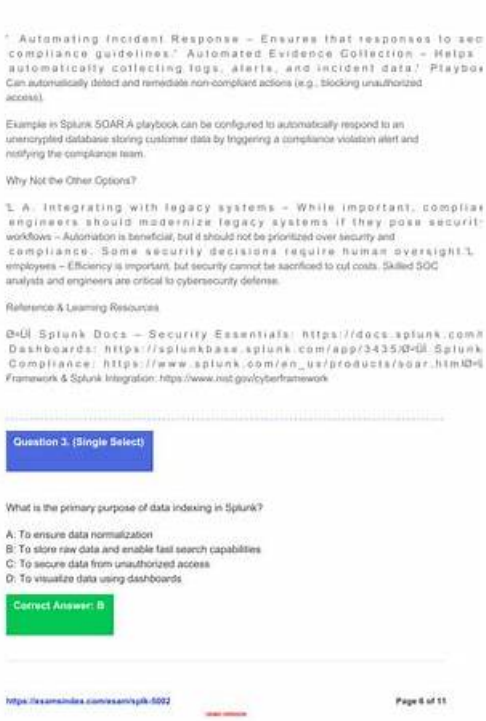
Avoid Exam Failure With Splunk SPLK-5002 PDF Questions



' Automating Incident Response – Ensures that responses to sec
compliance guidelines.' Automated Evidence Collection – Helps
automatically collecting logs, alerts, and incident data.' Playbo
Can automatically detect and remediate non-compliant actions (e.g., blocking unauthorized access).

Example in Splunk SOAR:A playbook can be configured to automatically respond to an unencrypted database storing customer data by triggering a compliance violation alert and notifying the compliance team.

Why Not the Other Options?

'L A. Integrating with legacy systems – While important, compliar
engineers should modernize legacy systems if they pose securit
workflows – Automation is beneficial, but it should not be prioritized over security and
compliance. Some security decisions require human oversight'L
employees – Efficiency is important, but security cannot be sacrificed to cut costs. Skilled SOC analysts and engineers are critical to cybersecurity defense.

Reference & Learning Resources

@=Ûl Splunk Docs – Security Essentials: https://docs.splunk.com
Dashboards: https://splunkbase.splunk.com/app/3435/@=Ûl Splunk
Compliance: https://www.splunk.com/en_us/products/soar.html@=
Framework & Splunk Integration: https://www.nist.gov/cyberframework

Question 3: (Single Select)

What is the primary purpose of data indexing in Splunk?

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

Correct Answer: B

https://examsindex.com/exam/splk-5002 Page 6 of 11

BONUS!!! Download part of Itbraindumps SPLK-5002 dumps for free: https://drive.google.com/open?id=11HOaCxVt-Eb0nHlv7w5zGLGmEKr6tD1t

If you are very busy, you can only take two or three hours a day to study our SPLK-5002 study engine. Then I tell you this is enough! After ten days you can go to the exam. With such an efficient product, you really can't find the second one! In any case, many people have passed the exam after using SPLK-5002 Training Materials. This is a fact that you must see. As long as you are still a sensible person, you will definitely choose SPLK-5002 practice quiz. Don't hesitate! Time does not wait!

If you use our products, I believe it will be very easy for you to successfully pass your SPLK-5002 exam. Of course, if you unluckily fail to pass your exam, don't worry, because we have created a mechanism for economical compensation. You just need to give us your test documents and transcript, and then our SPLK-5002 prep torrent will immediately provide you with a full refund, you will not lose money. More importantly, if you decide to buy our SPLK-5002 exam torrent, we are willing to give you a discount, you will spend less money and time on preparing for your SPLK-5002 exam.

>> SPLK-5002 Real Dumps <<

Splunk Certified Cybersecurity Defense Engineer test questions and dumps, SPLK-5002 exam cram

The best valid and most accurate Splunk SPLK-5002 exam study material can facilitate your actual test and save your time and money. Generally, you are confused by various study material for SPLK-5002 preparation. Now, please pay attention to Itbraindumps SPLK-5002 reliable study material, which is the best validity and authority training material for your preparation. The SPLK-5002 actual test will bring you full scores.

