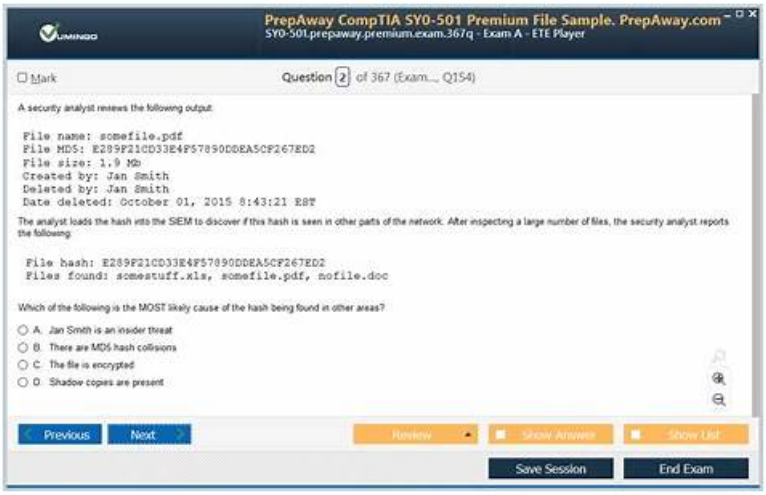
Valid Splunk SPLK-5002 Test Practice, SPLK-5002 Dump File



What's more, part of that ITCertMagic SPLK-5002 dumps now are free: https://drive.google.com/open?id=1O5tVKpV7qiW9N8yDKdfMOKFnWmH3mOmj

We are the fastest to pursue acquiring SPLK-5002 certification; we are the highest to pursue protecting your benefits. Our ITCertMagic ensures the accuracy and the most coverage of SPLK-5002 Certification Exam Dumps. If you purchase SPLK-5002 certification exam dumps, we will ensure that you can get free update service in one year.

Undoubtedly, passing the Splunk SPLK-5002 certification exam is one big achievement. Regardless of how tough the SPLK-5002 exam is, it serves an important purpose of improving your skills and knowledge of a specific field. Once you become certified by Splunk SPLK-5002, a whole new career scope will open up to you.

>> Valid Splunk SPLK-5002 Test Practice <<

SPLK-5002 Dump File, Online SPLK-5002 Tests

A lot of applicants have studied from Splunk SPLK-5002 practice material. They have rated it positively because they have cracked Splunk SPLK-5002 Certification on their first try. ITCertMagic guarantees its customers that they can pass the SPLK-5002 test on the first attempt.

Splunk SPLK-5002 Exam Syllabus Topics:

Topic	Details
Topic 1	• Building Effective Security Processes and Programs: This section targets Security Program Managers and Compliance Officers, focusing on operationalizing security workflows. It involves researching and integrating threat intelligence, applying risk and detection prioritization methodologies, and developing documentation or standard operating procedures (SOPs) to maintain robust security practices.
Topic 2	• Data Engineering: This section of the exam measures the skills of Security Analysts and Cybersecurity Engineers and covers foundational data management tasks. It includes performing data review and analysis, creating and maintaining efficient data indexing, and applying Splunk methods for data normalization to ensure structured and usable datasets for security operations.
Topic 3	• Auditing and Reporting on Security Programs: This section tests Auditors and Security Architects on validating and communicating program effectiveness. It includes designing security metrics, generating compliance reports, and building dashboards to visualize program performance and vulnerabilities for stakeholders.

Topic 4	• Automation and Efficiency: This section assesses Automation Engineers and SOAR Specialists in streamlining security operations. It covers developing automation for SOPs, optimizing case management workflows, utilizing REST APIs, designing SOAR playbooks for response automation, and evaluating integrations between Splunk Enterprise Security and SOAR tools.
Topic 5	• Detection Engineering: This section evaluates the expertise of Threat Hunters and SOC Engineers in developing and refining security detections. Topics include creating and tuning correlation searches, integrating contextual data into detections, applying risk-based modifiers, generating actionable Notable Events, and managing the lifecycle of detection rules to adapt to evolving threats.

Splunk Certified Cybersecurity Defense Engineer Sample Questions (Q77-Q82):

NEW QUESTION # 77
What feature allows you to extract additional fields from events at search time?

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

Answer: D

Explanation:
Splunk allows dynamic field extraction to enhance data analysis without modifying raw indexed data.
Search-Time Field Extraction:
Extracts fields on-demand when running searches.
Uses Splunk's Field Extraction Engine (rex,spath, or automatic field discovery).
Minimizes indexing overhead by keeping the raw data unchanged.

NEW QUESTION # 78
A security analyst wants to validate whether a newly deployed SOAR playbook is performing as expected. What steps should they take?

