Useful SPLK-5002 Latest Braindumps Pdf Provide Prefect Assistance in SPLK-5002 Preparation

What's more, part of that PassTestking SPLK-5002 dumps now are free: https://drive.google.com/open?id=1rhPTTwey53SVqb595ZVXbK4IjbtHIXyK

The practice test is a convenient tool to identify weak points in the Splunk Certified Cybersecurity Defense Engineer preparation. You can easily customize the level of difficulty of Splunk SPLK-5002 Practice Test to suit your study tempo. Our web-based practice test is an ideal way to create an Splunk exam-like situation.

You can use this Splunk Certified Cybersecurity Defense Engineer (SPLK-5002) practice exam software to test and enhance your Splunk Certified Cybersecurity Defense Engineer (SPLK-5002) exam preparation. Your practice will be made easier by having the option to customize the Splunk in SPLK-5002 exam dumps. Only Windows-based computers can run this Splunk SPLK-5002 Exam simulation software. The fact that it runs without an active internet connection is an incredible comfort for users who don't have access to the internet all the time.

>> SPLK-5002 Latest Braindumps Pdf <<

Reliable SPLK-5002 Dumps Pdf, Download SPLK-5002 Pdf

The Splunk Certified Cybersecurity Defense Engineer (SPLK-5002) exam questions can help you gain the high-in-demand skills and credentials you need to pursue a rewarding career. To do this you just need to pass the Splunk Certified Cybersecurity Defense Engineer (SPLK-5002) certification exam which is not easy to crack. You have to put in some extra effort, and time and prepare thoroughly to pass the Splunk SPLK-5002 Exam. For the quick, complete, and comprehensive Splunk Certified Cybersecurity Defense Engineer (SPLK-5002) exam dumps preparation you can get help from top-notch and easy-to-use SPLK-5002 Questions.

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	• 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 3	• 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 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	• 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.

Splunk Certified Cybersecurity Defense Engineer Sample Questions (Q17-Q22):

NEW QUESTION # 17
What should a security engineer prioritize when building a new security process?

- A. Integrating it with legacy systems
- B. Reducing the overall number of employees required
- C. Ensuring it aligns with compliance requirements
- D. Automating all workflows within the process

Answer: C

Explanation:
When aSecurity Engineeris building a new security process, theirtop priorityshould be ensuring that the process aligns withcompliance requirements. This is crucial because compliance dictates the legal, regulatory, and industry standards that organizations must follow to protect sensitive data and maintain trust.
Why Compliance is the Top Priority?
Legal and Regulatory Obligations- Many industries are required to follow compliance standards such asGDPR, HIPAA, PCI-DSS, NIST, ISO 27001, and SOX. Non-compliance can lead toheavy fines and legal actions.
Data Protection & Privacy- Compliance ensures that sensitive information is handled securely, preventingdata breachesandunauthorized access.
Risk Reduction- Following compliance standards helps mitigate cybersecurity risks byimplementing security best practicessuch as encryption, access controls, and logging.
Business Reputation & Trust- Organizations that comply with standards buildcustomer confidence and industry credibility.
Audit Readiness- Security teams must ensure that logs, incidents, and processes align with compliance frameworks topass internal/external auditseasily.
How Does Splunk Enterprise Security (ES) Help with Compliance?
Splunk ES is aSecurity Information and Event Management (SIEM)tool that helps organizations meet compliance requirements by:
#Log Management & Retention- Stores and correlates security logs forauditability and forensic investigation.
#Real-time Monitoring & Alerts- Detects suspicious activity andalerts SOC teams.#Prebuilt Compliance Dashboards- Comes with out-of-the-box dashboards forPCI-DSS, GDPR, HIPAA, NIST 800-53, and other frameworks.#Automated Reporting- Generates reports that can be used forcompliance audits.
Example in Splunk ES:A security engineer can createcorrelation searches and risk-based alerting (RBA)to monitor and enforce compliance policies.
How Does Splunk SOAR Help Automate Compliance-Driven Security Processes?
Splunk SOAR (Security Orchestration, Automation, and Response) enhances compliance processes by:
#Automating Incident Response- Ensures that responses to security threats followpredefined compliance guidelines.#Automated Evidence Collection- Helps inaudit documentationby automatically collecting logs, alerts, and incident data.#Playbooks for Compliance Violations- Can automaticallydetect and remediatenon- compliant actions (e.g., blocking unauthorized access).
Example in Splunk SOAR:Aplaybookcan be configured to automaticallyrespond to an unencrypted database storing customer databy triggering a compliance violation alert and notifying the compliance team.
Why Not the Other Options?
#A. Integrating with legacy systems- While important,compliance is a higher priority. Security engineers shouldmodernizelegacy

systems if they pose security risks.#C. Automating all workflows- Automation is beneficial, but it should not be prioritizedover security and compliance. Some security decisions requirehuman oversight.#D. Reducing the number of employees- Efficiency is important, butsecurity cannot be sacrificedto cut costs. Skilled SOC analysts and engineers arecritical to cybersecurity defense.
References & Learning Resources
#Splunk Docs - Security Essentials: https://docs.splunk.com/#Splunk ES Compliance Dashboards: https://splunkbase.splunk.com/app/3435/#Splunk SOAR Playbooks for Compliance: https://www.splunk.com/en_us/products/soar.html#NIST Cybersecurity Framework & Splunk Integration: https://www.nist.gov/cyberframework

