Splunk

Exam Questions SPLK-3001

Splunk Enterprise Security Certified Admin Exam

NEW QUESTION 1
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 2
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 3
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 4
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 5
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 6
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 7
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 8
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 9
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 10
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?

A. OS: 32 bit, RAM: 16 MB, CPU: 12 cores
B. OS: 64 bit, RAM: 32 MB, CPU: 12 cores
C. OS: 64 bit, RAM: 12 MB, CPU: 16 cores
D. OS: 64 bit, RAM: 32 MB, CPU: 16 cores

Answer: C

Explanation:
Reference: https://docs.splunk.com/Documentation/Splunk/8.0.2/Capacity/Referencehardware

NEW QUESTION 11
What tools does the Risk Analysis dashboard provide?

A. High risk threats.
B. Notable event domains displayed by risk score.
C. A display of the highest risk assets and identities.
D. Key indicators showing the highest probability correlation searches in the environment.

Answer: C

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

NEW QUESTION 12
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 13
......

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

100% Actual & Verified — Instant Download, Please Click
Order The SPLK-3001 Practice Test Here