Splunk

Exam Questions SPLK-3001

Splunk Enterprise Security Certified Admin Exam

About Exambible

Your Partner of IT Exam

Found in 1998

Exambible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, Exambible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1
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

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

NEW QUESTION 2
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

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

NEW QUESTION 3
What does the risk framework add to an object (user, server or other type) to indicate increased risk?

A. An urgency.
B. A risk profile.
C. An aggregation.
D. A numeric score.

Answer: C

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

NEW QUESTION 4
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: B

NEW QUESTION 5
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: A

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

NEW QUESTION 6
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

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

NEW QUESTION 7
At what point in the ES installation process should Splunk_TA_ForIndexes.spl be deployed to the indexers?

A. When adding apps to the deployment server.
B. Splunk_TA_ForIndexers.spl is installed first.
C. After installing ES on the search head(s) and running the distributed configuration management tool.
D. Splunk_TA_ForIndexers.spl is only installed on indexer cluster sites using the cluster master and the splunk apply cluster-bundle command.

Answer: B

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

NEW QUESTION 8
Both “Recommended Actions” and “Adaptive Response Actions” use adaptive response. How do they differ?

A. Recommended Actions show a textual description to an analyst, Adaptive Response Actions show them encoded.
B. Recommended Actions show a list of Adaptive Responses to an analyst, Adaptive Response Actions run them automatically.
C. Recommended Actions show a list of Adaptive Responses that have already been run, Adaptive Response Actions run them automatically.
D. Recommended Actions show a list of Adaptive Resposes to an analyst, Adaptive Response Actions run manually with analyst intervention.

Answer: D

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

NEW QUESTION 9
“10.22.63.159”, “websvr4”, and “00:26:08:18: CF:1D” would be matched against what in ES?

A. A user.
B. A device.
C. An asset.
D. An identity.

Answer: B

NEW QUESTION 10
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: C

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

NEW QUESTION 10
Which of the following actions would not reduce the number of false positives from a correlation search?

A. Reducing the severity.
B. Removing throttling fields.
C. Increasing the throttling window.
D. Increasing threshold sensitivity.

Answer: A

NEW QUESTION 11
Where is the Add-On Builder available from?

A. GitHub
B. SplunkBase
C. www.splunk.com
D. The ES installation package

Answer: B

Explanation:
Reference: https://docs.splunk.com/Documentation/AddonBuilder/3.0.1/UserGuide/Installation

NEW QUESTION 14
ES apps and add-ons from $SPLUNK_HOME/etc/apps should be copied from the staging instance to what location on the cluster deployer instance?

A. $SPLUNK_HOME/etc/master-apps/
B. $SPLUNK_HOME/etc/system/local/
C. $SPLUNK_HOME/etc/shcluster/apps
D. $SPLUNK_HOME/var/run/searchpeers/

Answer: C

Explanation:
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 15
How is notable event urgency calculated?

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

Answer: D

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

NEW QUESTION 16
What kind of value is in the red box in this picture?

Additional Fields	Value
HTTP Method	GET
Source	10.98.27.195 500
Source Expected	false
Source PCI Domain	untrust
Source Requires Antivirus	false
Source Should Time Synchronize	false
Source Should Update	false
Tag	modaction_result

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

Answer: C

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

NEW QUESTION 17
Where is it possible to export content, such as correlation searches, from ES?

A. Content exporter
B. Configure -> Content Management
C. Export content dashboard
D. Settings Menu -> ES -> Export

Answer: B

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

NEW QUESTION 22
Enterprise Security’s dashboards primarily pull data from what type of knowledge object?

A. Tstats
B. KV Store
C. Data models
D. Dynamic lookups

Answer: C

Explanation:
Reference: https://docs.splunk.com/Splexicon:Knowledgeobject

NEW QUESTION 23
To which of the following should the ES application be uploaded?

A. The indexer.
B. The KV Store.
C. The search head.
D. The dedicated forwarder.

Answer: C

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

NEW QUESTION 26
If a username does not match the 'identity' column in the identities list, which column is checked next?

A. Email.
B. Nickname
C. IP address.
D. Combination of Last Name, First Name.

Answer: C

NEW QUESTION 30
Which of the following features can the Add-on Builder configure in a new add-on?

A. Expire data.
B. Normalize data.
C. Summarize data.
D. Translate data.

Answer: B

Explanation:
Reference: https://docs.splunk.com/Documentation/AddonBuilder/3.0.1/UserGuide/Overview

NEW QUESTION 33
Which settings indicated that the correlation search will be executed as new events are indexed?

A. Always-On
B. Real-Time
C. Scheduled
D. Continuous

Answer: C

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

NEW QUESTION 37
How is it possible to navigate to the ES graphical Navigation Bar editor?

A. Configure -> Navigation Menu
B. Configure -> General -> Navigation
C. Settings -> User Interface -> Navigation -> Click on "Enterprise Security"
D. Settings -> User Interface -> Navigation Menus -> Click on "default" next to SplunkEnterpriseSecuritySuite

Answer: B

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

NEW QUESTION 39
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: A

NEW QUESTION 40
Who can delete an investigation?

A. ess_admin users only.
B. The investigation owner only.
C. The investigation owner and ess-admin.
D. The investigation owner and collaborators.

Answer: A

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

NEW QUESTION 42
After installing Enterprise Security, the distributed configuration management tool can be used to create which app to configure indexers?

A. Splunk_DS_ForIndexers.spl
B. Splunk_ES_ForIndexers.spl
C. Splunk_SA_ForIndexers.spl
D. Splunk_TA_ForIndexers.spl

Answer: D

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

NEW QUESTION 43
The Brute Force Access Behavior Detected correlation search is enabled, and is generating many false positives. Assuming the input data has already been validated. How can the correlation search be made less sensitive?

A. Edit the search and modify the notable event status field to make the notable events less urgent.
B. Edit the search, look for where or xswhere statements, and after the threshold value being compared to make it less common match.
C. Edit the search, look for where or xswhere statements, and alter the threshold value being compared to make it a more common match.
D. Modify the urgency table for this correlation search and add a new severity level to make notable events from this search less urgent.

Answer: B

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

NEW QUESTION 46
What is the first step when preparing to install ES?

A. Install ES.
B. Determine the data sources used.
C. Determine the hardware required.
D. Determine the size and scope of installation.

Answer: D

NEW QUESTION 50
What is the default schedule for accelerating ES Datamodels?

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

Answer: B

Explanation:
Reference: https://docs.splunk.com/Documentation/Splunk/8.0.2/Knowledge/Acceleratedatamodels

NEW QUESTION 53
.....

Relate Links

100% Pass Your SPLK-3001 Exam with Exambible Prep Materials

https://www.exambible.com/SPLK-3001-exam/

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - https://www.exambible.com/