100% Updated Splunk SPLK-3001 Enterprise PDF Dumps [Q14-Q34

100% Updated Splunk SPLK-3001 Enterprise PDF Dumps
Use Valid Exam SPLK-3001 by VCEPrep Books For Free Website

Achieving the Splunk SPLK-3001 certification can help IT professionals advance their careers in the field of security operations. Splunk Enterprise Security Certified Admin Exam certification is recognized by employers and demonstrates that candidates have the knowledge and skills needed to effectively manage security incidents and threats using Splunk Enterprise Security.

Splunk SPLK-3001 certification exam is a vendor-neutral certification that is recognized globally. Splunk Enterprise Security Certified Admin Exam certification validates an individual's ability to deploy, manage, and administer Splunk Enterprise Security to protect an organization's assets against potential security threats. By passing the Splunk SPLK-3001 exam, IT professionals can demonstrate their commitment to their profession, their dedication to their craft, and their willingness to go the extra mile to ensure the security of their organization.

NEW QUESTION 14

When using distributed configuration management to create the Splunk_TA_ForIndexerspackage, which three files can be included?
- indexes.conf, props.conf, transforms.conf
- web.conf, props.conf, transforms.conf
- inputs.conf, props.conf, transforms.conf
- eventtypes.conf, indexes.conf, tags.conf

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

NEW QUESTION 15

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?
- OS: 32 bit, RAM: 16 MB, CPU: 12 cores
- OS: 64 bit, RAM: 32 MB, CPU: 12 cores
- OS: 64 bit, RAM: 12 MB, CPU: 16 cores
- OS: 64 bit, RAM: 32 MB, CPU: 16 cores

NEW QUESTION 16

An administrator wants to ensure that none of the ES indexed data could be compromised through tampering.

What feature would satisfy this requirement?
- Index consistency.
- Data integrity control.
- Indexer acknowledgement.
- Index access permissions.

Explanation

Data integrity control is a feature of Splunk Enterprise that helps you verify the integrity of data that it indexes. When you enable data integrity control for an index, Splunk Enterprise computes hashes on every slice of data using the SHA-256 algorithm. It then stores those hashes so that you can verify the integrity of your data later. This feature prevents data tampering and ensures that the data is trustworthy and reliable.

Therefore, the correct answer is B. Data integrity control. References = Manage data integrity &#8211; Splunk Documentation.

NEW QUESTION 17

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?
- Endpoint dashboards.
- User Intelligence dashboards.
- Protocol Intelligence dashboards.
- Web Intelligence dashboards.

NEW QUESTION 18

What does the risk framework add to an object (user, server or other type) to indicate increased risk?

* An urgency.
* A risk profile.
* An aggregation.
* A numeric score.

Reference:

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

NEW QUESTION 19

How is notable event urgency calculated?

* Asset priority and threat weight.
* Alert severity found by the correlation search.
* Asset or identity risk and severity found by the correlation search.
* Severity set by the correlation search and priority assigned to the associated asset or identity.

Reference:

https://docs.splunk.com/Documentation/ES/6.1.0/User/Howurgencyisassigned

NEW QUESTION 20

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

* Only correlation searches, managed lookups, and glass tables.
* Only correlation searches.
* Any content type listed in the Content Management page.
* Only correlation searches, glass tables, and workbench panels.

NEW QUESTION 21

What does the Security Posture dashboard display?

* Active investigations and their status.
* A high-level overview of notable events.
* Current threats being tracked by the SOC.
* A display of the status of security tools.

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 22

ES needs to be installed on a search head with which of the following options?

* No other apps.
* Any other apps installed.
* All apps removed except for TA-*.
* Only default built-in and CIM-compliant apps.

NEW QUESTION 23

Where should an ES search head be installed?

* On a Splunk server running Splunk DB Connect.
* On a Splunk server with top level visibility.
* On a server with a new install of Splunk.
* On any Splunk server.

NEW QUESTION 24

Who can delete an investigation?
* ess_admin users only.
* The investigation owner only.
* The investigation owner and ess-admin.
* The investigation owner and collaborators.
Reference:

https://docs.splunk.com/Documentation/ES/6.1.0/Admin/Manageinvestigations

NEW QUESTION 25

Which of the following would allow an add-on to be automatically imported into Splunk Enterprise Security?
* A prefix of CIM_
* A suffix of .spl
* A prefix of TECH_
* A prefix of Splunk_TA_
Reference:

https://dev.splunk.com/enterprise/docs/developapps/enterprisesecurity/planintegrationes/

NEW QUESTION 26

When installing Enterprise Security, what should be done after installing the add-ons necessary for normalizing data?
* Configure the add-ons according to their README or documentation.
* Disable the add-ons until they are ready to be used, then enable the add-ons.
* Nothing, there are no additional steps for add-ons.
* Configure the add-ons via the Content Management dashboard.

