results status.
B. REST API invocations.
C. Workstations, notebooks, and point-of-sale systems.
D. Lifecycle auditing of incidents, from assignment to resolution.
Answer: (SHOW ANSWER)

NEW QUESTION: 29
Which of the following actions may be necessary before installing ES?
A. Redirect distributed search connections.
B. Add additional indexers.
C. Purge KV Store.
D. Add additional forwarders.
Answer: (SHOW ANSWER)

NEW QUESTION: 30
Which of the following are data models used by ES? (Choose all that apply)
A. Anomalies
B. Web
C. Authentication
D. Network Traffic
Answer: (SHOW ANSWER)

NEW QUESTION: 31
Which setting is used in indexes.conf to specify alternate locations for accelerated storage?
A. summaryHomePath
B. tstatsHomePath
C. thawedPath
D. warmToColdScript
Answer: B (LEAVE A REPLY)

NEW QUESTION: 32
What should be used to map a non-standard field name to a CIM field name?

A. Field alias.
B. Tag.
C. Eventtype.
D. Search time extraction.
Answer: (SHOW ANSWER)