SPLK-5001 Standard Answers, SPLK-5001 Exam Assessment

Pass Splunk SPLK-5001 Exam | Latest SPLK-5001 Dumps & Practice Exams - Cert007

1.Which of the following is the primary benefit of using the CIM in Splunk?
A. It allows for easier correlation of data from different sources.
B. It improves the performance of search queries on raw data.
C. It enables the use of advanced machine learning algorithms.
D. It automatically detects and blocks cyber threats.
Answer: A

2.Which of the following data sources would be most useful to determine if a user visited a recently identified malicious website?
A. Active Directory Logs
B. Web Proxy Logs
C. Intrusion Detection Logs
D. Web Server Logs
Answer: B

3.Which of the following is a tactic used by attackers, rather than a technique?
A. Gathering information about a target.
B. Establishing persistence with a scheduled task.
C. Using a phishing email to gain initial access.
D. Escalating privileges via UAC bypass.
Answer: A

4.Enterprise Security has been configured to generate a Notable Event when a user has quickly authenticated from multiple locations between which travel would be impossible.
This would be considered what kind of an anomaly?
A. Access Anomaly
B. Identity Anomaly
C. Endpoint Anomaly
D. Threat Anomaly
Answer: A

5.An analyst is investigating a network alert for suspected lateral movement from one Windows host to another Windows host.
According to Splunk CIM documentation, the IP address of the host from which the attacker is moving would be in which field?
A. host
B. dest
C. src_nt_host
D. src_ip
Answer: D

6.Which pre-packaged app delivers security content and detections on a regular, ongoing basis for Enterprise Security and SOAR?
A. SSE

2 / 3

What's more, part of that BootcampPDF SPLK-5001 dumps now are free: https://drive.google.com/open?id=1UE3qVQehy6TT-rkSLCLEtVO_CNZsujwd

If you cannot complete the task efficiently, we really recommend using SPLK-5001 learning materials. Through the assessment of your specific situation, we will provide you with a reasonable schedule, and provide the extensible version of SPLK-5001 exam training you can quickly grasp more knowledge in a shorter time. In the same time, you will do more than the people around you. This is what you can do with SPLK-5001 Test Guide. Our SPLK-5001 learning guide is for you to improve your efficiency and complete the tasks with a higher quality. You will stand out from the crowd both in your studies and your work. The high quality of SPLK-5001 exam training is tested and you can be assured of choice.

Splunk SPLK-5001 Exam Syllabus Topics:

Topic	Details
Topic 1	• Installation and Configuration: In the Installation and Configuration section, the focus is on the procedures for installing and setting up Splunk Enterprise. This includes the installation process across different operating systems and the configuration of necessary components to ensure proper functionality. Key topics include installing the Splunk software, setting up the Deployment Server, and configuring Data Inputs for data collection and indexing.

Topic 2	• Monitoring and Performance Tuning: The Monitoring and Performance Tuning section addresses strategies for overseeing and optimizing the performance of a Splunk deployment.
Topic 3	• Troubleshooting and Maintenance: The Troubleshooting and Maintenance section focuses on diagnosing and resolving issues within a Splunk deployment. This involves using diagnostic tools and logs to troubleshoot common problems such as data ingestion issues, search performance, and system errors.

Free PDF Quiz 2026 Fantastic Splunk SPLK-5001 Standard Answers

Our SPLK-5001 study materials are very popular in the international market and enjoy wide praise by the people in and outside the circle. We have shaped our SPLK-5001 exam questions into a famous and top-ranking brand and we enjoy well-deserved reputation among the clients. Our SPLK-5001 learning guide boosts many outstanding and superior advantages which other same kinds of exam materials don't have. And we are very reliable in every aspect no matter on the quality or the according service.

Splunk Certified Cybersecurity Defense Analyst Sample Questions (Q67-Q72):

NEW QUESTION # 67
Splunk SOAR uses what feature to automate security workflows so that analysts can spend more time performing analysis and investigation?

- A. Adaptive Actions
- B. Workbooks
- C. Analytic Stories
- D. Playbooks

Answer: D

NEW QUESTION # 68
A threat hunter generates a report containing the list of users who have logged in to a particular database during the last 6 months, along with the number of times they have each authenticated. They sort this list and remove any user names who have logged in more than 6 times. The remaining names represent the users who rarely log in, as their activity is more suspicious. The hunter examines each of these rare logins in detail.
This is an example of what type of threat-hunting technique?

- A. Time Series Analysis
- B. Least Frequency of Occurrence Analysis
- C. Outlier Frequency Analysis
- D. Co-Occurrence Analysis

Answer: B

NEW QUESTION # 69
Which of the following is a best practice for searching in Splunk?

- A. Streaming commands run before aggregating commands in the Search pipeline.
- B. Limit fields returned from the search utilizing the cable command.
- C. Searching over All Time ensures that all relevant data is returned.
- D. Raw word searches should contain multiple wildcards to ensure all edge cases are covered.

Answer: B

NEW QUESTION # 70
Upon investigating a report of a web server becoming unavailable, the security analyst finds that the web server's access log has the same log entry millions of times:
147.186.119.200 - - [28/Jul/2023:12:04:13 -0300] "GET /login/ HTTP/1.0" 200 3733 What kind of attack is occurring?

- A. Database Injection Attack
- B. Distributed Denial of Service Attack
- C. Cross-Site Scripting Attack
- D. Denial of Service Attack

Answer: B

NEW QUESTION # 71
An analyst is attempting to investigate a Notable Event within Enterprise Security. Through the course of their investigation they determined that the logs and artifacts needed to investigate the alert are not available.
What event disposition should the analyst assign to the Notable Event?

- A. True Positive, since there are no logs to prove that the event did not occur.
- B. Benign Positive, since there was no evidence that the event actually occurred.
- C. False Negative, since there are no logs to prove the activity actually occurred.
- D. Other, since a security engineer needs to ingest the required logs.

Answer: D

NEW QUESTION # 72
.....

No matter in China or other company, Splunk has great influence for both enterprise and personal. If you can go through examination with SPLK-5001 latest exam study guide and obtain a certification, there may be many jobs with better salary and benefits waiting for you. Most large companies think a lot of IT professional certification. SPLK-5001 Latest Exam study guide makes your test get twice the result with half the effort and little cost.

Search for （ SPLK-5001 ） and easily obtain a free download on ➽ www.pdfvce.com □ □SPLK-5001 Reliable Study Plan

- New SPLK-5001 Standard Answers | High Pass-Rate Splunk SPLK-5001: Splunk Certified Cybersecurity Defense Analyst 100% Pass □ Download ➽ SPLK-5001 □ for free by simply entering ➤ www.examcollectionpass.com □ website □ □SPLK-5001 Mock Exam
- antonqmuq117800.blogdanica.com, hassanczdv503559.wikiusnews.com, dl.instructure.com, victorvmzw573022.wikifiltraciones.com, zayneufd886011.glifeblog.com, dawuduvty576126.blogitright.com, tessgxpn788073.bloggazzo.com, dl.instructure.com, diegoymzw108491.evawiki.com, gerardjjih729636.csublogs.com, Disposable vapes

BTW, DOWNLOAD part of BootcampPDF SPLK-5001 dumps from Cloud Storage: https://drive.google.com/open?id=1UE3qVQehy6TT-rkSLCLEtVO_CNZsujwd