Boost up Your Certification Score

Splunk
SPLK-5003
Splunk Certified Cybersecurity Defense Architect

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-5003

Latest Version: 6.0

Question: 1

Sophia oversees data ingestion for her organization's SIEM. The data science team wants to run real-time analytics on security data and asks Sophia to provide a copy of all new endpoint telemetry from this point forward. The SIEM currently ingests 15 TB of endpoint telemetry per day.
Which of the following solutions can Sophia use to best support the data science team?

A. Export the last 12 months of telemetry data from the SIEM in OCSF.
B. Use a message bus to send data to both the SIEM and data science team.
C. Export the last 12 months of telemetry data from the SIEM in JSON format.
D. Configure the SIEM to export a CSV report of all new telemetry data every night.

Answer: B

Explanation:
A message bus provides a scalable, event-driven mechanism for distributing high-volume security telemetry to multiple consumers independently. With endpoint telemetry reaching 15 TB daily, Sophia requires a solution that supports continuous ingestion, low-latency delivery, and parallel consumption without introducing unnecessary processing overhead into the SIEM.
A message bus enables endpoint telemetry to be published to a common messaging infrastructure. The SIEM and data science platform can subscribe to the relevant data streams and process events according to their operational requirements. This architecture decouples data producers from consumers, allowing independent scaling, buffering, and failure recovery. Technologies such as Apache Kafka provide capabilities for partitioned event streams, durable message retention, and consumer groups. These capabilities support security analytics workloads while preserving flexibility for additional downstream systems.
Options A and C involve historical exports and do not address the requirement for continuous delivery of newly generated events. Option D introduces batch-processing delays and is unsuitable for real-time analysis.
The architecture also requires appropriate throughput planning, access controls, delivery guarantees, and retention policies.
Official reference / study topic: Splunk Cybersecurity Defense Architect blueprint, Security Data Management Objectives 2.1 and 2.8: message buses and scalable integration architectures.
==========

Question: 2

Which MLTK command can be used with tstats in an ES detection to apply a machine learning model to the search results?

A. Summary
B. Fit
C. Cluster
D. Sample

Answer: B

Explanation:
The Splunk Machine Learning Toolkit (MLTK) provides specialized Search Processing Language commands for applying statistical and machine-learning algorithms to security telemetry. Among the listed options, fit is the appropriate command because it trains a machine-learning model and applies that model to the current search results.
The tstats command efficiently retrieves aggregated information from indexed fields and accelerated data models. It can produce datasets containing activity frequencies, authentication counts, network connections, and other security measurements. These results can be passed into supported machine-learning algorithms for behavioral analysis and anomaly identification.
An example workflow is:
| tstats count where index=security by host
| fit DensityFunction count
The fit operation evaluates the resulting data and generates model-derived output for analysis. However, an important distinction exists in Splunk's official documentation: `apply` is the dedicated command for applying a previously trained and saved model to new search results. That command is missing from the supplied choices. Therefore, B is the best available answer, but the question is technically imprecise if it specifically refers to an existing model.
summary describes a learned model, sample selects subsets of data, and cluster is not the MLTK operation being requested.
Official reference / study topic: Splunk Machine Learning Toolkit, Search Commands for Machine Learning: fit and apply; certification blueprint Objective 4.4.
==========

Question: 3

To ensure that leadership remains aware of the security team's performance, which measurements should be reported regularly?
Choose three