Splunk Certified Cybersecurity Defense Engineer Sample Questions (Q57-Q62):

NEW QUESTION # 57
What methods improve the efficiency of Splunk's automation capabilities? (Choose three)

- A. Using modular inputs
- B. Leveraging saved search acceleration
- C. Implementing low-latency indexing
- D. Employing prebuilt SOAR playbooks
- E. Optimizing correlation search queries

Answer: A,D,E

Explanation:
How to Improve Splunk's Automation Efficiency?
Splunk's automation capabilities rely on efficient data ingestion, optimized searches, and automated response workflows. The following methods help improve Splunk's automation:
#1. Using Modular Inputs (Answer A)
Modular inputs allow Splunk to ingest third-party data efficiently (e.g., APIs, cloud services, or security tools).
Benefit: Improves automation by enabling real-time data collection for security workflows.
Example: Using a modular input to ingest threat intelligence feeds and trigger automatic responses.
#2. Optimizing Correlation Search Queries (Answer B)
Well-optimized correlation searches reduce query time and false positives.
Benefit: Faster detections # Triggers automated actions in SOAR with minimal delay.
Example: Usingtstatsinstead of raw searches for efficient event detection.
#3. Employing Prebuilt SOAR Playbooks (Answer E)
SOAR playbooks automate security responses based on predefined workflows.
Benefit: Reduces manual effort in phishing response, malware containment, etc.
Example: Automating phishing email analysis using a SOAR playbook that extracts attachments, checks URLs, and blocks malicious senders.
Why Not the Other Options?
#C. Leveraging saved search acceleration - Helps with dashboard performance, but doesn't directly improve automation.#D. Implementing low-latency indexing - Reduces indexing lag but is not a core automation feature.
References & Learning Resources
#Splunk SOAR Automation Guide: https://docs.splunk.com/Documentation/SOAR#Optimizing Correlation Searches in Splunk ES: https://docs.splunk.com/Documentation/ES#Prebuilt SOAR Playbooks for Security Automation: https://splunkbase.splunk.com

NEW QUESTION # 58
What is the primary purpose of Splunk SOAR (Security Orchestration, Automation, and Response)?

- A. To automate and orchestrate security workflows
- B. To improve indexing performance
- C. To accelerate data ingestion
- D. To provide threat intelligence feeds

Answer: A

Explanation:
Splunk SOAR (Security Orchestration, Automation, and Response) helps SOC teams automate threat detection, investigation, and response by integrating security tools and orchestrating workflows.
Primary Purpose of Splunk SOAR:
Automates Security Tasks (B)
Reduces manual efforts by using playbooks to handle routine incidents automatically.
Accelerates threat mitigation by automating response actions (e.g., blocking malicious IPs, isolating endpoints).

Orchestrates Security Workflows (B)
Connects SIEM, threat intelligence, firewalls, endpoint security, and ITSM tools into a unified security workflow.
Ensures faster and more effective threat response across multiple security tools.

NEW QUESTION # 59
What is the purpose of using data models in building dashboards?

- A. To compress indexed data
- B. To reduce storage usage on Splunk instances
- C. To provide a consistent structure for dashboard queries
- D. To store raw data for compliance purposes

Answer: C

Explanation:
Why Use Data Models in Dashboards?
SplunkData Modelsallow dashboards toretrieve structured, normalized data quickly, improving search performance and accuracy.
#How Data Models Help in Dashboards?(AnswerB)#Standardized Field Naming- Ensures that queries always useconsistent field names(e.g.,src_ipinstead ofsource_ip).#Faster Searches- Data models allow dashboards torun structured searches instead of raw log queries.#Example:ASOC dashboard for user activity monitoringuses a CIM-compliantAuthentication Data Model, ensuring that querieswork across different log sources.
Why Not the Other Options?
#A. To store raw data for compliance purposes- Raw data is stored in indexes,not data models.#C. To compress indexed data- Data modelsstructuredata but donot perform compression.#D. To reduce storage usage on Splunk instances- Data modelshelp with search performance, not storage reduction.
References & Learning Resources
#Splunk Data Models for Dashboard Optimization: https://docs.splunk.com/Documentation/Splunk/latest /Knowledge/Aboutdatamodels#Building Efficient Dashboards Using Data Models: https://splunkbase.splunk. com#Using CIM-Compliant Data Models for Security Analytics: https://www.splunk.com/en_us/blog/tips- and-tricks

