Mock SPLK-5002 Exam - SPLK-5002 Authentic Exam Questions

What's more, part of that PDFBraindumps SPLK-5002 dumps now are free: https://drive.google.com/open?id=1mV8p3gHt_Vk7KSqTrbkJw_7vBNTjkqag

If you choose our study materials and use our products well, we can promise that you can pass the exam and get the SPLK-5002 certification. Then you will find you have so many chances to advance in stages to a great level of social influence and success. Our SPLK-5002 Dumps Torrent can also provide all candidates with our free demo, in order to exclude your concerts that you can check our products. We believe that you will be fond of our products.

Today is the right time to advance your career. Yes, you can do this easily. Just need to pass the SPLK-5002 certification exam. Are you ready for this? If yes then get registered in Splunk SPLK-5002 certification exam and start preparation with top-notch SPLK-5002 Exam Practice questions today. These SPLK-5002 questions are available at PDFBraindumps with up to 1 year of free updates. Download PDFBraindumps SPLK-5002 exam practice material demo and check out its top features.

>> Mock SPLK-5002 Exam <<

SPLK-5002 Practice Questions & SPLK-5002 Actual Lab Questions: Splunk Certified Cybersecurity Defense Engineer

Owing to the industrious dedication of our experts and other working staff, our SPLK-5002 study materials grow to be more mature and are able to fight against any difficulties. Our SPLK-5002 preparation exam have achieved high pass rate in the industry, and we always maintain a 99% pass rate on our SPLK-5002 Exam Questions with our endless efforts. We have to admit that behind such a starling figure, there embrace mass investments from our company. Since our company's establishment, we have devoted mass manpower, materials and financial resources into SPLK-5002 exam materials.

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	• 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 3	• 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 4	• 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 5	• 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.

Splunk Certified Cybersecurity Defense Engineer Sample Questions (Q27-Q32):

NEW QUESTION # 27
Which practices strengthen the development of Standard Operating Procedures (SOPs)?(Choosethree)

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

Answer: A,C,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 # 28
What is the main purpose of Splunk's Common Information Model (CIM)?

- A. To extract fields from raw events
- B. To create accelerated reports
- C. To compress data during indexing
- D. To normalize data for correlation and searches

Answer: D

Explanation:
What is the Splunk Common Information Model (CIM)?
Splunk's Common Information Model (CIM) is a standardized way to normalize and map event data from different sources to a common field format. It helps with:
Consistent searches across diverse log sources
Faster correlation of security events
Better compatibility with prebuilt dashboards, alerts, and reports
Why is Data Normalization Important?
Security teams analyze data from firewalls, IDS/IPS, endpoint logs, authentication logs, and cloud logs.
These sources have different field names (e.g., "src_ip" vs. "source_address").
CIM ensures a standardized format, so correlation searches work seamlessly across different log sources.
How CIM Works in Splunk?
#Maps event fields to a standardized schema#Supports prebuilt Splunk apps like Enterprise Security (ES)
#Helps SOC teams quickly detect security threats
#Example Use Case:
A security analyst wants to detect failed admin logins across multiple authentication systems.
Without CIM, different logs might use:
user_login_failed
auth_failure
login_error
With CIM, all these fields map to the same normalized schema, enabling one unified search query.
Why Not the Other Options?
#A. Extract fields from raw events - CIM does not extract fields; it maps existing fields into a standardized format.#C. Compress data during indexing - CIM is about data normalization, not compression.#D. Create accelerated reports - While CIM supports acceleration, its main function is standardizing log formats.
References & Learning Resources
#Splunk CIM Documentation: https://docs.splunk.com/Documentation/CIM#How Splunk CIM Helps with Security Analytics: https://www.splunk.com/en_us/solutions/common-information-model.html#Splunk Enterprise Security & CIM Integration: https://splunkbase.splunk.com/app/263

NEW QUESTION # 29
Which practices improve the effectiveness of security reporting?(Choosethree)

- A. Providing actionable recommendations
- B. Using dynamic filters for better analysis
- C. Customizing reports for different audiences
- D. Including unrelated historical data for context
- E. Automating report generation

Answer: A,C,E

Explanation:
Effective security reporting helps SOC teams, executives, and compliance officers make informed decisions.