A. Patch compliance percentage
B. Mean time to contain
C. Number of emergency change requests
D. Mean time to respond

Answer: A, B, D

Explanation:
Security leadership requires operational performance indicators that communicate risk reduction, defensive effectiveness, and incident-response capability. Patch compliance percentage, Mean Time to Contain (MTTC), and Mean Time to Respond (MTTR) provide complementary measurements of these outcomes.
Patch compliance percentage measures how effectively the organization maintains required security updates across its managed assets. High compliance with risk-based remediation deadlines generally indicates stronger vulnerability-management practices and reduced exposure to known vulnerabilities.
Mean Time to Contain measures the elapsed time required to restrict an incident's scope following detection or recognition. A lower containment time can reduce attacker movement, business interruption, and potential data loss.
Mean Time to Respond evaluates response efficiency across a defined incident population. Its precise start and end points must be standardized, particularly because organizations sometimes use MTTR to mean either response or resolution time.
These measures should be accompanied by consistent reporting periods, severity segmentation, historical trends, and agreed targets.
The number of emergency change requests is principally an IT service-management indicator. Although it may expose operational instability or process weaknesses, it does not directly measure cybersecurity-team effectiveness.
Together, the selected measurements provide leadership with an actionable view of prevention and response performance.
Official reference / study topic: Splunk certification blueprint, Measuring and Improving Security Program Effectiveness, Objectives 7.1–7.2.
==========

Question: 4

Which of the following are commonly used criteria for evaluating threat-intelligence feeds? Choose three

A. TLP
B. Industry
C. Source
D. Severity

Answer: B, C, D

Explanation:
Threat-intelligence feeds should be evaluated according to their relevance, credibility, and capacity to support practical cybersecurity decisions. Industry, source, and severity are meaningful dimensions for assessing intelligence suitability.

Industry relevance determines whether the intelligence reflects adversaries, campaigns, vulnerabilities, and attack methods affecting the organization's sector. Intelligence targeting financial institutions may have different operational value from intelligence focused on manufacturing or healthcare.
Source is important because intelligence quality depends on collection methodology, provenance, reputation, and confidence. A feed drawing from validated investigations and credible research generally provides stronger decision support than an unverified collection of indicators.
Severity helps analysts prioritize the threats described by the feed according to their potential consequences. Severity alone is insufficient; it should be interpreted alongside confidence, relevance, timeliness, and organizational exposure.
Traffic Light Protocol (TLP), option A, governs the permitted disclosure and redistribution of information. TLP classifications describe sharing restrictions rather than the intrinsic reliability, technical severity, or relevance of intelligence.
Therefore, B, C, and D best represent the specified evaluation dimensions.
Effective feed management should additionally measure false-positive rates, indicator expiration, freshness, coverage, and integration requirements.
Official reference / study topic: Splunk certification blueprint, Advanced Threat Intelligence and Analysis Objective 1.2; FIRST TLP 2.0 guidance.
==========

Question: 5

Justin has successfully completed importing data from the CMDB platform into the SIEM. During data validation, he finds a host with the MAC address 35:33:33:20:76, which does not share the OUI (03:83:71) of the other deployed devices.
Which of the following most likely explains this discrepancy?

A. CMDB contains data from personal devices managed under MDM
B. CMDB data was normalized during the SIEM import process
C. CMDB data was corrupted during the export process
D. CMDB contains data related to dynamic VPN pool addresses

Answer: C

Explanation:
Configuration Management Database (CMDB) imports require validation of asset identifiers, data completeness, field formatting, and consistency before information is used for security analytics.
The most significant problem in this scenario is the supplied address 35:33:33:20:76. A conventional Ethernet MAC address contains six octets, totaling 48 bits. The address in the question contains only five octets and therefore does not represent a valid EUI-48 address. Additionally, the initial octet 35 has its least significant bit set, indicating a group-address designation rather than a conventional individual interface address. These characteristics suggest malformed source data or corruption during extraction, transformation, or export.

A different Organizationally Unique Identifier (OUI) does not independently demonstrate corruption. Organizations routinely deploy equipment from multiple manufacturers, and personal devices managed through MDM may introduce additional vendor identifiers. However, the invalid address structure provides stronger evidence of a data-integrity problem than an ordinary manufacturer discrepancy.
Data normalization should standardize representations rather than create invalid hardware identifiers. Dynamic VPN address pools primarily concern IP address allocation and do not explain the malformed MAC value.
Justin should compare the imported record against the authoritative CMDB entry, inspect export transformations, and implement format-validation checks before accepting the asset record.
Official reference / study topic: Splunk certification blueprint, Security Data Management Objectives 2.2 and 2.6; IEEE EUI-48 and OUI definitions.
==========

Visit us at: https://www.examsboost.com/test/splk-5003

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