NEW QUESTION # 18
Which components are necessary to develop a SOAR playbook in Splunk?(Choosethree)

- A. Threat intelligence feeds
- B. Manual approval processes
- C. Integration with external tools
- D. Actionable steps or tasks
- E. Defined workflows

Answer: C,D,E

Explanation:
Splunk SOAR (Security Orchestration, Automation, and Response) playbooks automate security processes, reducing response times.
#1. Defined Workflows (A)
A structured flowchart of actions for handling security events.
Ensures that the playbook follows a logical sequence (e.g., detect # enrich # contain # remediate).
Example:
If a phishing email is detected, the workflow includes:
Extract email artifacts (e.g., sender, links).
Check indicators against threat intelligence feeds.
Quarantine the email if it is malicious.
#2. Actionable Steps or Tasks (C)
Each playbook contains specific, automated steps that execute responses.
Examples:
Extracting indicators from logs.
Blocking malicious IPs in firewalls.
Isolating compromised endpoints.
#3. Integration with External Tools (E)
Playbooks must connect with SIEM, EDR, firewalls, threat intelligence platforms, and ticketing systems.
Uses APIs and connectors to integrate with tools like:
Splunk ES
Palo Alto Networks
Microsoft Defender
ServiceNow
#Incorrect Answers:
B: Threat intelligence feeds # These enrich playbooks but are not mandatory components of playbook development.
D: Manual approval processes # Playbooks are designed for automation, not manual approvals.
#Additional Resources:
Splunk SOAR Playbook Documentation
Best Practices for Developing SOAR Playbooks

NEW QUESTION # 19
Which of the following cURL commands would allow an engineer to effectively disable the REST API endpoint they've been utilizing for testing a detection named TestSearchDevelopment?

- A. curl -k -u admin:pass https://localhost:8089/servicesNS/admin/search/saved/searches/TestSearchDevelopment/ -X DELETE
- B. curl -k -u admin:pass

https://localhost:8089/servicesNS/admin/search/saved/searches/TestSearchDevelopment/disable
-X POST

- C. Splunk endpoints cannot be disabled.
- D. curl -k -u admin:pass
https://localhost:8089/servicesNS/admin/search/saved/searches/TestSearchDevelopment/disable
-X PUT

Answer: B

Explanation:
To disable a saved search (detection) via the Splunk REST API, the correct syntax is a POST request to the .../disable endpoint.
Thus, the proper cURL command is curl -k -u admin:pass
https://localhost:8089/servicesNS/admin/search/saved/searches/TestSearchDevelopment/disable
-X POST

NEW QUESTION # 20
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 # 21
A new playbook needs to be developed for automated phishing analysis and response.
Configured in SOAR are integrations with Splunk Enterprise Security and actions from assets that pull in user-reported emails, perform automated threat analysis, add blocks on the proxy, and an EDR vendor to take various actions. Which would be the best workflow for the new playbook?

- A. 1. Ingest the email from the mail vendor
2. Detonate email in the automated threat analysis system and collect verdict, looking for malicious indicators
3. Search the mail system for all users that received the email
4. Block any malicious URLs and processes with the proxy and EDR solutions
- B. 1. Ingest the email from the mail vendor
2. Detonate email in the automated threat analysis system and collect verdict, looking for malicious indicators
3. Search the mail system for all users that received the email
4. Block all URLs and processes with the proxy and EDR solutions
- C. 1. Submit the email from Splunk Enterprise Security
2. Search the mail system for all users that received the email
3. Review results from the automated threat analysis
4. Block any malicious URLs and processes with the proxy and EDR solutions
- D. 1. Submit the user reported email from Splunk Enterprise Security
2. Search the mail system for all users that received the email
3. Review results from the automated threat analysis
4. Block any malicious URLs and processes with the proxy and EDR solutions

Answer: A

Explanation:
The best workflow for automated phishing analysis and response is:
1. Ingest the email from the mail vendor - acquire the reported email for analysis.
2. Detonate the email in the automated threat analysis system and collect verdict - determine if the email is malicious and extract indicators.
3. Search the mail system for all users that received the email - identify impacted users.
4. Block any malicious URLs and processes with the proxy and EDR solutions - take targeted remediation based on verified malicious indicators.

NEW QUESTION # 22
.....

Our company is a professional exam dumps material providers, with occupying in this field for years, and we are quite familiar with compiling the SPLK-5002 exam materialls. If you choose us, we will give you free update for one year after purchasing. Besides, the quality of SPLK-5002 Exam Dumps is high, they contain both questions and answers, and you can practice first before seeing the answers. Choosing us means you choose to pass the exam successfully.