

Splunk SPLK-5002

Certified Cybersecurity Defense Engineer

Questions And Answers PDF Format:

For More Information – Visit link below:

<https://www.certsgrade.com/>

Version = Product



Latest Version: 6.0

Question: 1

A company wants to create a dashboard that displays normalized event data from various sources. What approach should they use?

Response:

- A. Implement a data model using CIM.
- B. Apply search-time field extractions.
- C. Use SPL queries to manually extract fields.
- D. Configure a summary index.

Answer: A

Question: 2

What is the primary purpose of data indexing in Splunk?

Response:

- A. To ensure data normalization
- B. To store raw data and enable fast search capabilities
- C. To secure data from unauthorized access
- D. To visualize data using dashboards

Answer: B

Question: 3

How can you ensure that a specific sourcetype is assigned during data ingestion?

Response:

- A. Use props.conf to specify the sourcetype.
- B. Define the sourcetype in the search head.
- C. Configure the sourcetype in the deployment server.
- D. Use REST API calls to tag sourcetypes dynamically.

Answer: A

Question: 4

A cybersecurity engineer notices a delay in retrieving indexed data during a security incident investigation. The Splunk environment has multiple indexers but only one search head. Which approach can resolve this issue?

Response:

- A. Increase search head memory allocation.
- B. Optimize search queries to use tstats instead of raw searches.
- C. Configure a search head cluster to distribute search queries.
- D. Implement accelerated data models for faster querying.

Answer: C

Question: 5

What is the main purpose of incorporating threat intelligence into a security program?

Response:

- A. To automate response workflows
- B. To proactively identify and mitigate potential threats
- C. To generate incident reports for stakeholders
- D. To archive historical events for compliance

Answer: B

Question: 6

What feature allows you to extract additional fields from events at search time?

Response:

- A. Index-time field extraction
- B. Event parsing
- C. Search-time field extraction
- D. Data modeling

Answer: C

Question: 7

Which Splunk feature helps to standardize data for better search accuracy and detection logic?

Response:

- A. Field Extraction
- B. Data Models
- C. Event Correlation
- D. Normalization Rules

Answer: D

Question: 8

Which methodology prioritizes risks by evaluating both their likelihood and impact?

Response:

- A. Threat modeling
- B. Risk-based prioritization
- C. Incident lifecycle management
- D. Statistical anomaly detection

Answer: B

Question: 9

During a high-priority incident, a user queries an index but sees incomplete results. What is the most likely issue?

Response:

- A. Buckets in the warm state are inaccessible.
- B. Data normalization was not applied.
- C. Indexers have reached their queue capacity.
- D. The search head configuration is outdated.

Answer: C

Question: 10

Which action improves the effectiveness of notable events in Enterprise Security?

Response:

- A. Applying suppression rules for false positives
- B. Disabling scheduled searches

- C. Using only raw log data in searches
- D. Limiting the search scope to one index

Answer: A

For More Information – **Visit link below:**
<https://www.certsgrade.com/>

PRODUCT FEATURES

-  **100% Money Back Guarantee**
-  **90 Days Free updates**
-  **Special Discounts on Bulk Orders**
-  **Guaranteed Success**
-  **50,000 Satisfied Customers**
-  **100% Secure Shopping**
-  **Privacy Policy**
-  **Refund Policy**

16 USD Discount Coupon Code: NB4XKTMZ



Visit us at: <https://www.certsgrade.com/pdf/splk-5002>