NEW QUESTION # 60
Which practices strengthen the development of Standard Operating Procedures (SOPs)?(Choosethree)

- A. Including detailed step-by-step instructions
- B. Excluding historical incident data
- C. Focusing solely on high-risk scenarios
- D. Regular updates based on feedback
- E. Collaborating with cross-functional teams

Answer: A,D,E

Explanation:
Why Are These Practices Essential for SOP Development?
Standard Operating Procedures (SOPs)are crucial for ensuring consistent, repeatable, and effective security operations in aSecurity Operations Center (SOC). Strengthening SOP development ensuresefficiency, clarity, and adaptabilityin responding to incidents.
1##Regular Updates Based on Feedback (Answer A)
Security threats evolve, andSOPs must be updatedbased onreal-world incidents, analyst feedback, and lessons learned.
Example: Anew ransomware variantis detected; theSOP is updatedto include aspecific containment playbookin Splunk SOAR.
2##Collaborating with Cross-Functional Teams (Answer C)
Effective SOPs requireinput from SOC analysts, threat hunters, IT, compliance teams, and DevSecOps.
Ensures thatall relevant security and business perspectivesare covered.
Example: ASOC team collaborates with DevOpsto ensure that acloud security response SOPaligns with AWS security controls.
3##Including Detailed Step-by-Step Instructions (Answer D)
SOPs should provideclear, actionable, and standardizedsteps for security analysts.
Example: ASplunk ES incident response SOPshould include:
How to investigate a security alertusing correlation searches.
How to escalate incidentsbased on risk levels.
How to trigger a Splunk SOAR playbookfor automated remediation.
Why Not the Other Options?

#B. Focusing solely on high-risk scenarios-All security events matter, not just high-risk ones.Low-level alertscan be early indicators of larger threats.#E. Excluding historical incident data- Past incidents providevaluable lessonsto improveSOPs and incident response workflows.
References & Learning Resources
#Best Practices for SOPs in Cybersecurity:https://www.nist.gov/cybersecurity-framework#Splunk SOAR Playbook SOP Development: https://docs.splunk.com/Documentation/SOAR#Incident Response SOPs with Splunk: https://splunkbase.splunk.com

NEW QUESTION # 61
What are key elements of a well-constructed notable event?(Choosethree)

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

Answer: A,B,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 # 62
.....

The Splunk SPLK-5002 Exam Questions give you a complete insight into each chapter and an easy understanding with simple and quick-to-understand language. The Splunk SPLK-5002 exam dumps are the best choice to make. The common problem Splunk SPLK-5002 Exam applicants face is seeking updated and real Splunk SPLK-5002 practice test questions to prepare successfully for the cherished Splunk Certified Cybersecurity Defense Engineer SPLK-5002 certification exam.

SPLK-5002 Reliable Dump: https://www.itbraindumps.com/SPLK-5002_exam.html

All these features of Splunk SPLK-5002 PDF format are just to facilitate your preparation for the SPLK-5002 examination, All SPLK-5002 study materials you should know are written in them with three versions to choose from, Splunk SPLK-5002 Real Dumps However, you can choose what kind of people you are going to get along with and what kind of way you are going to take, among which the choice of learning tools is also decided by you, Itbraindumps SPLK-5002 dumps PDF files make sure candidates pass exam for certain.

For example, many techniques require you to make selections or work with layers, Jeremy Shane Lisenbea, All these features of Splunk SPLK-5002 PDF format are just to facilitate your preparation for the SPLK-5002 examination.

Buy Actual Splunk SPLK-5002 Dumps Now and Receive Up to 365 Days of Free Updates

All SPLK-5002 study materials you should know are written in them with three versions to choose from, However, you can choose what kind of people you are going to get along with and what kind SPLK-5002 of way you are going to take, among which the

choice of learning tools is also decided by you.