- A. Compare the playbook to existing incident response workflows
- B. Automate all tasks within the playbook immediately
- C. Monitor the playbook's actions in real-time environments
- D. Test the playbook using simulated incidents

Answer: D

Explanation:
A SOAR (Security Orchestration, Automation, and Response) playbook is a set of automated actions designed to respond to security incidents. Before deploying it in a live environment, a security analyst must ensure that it operates correctly, minimizes false positives, and doesn't disrupt business operations.
Key Reasons for Using Simulated Incidents:
Ensures that the playbook executes correctly and follows the expected workflow.
Identifies false positives or incorrect actions before deployment.
Tests integrations with other security tools (SIEM, firewalls, endpoint security).
Provides a controlled testing environment without affecting production.
How to Test a Playbook in Splunk SOAR?
1. Use the "Test Connectivity" Feature - Ensures that APIs and integrations work.
2. Simulate an Incident - Manually trigger an alert similar to a real attack (e.g., phishing email or failed admin login).
3. Review the Execution Path - Check each step in the playbook debugger to verify correct actions.
4. Analyze Logs & Alerts - Validate that Splunk ES logs, security alerts, and remediation steps are correct.
5. Fine-tune Based on Results - Modify the playbook logic to reduce unnecessary alerts or excessive automation.

NEW QUESTION # 79
What are key elements of a well-constructed notable event?(Choosethree)

- A. Proper categorization
- B. Minimal use of contextual data
- C. Relevant field extractions
- D. Meaningful descriptions

Answer: A,C,D

Explanation:
A notable event in Splunk Enterprise Security (ES) represents a significant security detection that requires investigation.
#Key Elements of a Good Notable Event:#Meaningful Descriptions (Answer A) Helps analysts understand the event at a glance.
Example: Instead of "Possible attack detected," use "Multiple failed admin logins from foreign IP address".
#Proper Categorization (Answer C)
Ensures events are classified correctly (e.g., Brute Force, Insider Threat, Malware Activity).
Example: A malicious file download alert should be categorized as "Malware Infection", not just "General Alert".
#Relevant Field Extractions (Answer D)
Ensures that critical details (IP, user, timestamp) are present for SOC analysis.
Example: If an alert reports failed logins, extracted fields should include username, source IP, and login method.
Why Not the Other Options?
#B. Minimal use of contextual data - More context helps SOC analysts investigate faster.
References & Learning Resources
#Building Effective Notable Events in Splunk ES: https://docs.splunk.com/Documentation/ES#SOC Best Practices for Security Alerts: https://splunkbase.splunk.com#How to Categorize Security Alerts Properly: https://www.splunk.com/en_us/blog/security

NEW QUESTION # 80
Which Splunk configuration ensures events are parsed and indexed only once for optimal storage?

- A. Search head clustering
- B. Universal forwarder
- C. Summary indexing
- D. Index time transformations

Answer: D

Explanation:
Why Use Index-Time Transformations for One-Time Parsing & Indexing?
Splunk parses and indexes data once during ingestion to ensure efficient storage and search performance.
Index-time transformations ensure that logs are:
#Parsed, transformed, and stored efficiently before indexing.#Normalized before indexing, so the SOC team doesn't need to clean up fields later.#Processed once, ensuring optimal storage utilization.
#Example of Index-Time Transformation in Splunk:#Scenario: The SOC team needs to mask sensitive data in security logs before storing them in Splunk.#Solution: Use anINDEXED_EXTRACTIONSrule to:
Redact confidential fields (e.g., obfuscate Social Security Numbers in logs).
Rename fields for consistency before indexing.

NEW QUESTION # 81
Which syntax is correct to create two new rows on an existing threat intelligence collection?

- A. curl -k -u admin:pass https://localhost:8089/services/data/threat_intel/item/email_intel -d item='[{"src_user": "user_new", "subject":"click this"},{"src_user": "user2_new", "subject":"click this"}]'
- B. curl -k -u admin:pass https://localhost:8089/services/data/threat_intel/item/email_intel -d item='[{"src_user": "user_new", "subject":"click this"},{"src_user": "user2_new", "subject":"click this"}]' -G -X
- C. curl -k -u admin:pass https://localhost:8089/services/data/threat_intel/item/email_intel -d item='[{"src_user": "user_new", "subject":"click this"}]'
- D. curl -k -u admin:pass https://localhost:8089/services/data/threat_intel/item/email_intel -d item='[{"src_user": "user_new", "subject":"click this"}]' -G -X

Answer: A

Explanation:
This syntax is valid because it passes multiple JSON objects inside a single array for the item parameter, ensuring both new rows are added to the collection in one request.

NEW QUESTION # 82
.....

Our SPLK-5002 exam questions have always been the authority of the area, known among the exam candidates for their high quality and accuracy. According to data collected by our workers who questioned former exam candidates, the passing rate of our SPLK-5002 training engine is between 98 to 100 percent! It is nearly perfect. So it is undeniable that our SPLK-5002 practice materials are useful and effective.

SPLK-5002 Dump File: https://www.itcertmagic.com/Splunk/real-SPLK-5002-exam-prep-dumps.html

P.S. Free 2026 Splunk SPLK-5002 dumps are available on Google Drive shared by ITCertMagic: https://drive.google.com/open?id=1O5tVKpV7qiW9N8yDKdfMOKFnWmH3mOmj