Splunk

Exam Questions SPLK-3001

Splunk Enterprise Security Certified Admin Exam

NEW QUESTION 1
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

NEW QUESTION 2
What role should be assigned to a security team member who will be taking ownership of notable events in the incident review dashboard?

A. ess_user
B. ess_admin
C. ess_analyst
D. ess_reviewer

Answer: B

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

NEW QUESTION 3
Which indexes are searched by default for CIM data models?

A. notable and default
B. summary and notable
C. _internal and summary
D. All indexes

Answer: D

Explanation:
Reference: https://answers.splunk.com/answers/600354/indexes-searched-by-cim-data-models.html

NEW QUESTION 4
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 5
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 6
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 7
Which correlation search feature is used to throttle the creation of notable events?

A. Schedule priority.
B. Window interval.
C. Window duration.
D. Schedule windows.

Answer: C

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

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
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

NEW QUESTION 10
Adaptive response action history is stored in which index?

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

Answer: A

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

NEW QUESTION 10
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 15
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 20
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

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

NEW QUESTION 22
A site has a single existing search head which hosts a mix of both CIM and non-CIM compliant applications. All of the applications are mission-critical. The customer wants to carefully control cost, but wants good ES performance. What is the best practice for installing ES?

A. Install ES on the existing search head.
B. Add a new search head and install ES on it.
C. Increase the number of CPUs and amount of memory on the search head, then install ES.
D. Delete the non-CIM-compliant apps from the search head, then install ES.

Answer: B

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

NEW QUESTION 26
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 30
Where are attachments to investigations stored?

A. KV Store
B. notable index
C. attachments.csv lookup
D. <splunk_home>/etc/apps/SA-Investigations/default/ui/views/attachments

Answer: A

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

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

Explanation:
Reference: https://docs.splunk.com/Documentation/ES/6.1.0/User/RiskAnalysis#Dashboard_panels

NEW QUESTION 35
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 38
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 41
Which of the following actions can improve overall search performance?

A. Disable indexed real-time search.
B. Increase priority of all correlation searches.
C. Reduce the frequency (schedule) of lower-priority correlation searches.
D. Add notable event suppressions for correlation searches with high numbers of false positives.

Answer: A

NEW QUESTION 43
Which of the following ES features would a security analyst use while investigating a network anomaly notable?

A. Correlation editor.
B. Key indicator search.
C. Threat download dashboard.
D. Protocol intelligence dashboard.

Answer: D

Explanation:
Reference: https://www.splunk.com/en_us/products/premium-solutions/splunk-enterprise-security/features.html

NEW QUESTION 47
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

SPLK-3001 Practice Exam Features:

* SPLK-3001 Questions and Answers Updated Frequently

* SPLK-3001 Practice Questions Verified by Expert Senior Certified Staff

* SPLK-3001 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* SPLK-3001 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year