Splunk SPLK-5002 Questions PDF File

P.S. Free 2025 Splunk SPLK-5002 dumps are available on Google Drive shared by PassReview: https://drive.google.com/open?id=1qlaBf4nemimlFw7WPo8K2FSwOGGWITgu

Our SPLK-5002 study materials have won many people's strong support. And our SPLK-5002 learning quiz is famous all over the world. Now, our loyal customers have gained wealth and respect with the guidance of our SPLK-5002 learning materials. At the same time, the price is not so high. You totally can afford them. Do not make excuses for your laziness. Please take immediate actions. Our SPLK-5002 Study Guide is extremely superior.

Splunk SPLK-5002 Exam Syllabus Topics:

Topic	Details
Topic 1	• 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.
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	• 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 5	- 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.

>> SPLK-5002 Dumps Guide <<

SPLK-5002 Exam Preparation Files & SPLK-5002 Test Prep & SPLK-5002 Exam Resources

If you are worried for preparation of your SPLK-5002 exam, so stop distressing about it because you have reached to the reliable source of your success. PassReview is the ultimate solution to your all Splunk Designing and Implementing Cloud Data Platform Solutions related problem. It provides you with a platform which enables you to clear your SPLK-5002 Exam. PassReview provides you SPLK-5002 exam questions which is reliable and offers you a gateway to your destination.

Splunk Certified Cybersecurity Defense Engineer Sample Questions (Q69-Q74):

NEW QUESTION # 69
A security analyst wants to validate whether a newly deployed SOAR playbook is performing as expected.
Whatsteps should they take?

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

Answer: B

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.
Why Not the Other Options?
#B. Monitor the playbook's actions in real-time environments - Risky without prior validation. Itcan cause disruptions if the playbook misfires.#C. Automate all tasks immediately - Not best practice. Gradual deployment ensures better security control and monitoring.#D. Compare with existing workflows - Good practice, but it does not validate the playbook's real execution.
References & Learning Resources
#Splunk SOAR Documentation: https://docs.splunk.com/Documentation/SOAR#Testing Playbooks in Splunk SOAR: https://www.splunk.com/en_us/products/soar.html#SOAR Playbook Debugging Best Practices: https://splunkbase.splunk.com

NEW QUESTION # 70
Which configurations are required for data normalization in Splunk?(Choosetwo)

- A. savedsearches.conf
- B. authorize.conf
- C. eventtypes.conf
- D. transforms.conf
- E. props.conf

Answer: D,E

Explanation:
Configurations Required for Data Normalization in Splunk
Data normalization ensures consistent field naming and event structuring, especially for Splunk Common Information Model (CIM) compliance.
#1. props.conf (A)
Defines how data is parsed and indexed.
Controls field extractions, event breaking, and timestamp recognition.
Example:
Assigns custom sourcetypes and defines regex-based field extraction.
#2. transforms.conf (B)
Used for data transformation, lookup table mapping, and field aliasing.
Example:
Normalizes firewall logs by renaming src_ip # src to align with CIM.
#Incorrect Answers:
C: savedsearches.conf # Defines scheduled searches, not data normalization.
D: authorize.conf # Manages user permissions, not data normalization.
E: eventtypes.conf # Groups events into categories but doesn't modify data structure.
#Additional Resources:
Splunk Data Normalization Guide
Understanding props.conf and transforms.conf

NEW QUESTION # 71
A company wants to create a dashboard that displays normalized event data from various sources.
Whatapproach should they use?

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

Answer: A

Explanation:
When organizations need to normalize event data from various sources, using Common Information Model (CIM) in Splunk is the best approach.
Why Use CIM for Normalized Event Data?
Standardizes Data Across Different Log Sources
CIM ensures consistent field names and formats across varied log types.
Makes searches, reports, and dashboards easier to manage.
Enables Faster and More Efficient Searches
Uses Data Models to accelerate search queries.
Reduces the need for custom field extractions.

NEW QUESTION # 72
What methods improve risk and detection prioritization?(Choosethree)

- A. Enforcing strict search head resource limits
- B. Automating detection tuning
- C. Assigning risk scores to assets and events
- D. Incorporating business context into decisions
- E. Using predefined alert templates

Answer: B,C,D

Explanation:
Risk and detection prioritization in Splunk Enterprise Security (ES) helps SOC analysts focus on the most critical threats. By assigning risk scores, integrating business context, and automating detection tuning, organizations can prioritize security incidents efficiently.
Methods to Improve Risk and Detection Prioritization:
Assigning Risk Scores to Assets and Events (A)
Uses Risk-Based Alerting (RBA) to prioritize high-risk activities based on behavior and history.
Helps SOC teams focus on true threats instead of isolated events.
Incorporating Business Context into Decisions (C)
Adds context from asset criticality, user roles, and business impact.
Ensures alerts are ranked based on their potential business impact.
Automating Detection Tuning (D)
Uses machine learning and adaptive response actions to reduce false positives.
Dynamically adjusts alert thresholds based on evolving threat patterns.