NEW QUESTION 27

What do threat gen searches produce?
* Threat correlation searches.
* Threat Intel in KV Store collections.
* Threat notables in the notable index.
* Events in the threat_activity index.
https://docs.splunk.com/Documentation/ES/6.4.1/Admin/Createthreatmatchspecs

NEW QUESTION 28

What is an example of an ES asset?
* MAC address
* User name
* Server

* People
Explanation

According to the Splunk Enterprise Security documentation, an asset is a physical or logical device that is part of your network infrastructure, such as a server, a workstation, a router, or a firewall. An asset can have various attributes, such as IP address, MAC address, DNS name, NT host name, priority, business unit, owner, and others. Splunk Enterprise Security uses asset data to enrich and correlate security events and provide context for analysis. You can manage asset data using the Asset and Identity Management page in Splunk Enterprise Security. See Manage assets and identities in Splunk Enterprise Security for more details.

The other options are not examples of ES assets, but they may be related to other types of data. A MAC address is an attribute of an asset, not an asset itself. A user name is an example of an identity, which is a person or group that is associated with an asset or an event. Splunk Enterprise Security uses identity data to enrich and correlate security events and provide context for analysis. You can manage identity data using the Asset and Identity Management page in Splunk Enterprise Security. See Manage assets and identities in Splunk Enterprise Security for more details. People is a data model in the Splunk Common Information Model (CIM), which provides a common standard for organizing and naming data fields across different data sources.

Splunk Enterprise Security uses the CIM to enable cross-source analysis and correlation of security events.

The People data model contains the fields and tags for events that are related to people, such as user names, email addresses, phone numbers, and others. See People for more details. Therefore, the correct answer is C.

Server. References =

Manage assets and identities in Splunk Enterprise Security

People

NEW QUESTION 29

Which indexes are searched by default for CIM data models?
* notable and default
* summary and notable
* _internal and summary
* All indexes
Explanation/Reference: https://answers.splunk.com/answers/600354/indexes-searched-by-cim-data-models.html

NEW QUESTION 30

What is the first step when preparing to install ES?
* Install ES.
* Determine the data sources used.
* Determine the hardware required.
* Determine the size and scope of installation.

NEW QUESTION 31

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.

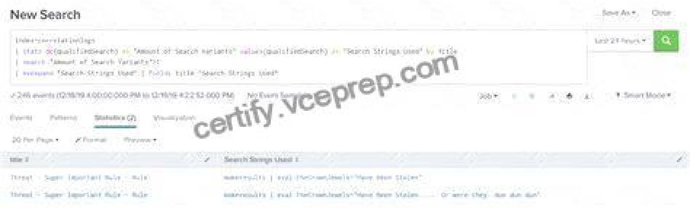
What is a solution for this issue?

- Suppress notable events from that correlation search.
- Disable acceleration for the correlation search to reduce storage requirements.
- Modify the correlation schedule and sensitivity for your site.
- Change the correlation search&#8217;s default status and severity.

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 &#8230;2

Upping the Auditing Game for Correlation Searches Within &#8230; &#8211; Splunk



```
index=correlationlogs
| stats dc(qualifiedSearch) as "Amount of Search Variants" values(qualifiedSearch) as "Search Strings Used" by title
| search "Amount of Search Variants">1
| mvexpand "Search Strings Used" | fields title "Search Strings Used"
```

✓ 246 events (12/18/19 4:00:00.000 PM to 12/19/19 4:22:52.000 PM) No Event Sampling

title	Search Strings Used
Threat - Super Important Rule - Rule	makeresults | eval TheCrownJewels="Have Been Stolen"
Threat - Super Important Rule - Rule	makeresults | eval TheCrownJewels="Have Been Stolen.... Or were they. dun dun dun"

NEW QUESTION 32

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

- Always-On
- Real-Time
- Scheduled
- Continuous

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 33

Which of the following features can the Add-on Builder configure in a new add-on?
* Expire data.
* Normalize data.
* Summarize data.
* Translate data.

NEW QUESTION 34

When installing Enterprise Security, what should be done after installing the add-ons necessary for normalizing data?
* Configure the add-ons according to their README or documentation.
* Disable the add-ons until they are ready to be used, then enable the add-ons.
* Nothing, there are no additional steps for add-ons.
* Configure the add-ons via the Content Management dashboard.
Explanation

After installing the add-ons necessary for normalizing data, you should configure the add-ons according to their README or documentation. The add-ons that are included in the Splunk Enterprise Security package are preconfigured and do not require additional steps. However, the add-ons that are downloaded separately from Splunkbase may require additional configuration steps, such as enabling inputs, setting up credentials, or modifying props and transforms. You should review the README or documentation for each add-on to determine the specific configuration requirements and follow the instructions accordingly.
References = Deploy add-ons to Splunk Enterprise Security About installing Splunk add-ons

What is a Splunk SPLK-3001?

A Splunk SPLK-3001 certification is an indication that an individual has mastered the fundamental knowledge in all aspects of running and managing a Splunk Enterprise deployment. As a Splunk SPLK-3001 certified engineer, you will be able to address issues on demand and scale the Splunk Enterprise deployment for maximum performance, scalability and availability.

Splunk SPLK-3001 Official Cert Guide PDF: https://www.vceprep.com/SPLK-3001-latest-vce-prep.html]