Boost up Your Certification Score

Splunk
SPLK-5002
Splunk Certified Cybersecurity Defense Engineer

For More Information – Visit link below:

https://www.examsboost.com/

Product Version

✓ Up to Date products, reliable and verified.
✓ Questions and Answers in PDF Format.

Visit us at: https://www.examsboost.com/test/splk-5002

Latest Version: 8.0

Question: 1

When creating a detection that searches user activity across CIM-compliant data, which CIM field should be reviewed to ensure that data is aggregated appropriately?

A. user_id
B. user
C. action
D. identity

Answer: B

Explanation:
The correct field is user, because Splunk's Common Information Model provides normalized fields that allow heterogeneous security data sources to be queried consistently. Authentication, endpoint, identity, operating-system, and application logs frequently use different native names for the same concept—for example, username, account_name, UserName, or src_user. CIM mappings normalize the appropriate value into the canonical user field.
This becomes particularly important when a detection performs aggregation such as:
| stats count by user
If contributing sources fail to populate user consistently, activity belonging to the same account can be fragmented, omitted, or incorrectly represented in the detection results. action identifies the result or nature of activity rather than the account responsible for it. user_id may occur in individual schemas but is not the general CIM field being tested here. identity represents a different conceptual object and is not the standard aggregation field for this use case.
The question appears on page 1 of the supplied certification material.
Study Guide topics: Common Information Model, CIM normalization, normalized fields, data-model consistency, user attribution, detection data preparation.

Question: 2

For detections that leverage a CIM data model, which aspect of the configuration is responsible for determining which indexes are being searched?

A. The data model's constraint macro.
B. The data model's index list.
C. The data model's root expression.
D. The data model's dataset hierarchy.

Answer: A

Explanation:
A CIM data model commonly uses a constraint macro to control the indexes from which qualifying events are retrieved. Splunk CIM implementations use macros to abstract index-selection logic away from individual searches. This provides administrators with a centralized mechanism for defining which indexes contain data relevant to a particular CIM domain.
Conceptually, a data-model constraint can resolve to logic comparable to:
index=wineventlog OR index=endpoint
Rather than embedding those indexes separately into every detection, the associated macro can be maintained centrally. Consequently, changing the macro modifies the effective search scope for searches that depend on that CIM configuration.
The dataset hierarchy describes relationships between root datasets and child datasets but does not itself serve as the primary mechanism for enumerating indexes. Likewise, an "index list" is not the configuration construct being referenced by the CIM architecture in this question. Root dataset constraints define qualifying event characteristics, but the constraint macro is what enables deployment-specific index scoping.
This distinction matters operationally because a perfectly written detection can return incomplete results when its CIM constraint macro excludes an index containing relevant normalized data.
Study Guide topics: CIM data models, constraints, CIM macros, index scoping, data-model configuration, detection data availability.

Question: 3

Once an engineer has determined that a new detection will fire, what is the next priority for that detection?

A. Ensure that threat intelligence has been integrated for use with the detection.
B. Ensure that all annotations, such as MITRE ATT&CK, are attached and understood with the detection.
C. Ensure that the SOAR playbooks are available to automate the outcomes from the detection.
D. Ensure that all fields that an analyst would need are present in the output from the detection.

Answer: D

Explanation:
Once detection logic has been proven capable of firing under the intended conditions, the immediate engineering priority is ensuring that its output provides the context required by the analyst. A technically correct detection that generates a finding without useful investigative fields merely transfers work from the detection engineer to the SOC analyst.
Useful output may include fields such as user, src, dest, process information, timestamps, parent processes, URLs, authentication results, risk objects, or other contextual values appropriate to

the detection. These fields allow an analyst to validate the activity, establish scope, determine severity, and choose an appropriate response without immediately rebuilding the originating search.
MITRE ATT&CK annotations are important for classification, reporting, and coverage analysis, while threat intelligence can enrich particular detections and SOAR can automate downstream response. However, those capabilities do not replace adequate detection output. Analyst usability logically precedes extensive enrichment and automation.
This reflects an important detection-engineering principle: detection efficacy is not simply whether a search generates an alert; the resulting security finding must be actionable and investigable.
Study Guide topics: Detection development, analyst workflow, actionable findings, contextual fields, detection validation, operationalization.

Question: 4

An engineer is writing a correlation search and needs to use T1059 from MITRE ATT&CK as a field in Incident Review. Assuming they are writing a correlation search that does not use the Risk data model, which example statement should be appended to the correlation search?

A. The expression assigning T1059 to the correlation search's MITRE ATT&CK annotation field.
B. The expression assigning T1059 to an unrelated event field.
C. The expression applying T1059 only through a risk-model field.
D. The expression using a non-annotation field for the ATT&CK technique.

Answer: A

Explanation:
For a conventional correlation search that creates findings outside the Risk data model, the MITRE ATT&CK technique must be represented through the detection's annotation metadata so that downstream Enterprise Security interfaces such as Incident Review can retain and display the technique context.
T1059 corresponds to the MITRE ATT&CK technique family Command and Scripting Interpreter. Assigning the technique to the appropriate MITRE ATT&CK annotation establishes structured metadata rather than simply placing the string T1059 into an arbitrary result field.
This distinction is important because detection annotations support consistent categorization, ATT&CK coverage reporting, analyst interpretation, and security-content management. An arbitrary field containing T1059 does not automatically carry the same semantic meaning. Likewise, a risk-model-specific representation is inappropriate when the question explicitly states that the correlation search does not use the Risk data model.
The supplied material presents this as an SPL/annotation implementation question on page 1.
Study Guide topics: Correlation searches, MITRE ATT&CK annotations, Incident Review, security-content metadata, event-based detections versus risk-based detections.

Question: 5

Which of the following is the most efficient search to return a list of all visible indexes and the sourcetypes contained within them?

A. A raw-event search followed by aggregation.
B. A non-index-grouped metadata search.
C. An index=* event search followed by stats.
D. A tstats search returning sourcetypes and grouping them by index.

Answer: D

Explanation:
The preferred approach is tstats, because tstats operates against indexed metadata rather than requiring Splunk to retrieve and process every matching raw event. A conceptual implementation is:
| tstats values(sourcetype) WHERE index=* BY index
This produces one result per visible index and lists the sourcetypes associated with each index. It is significantly more efficient than executing:
index=* | stats ...
because the latter can require broad raw-event retrieval across every searchable index. In a large security deployment containing billions of events, that difference is operationally significant.
The tstats command is particularly useful when the required information can be derived from indexed fields or accelerated data structures. Here, both index and sourcetype information can be obtained without inspecting full _raw event payloads.
The phrase "most efficient" is therefore central to the question. Several approaches may theoretically obtain similar information, but a broad raw-event search is unnecessarily expensive when indexed metadata already contains what is required.
This question appears on page 2 of the supplied material.
Study Guide topics: SPL efficiency, tstats, indexed metadata, index discovery, sourcetype inventory, search optimization.

Thank You for Trying Our Product

For More Information – Visit link below:

https://www.examsboost.com/

15 USD Discount Coupon Code:

G74JA8UF

FEATURES

- ✓ 90 Days Free Updates
- ✓ Money Back Pass Guarantee
- ✓ Instant Download or Email Attachment
- ✓ 24/7 Live Chat Support
- ✓ PDF file could be used at any Platform
- ✓ 50,000 Happy Customer