NEW QUESTION # 73
Which actions enhance the accuracy of Splunk dashboards?(Choosetwo)

- A. Avoiding token-based filters
- B. Performing regular data validation
- C. Using accelerated data models
- D. Disabling drill-down features

Answer: B,C

Explanation:
How to Improve Dashboard Accuracy in Splunk?
#1. Using Accelerated Data Models (Answer A)#Increases search speedand ensuresdashboards load faster.
#Provides pre-processed structured dataforreal-time analysis.#Example:ASOC dashboard tracking failed loginsuses an accelerated authentication data model forfaster rendering.
#2. Performing Regular Data Validation (Answer C)#Ensures that the indexed data is accurate and complete.
#Prevents misleading dashboardscaused by incomplete logs or incorrect field extractions.#Example:If afirewall log source stops sending data, regular validation detects missing logsbefore analysts rely on incorrect dashboards.
Why Not the Other Options?
#B. Avoiding token-based filters- Tokensimprovedashboard flexibility; avoiding themreduces usability.#D.
Disabling drill-down features- Drill-downsenhance insightsby allowing analysts to investigate details easily.
References & Learning Resources
#Splunk Dashboard Performance Optimization: https://docs.splunk.com/Documentation/Splunk/latest/Viz
/Dashboards#Using Data Models for Fast and Accurate Dashboards: https://splunkbase.splunk.com#Regular Data Validation for SOC Dashboards: https://www.splunk.com/en_us/blog/security

NEW QUESTION # 74
......

Contrary to the high prices of the other exam materials available online, our SPLK-5002 exam questions can be obtained on an affordable price yet their quality and benefits beat all similar products of our competitors. Some of our customer will be surprised to find that the price of our SPLK-5002 Study Guide is too low to believe for they had been charged a lot before on the other websites. But after they passed their exams with our SPLK-5002 praparation materials. They said that our SPLK-5002 simulating exam is proved the best alternative of the time and money.

Valid SPLK-5002 Exam Tips: https://www.passreview.com/SPLK-5002_exam-braindumps.html

- Pass Guaranteed Quiz Splunk - Latest SPLK-5002 Dumps Guide □ Open ☀ www.validtorrent.com □☀□ and search for { SPLK-5002 } to download exam materials for free □SPLK-5002 New Braindumps Ebook
- Latest SPLK-5002 Exam Bootcamp □ Latest SPLK-5002 Exam Bootcamp □ SPLK-5002 Latest Exam Testking □ Search for ➽ SPLK-5002 □ and easily obtain a free download on ▶ www.pdfvce.com ◀ □Reliable SPLK-5002 Exam Sample
- SPLK-5002 Valid Exam Syllabus ✴ SPLK-5002 Latest Test Simulations □ SPLK-5002 Latest Exam Price □ Go to website “ www.easy4engine.com ” open and search for 《 SPLK-5002 》 to download for free □SPLK-5002 Latest Exam Price
- SPLK-5002 Latest Test Simulations □ SPLK-5002 Latest Test Simulations □ SPLK-5002 Pass Leader Dumps □ Open □ www.pdfvce.com □ and search for ▷ SPLK-5002 ◁ to download exam materials for free □SPLK-5002 Latest Test Simulations
- 2026 100% Free SPLK-5002 –High Hit-Rate 100% Free Dumps Guide | Valid SPLK-5002 Exam Tips □ ➡ www.examcollectionpass.com □□□ is best website to obtain □ SPLK-5002 □ for free download □Exam SPLK-5002 Objectives
- Splunk - SPLK-5002 Authoritative Dumps Guide □ Search for ➠ SPLK-5002 □ on ☀ www.pdfvce.com □☀□ immediately to obtain a free download □SPLK-5002 Latest Test Simulations
- Splunk - SPLK-5002 Authoritative Dumps Guide □ Search for 【 SPLK-5002 】 and download it for free immediately on “ www.practicevce.com ” □Latest SPLK-5002 Exam Bootcamp
- SPLK-5002 Exam Reference □ SPLK-5002 Latest Exam Testking □ SPLK-5002 Latest Exam Price □ Copy URL □ www.pdfvce.com □ open and search for ▶ SPLK-5002 ◀ to download for free □SPLK-5002 Valid Exam Syllabus
- SPLK-5002 Exam Reference □ SPLK-5002 Pass Leader Dumps □ SPLK-5002 New Braindumps Ebook □ Easily obtain □ SPLK-5002 □ for free download through □ www.prepawaypdf.com □ □SPLK-5002 Latest Test Simulations
- myportal.utt.edu.tt, www.stes.tyc.edu.tw, paidforarticles.in, www.stes.tyc.edu.tw, www.skillstopaythebills.co.uk, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, myportal.utt.edu.tt, Disposable vapes

BTW, DOWNLOAD part of PassReview SPLK-5002 dumps from Cloud Storage: https://drive.google.com/open?id=1qlaBf4nemimlFw7WPo8K2FSwOGGWITgu