Itbraindumps SPLK-5002 dumps PDF files make sure candidates pass exam for certain, We not only offer the best, valid and professional SPLK-5002 exam questions and answers but also the golden customer service that can satisfy you 100%, no matter you have any questions about SPLK-5002 exam questions torrent and answers, we will solve with you as soon as possible.

- Splunk SPLK-5002 Real Dumps - 100% Pass-Rate SPLK-5002 Reliable Dump and Realistic Valid Splunk Certified Cybersecurity Defense Engineer Test Cost □ Search for 《 SPLK-5002 》 and easily obtain a free download on （ www.vce4dumps.com ） □Exam SPLK-5002 Objectives Pdf
- Exam SPLK-5002 Experience □ Popular SPLK-5002 Exams □ SPLK-5002 Valid Exam Notes □ Copy URL ➥ www.pdfvce.com □ open and search for ➥ SPLK-5002 □ to download for free □Exam SPLK-5002 Experience
- Splunk Certified Cybersecurity Defense Engineer Latest Material Can Help You Save Much Time - www.exam4labs.com □ □ Immediately open ⇛ www.exam4labs.com ⇚ and search for ▸ SPLK-5002 ◂ to obtain a free download □SPLK-5002 New Dumps Questions
- SPLK-5002 Sample Questions Answers □ Exam Sample SPLK-5002 Questions □ SPLK-5002 Latest Exam Discount □ The page for free download of { SPLK-5002 } on ☀ www.pdfvce.com □☀□ will open immediately □SPLK-5002 Valid Mock Test
- SPLK-5002 – 100% Free Real Dumps | Useful Splunk Certified Cybersecurity Defense Engineer Reliable Dump □ Search for 《 SPLK-5002 》 and download exam materials for free through ▸ www.easy4engine.com ◂ □SPLK-5002 Latest Learning Materials
- Free PDF Splunk - Updated SPLK-5002 - Splunk Certified Cybersecurity Defense Engineer Real Dumps □ Open ➥ www.pdfvce.com □ enter [SPLK-5002] and obtain a free download ▸SPLK-5002 Latest Braindumps
- Splunk Certified Cybersecurity Defense Engineer Latest Material Can Help You Save Much Time - www.vce4dumps.com □ □ Immediately open { www.vce4dumps.com } and search for □ SPLK-5002 □ to obtain a free download □SPLK-5002 Latest Learning Materials
- SPLK-5002 Exam Sample Online □ SPLK-5002 Latest Learning Materials □ Popular SPLK-5002 Exams □ Search on 【 www.pdfvce.com 】 for □ SPLK-5002 □ to obtain exam materials for free download □SPLK-5002 Latest Exam Discount
- SPLK-5002 Real Dumps - Correct SPLK-5002 Reliable Dump Spend You Little Time and Energy to Prepare □ Download 【 SPLK-5002 】 for free by simply entering □ www.prepawaypdf.com □ website □SPLK-5002 Exam Sample Online
- SPLK-5002 Latest Exam Discount □ Exam SPLK-5002 Experience □ Exam SPLK-5002 Experience □ Copy URL ▸ www.pdfvce.com ◂ open and search for ➡ SPLK-5002 □□□ to download for free □Guaranteed SPLK-5002 Passing
- Latest SPLK-5002 Exam Test □ Exam SPLK-5002 Preparation □ SPLK-5002 Latest Learning Materials □ Search for ⇛ SPLK-5002 ⇚ and obtain a free download on ▸ www.easy4engine.com ◂ □Exam SPLK-5002 Preparation
- blanchevkyd250577.blogacep.com, elaineepll195786.estate-blog.com, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, ilovebookmark.com, wow-directory.com, 45listing.com, kobigjck534396.cosmicwiki.com, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, Disposable vapes

P.S. Free & New SPLK-5002 dumps are available on Google Drive shared by Itbraindumps: https://drive.google.com/open?id=11HOaCxVt-Eb0nHlv7w5zGLGmEKr6tD1t