Exam Questions SPLK-3001

Splunk Enterprise Security Certified Admin Exam

https://www.2passeasy.com/dumps/SPLK-3001/

NEW QUESTION 1
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: C

Explanation:
Reference: https://docs.splunk.com/Documentation/ITSI/4.4.2/Configure/Createcorrelationsearch

NEW QUESTION 2
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 3
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 4
Which column in the Asset or Identity list is combined with event security to make a notable event’s urgency?

A. VIP
B. Priority
C. Importance
D. Criticality

Answer: B

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

NEW QUESTION 5
Which setting is used in indexes.conf to specify alternate locations for accelerated storage?

A. thawedPath
B. tstatsHomePath
C. summaryHomePath
D. warmToColdScript

Answer: B

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

NEW QUESTION 6
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

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

NEW QUESTION 7
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 8
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 9
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 10
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 10
How should an administrator add a new lookup through the ES app?

A. Upload the lookup file in Settings -> Lookups -> Lookup Definitions
B. Upload the lookup file in Settings -> Lookups -> Lookup table files
C. Add the lookup file to /etc/apps/SplunkEnterpriseSecuritySuite/lookups
D. Upload the lookup file using Configure -> Content Management -> Create New Content -> Managed Lookup

Answer: D

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

NEW QUESTION 14
Glass tables can display static images and text, the results of ad-hoc searches, and which of the following objects?

A. Lookup searches.
B. Summarized data.
C. Security metrics.
D. Metrics store searches.

Answer: C

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

NEW QUESTION 15
Which of the following is a key feature of a glass table?

A. Rigidity.
B. Customization.
C. Interactive investigations.
D. Strong data for later retrieval.

Answer: B

NEW QUESTION 20
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 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: A

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

NEW QUESTION 23
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

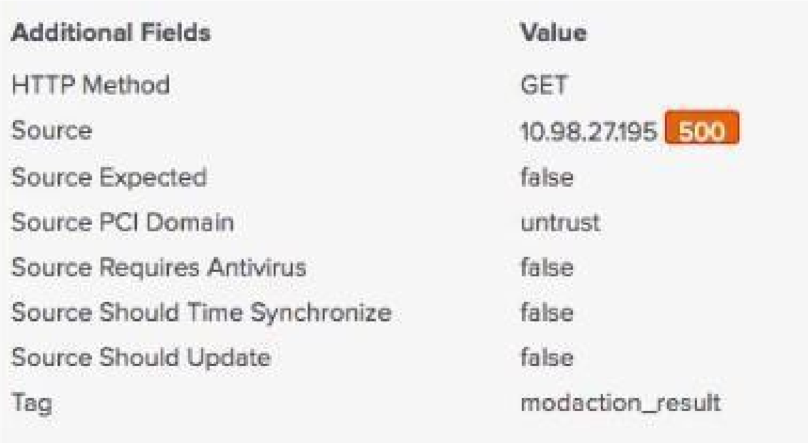
NEW QUESTION 25
Which of the following would allow an add-on to be automatically imported into Splunk Enterprise Security?

A. A prefix of CIM_
B. A suffix of .spl
C. A prefix of TECH_
D. A prefix of Splunk_TA_

Answer: D

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

NEW QUESTION 27
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 28
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 29
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 30
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 35
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 39
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 40

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 45
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 49
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 52
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 53
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 56
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

Explanation:
Reference: https://answers.splunk.com/answers/790783/anti-tampering-features-to-protect-splunk-logs-the.html

NEW QUESTION 58
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 60
......