#1. Automating Report Generation (A)
Saves time by scheduling reports for regular distribution.
Reduces manual effort and ensures timely insights.
Example:
A weekly phishing attack report sent to SOC analysts.
#2. Customizing Reports for Different Audiences (B)
Technical reports for SOC teams include detailed event logs.
Executive summaries provide risk assessments and trends.
Example:
SOC analysts see incident logs, while executives get a risk summary.
#3. Providing Actionable Recommendations (D)
Reports should not just show data but suggest actions.
Example:
If failed login attempts increase, recommend MFA enforcement.
#Incorrect Answers:
C: Including unrelated historical data for context # Reports should be concise and relevant.
E: Using dynamic filters for better analysis # Useful in dashboards, but not a primary factor in reporting effectiveness.
#Additional Resources:
Splunk Security Reporting Guide
Best Practices for Security Metrics

NEW QUESTION # 30
What is the primary purpose of data indexing in Splunk?

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

Answer: A

Explanation:
Understanding Data Indexing in Splunk
In Splunk Enterprise Security (ES) and Splunk SOAR, data indexing is a fundamental process that enables efficient storage, retrieval, and searching of data.
#Why is Data Indexing Important?
Stores raw machine data (logs, events, metrics) in a structured manner.
Enables fast searching through optimized data storage techniques.
Uses an indexer to process, compress, and store data efficiently.
Why the Correct Answer is B?
Splunk indexes data to store it efficiently while ensuring fast retrieval for searches, correlation searches, and analytics.
It assigns metadata to indexed events, allowing SOC analysts to quickly filter and search logs.
#Incorrect Answers & Explanations
A: To ensure data normalization # Splunk normalizes data using Common Information Model (CIM), not indexing.
C: To secure data from unauthorized access # Splunk uses RBAC (Role-Based Access Control) and encryption for security, not indexing.
D: To visualize data using dashboards # Dashboards use indexed data for visualization, but indexing itself is focused on data storage and retrieval.
#Additional Resources:
Splunk Data Indexing Documentation
Splunk Architecture & Indexing Guide

NEW QUESTION # 31
Which action improves the effectiveness of notable events in Enterprise Security?

- A. Applying suppression rules for false positives
- B. Disabling scheduled searches
- C. Limiting the search scope to one index

- D. Using only raw log data in searches

Answer: A

Explanation:
Notable events in Splunk Enterprise Security (ES) are triggered by correlation searches, which generate alerts when suspicious activity is detected. However, if too many false positives occur, analysts waste time investigating non-issues, reducing SOC efficiency.
How to Improve Notable Events Effectiveness:
Apply suppression rules to filter out known false positives and reduce alert fatigue.
Refine correlation searches by adjusting thresholds and tuning event detection logic.
Leverage risk-based alerting (RBA) to prioritize high-risk events.
Use adaptive response actions to enrich events dynamically.
By suppressing false positives, SOC analysts focus on real threats, making notable events more actionable.
Thus, the correct answer is A. Applying suppression rules for false positives.
References:
Managing Notable Events in Splunk ES
Best Practices for Tuning Correlation Searches
Using Suppression in Splunk ES

NEW QUESTION # 32
.....

Perhaps you have had such an unpleasant experience about SPLK-5002 exam questions you brought in the internet was not suitable for you in actual use, to avoid this, our company has prepared SPLK-5002 free demo in this website for our customers, with which you can have your first-hand experience before making your final decision. The content of the free demo is part of the content in our real SPLK-5002 Study Guide. And you can see how excellent our SPLK-5002 training dumps are!

myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, www.stes.tyc.edu.tw, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, Disposable vapes

BTW, DOWNLOAD part of PDFBraindumps SPLK-5002 dumps from Cloud Storage: https://drive.google.com/open?id=1mV8p3gHt_Vk7KSqTrbkJw_7vBNTjkqag