퍼펙트한SPLK-5002완벽한덤프공부자료최신덤프

ExamPassdump SPLK-5002 최신 PDF 버전 시험 문제집을 무료로 Google Drive에서 다운로드하세요: https://drive.google.com/open?id=1FPQZlk1Z8lm1TFZNVpZvouyXqsShkubb

Splunk SPLK-5002인증은 아주 중요한 인증시험중의 하나입니다. ExamPassdump의 베터랑의 전문가들이 오랜 풍부한 경험과 IT지식으로 만들어낸 IT관연인증시험 자격증자료들입니다. 이런 자료들은 여러분이Splunk인증시험중의SPLK-5002시험을 안전하게 패스하도록 도와줍니다. ExamPassdump에서 제공하는 덤프들은 모두 100%통과 율을 보장하며 그리고 일년무료 업뎃을 제공합니다

Splunk SPLK-5002 시험요강:

주제	소개
주제 1	• 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.
주제 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.

주제 3	• 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.
주제 4	• 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.
주제 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.

SPLK-5002시험문제 & SPLK-5002퍼펙트 최신 덤프모음집

SPLK-5002시험은 영어로 출제되는 만큼 시험난이도가 높다고 볼수 있습니다.하지만 SPLK-5002덤프만 있다면 아무리 어려운 시험도 쉬워집니다. 오르지 못할 산도 정복할수 있는게 SPLK-5002덤프의 우점입니다.SPLK-5002덤프로 시험을 패스하여 자격증을 취득하시면 굳게 닫혔던 취업문도 자신있게 두드릴수 있습니다. SPLK-5002덤프를 구매하시고 공부하시면 밝은 미래를 예약한것과 같습니다.

최신 Cybersecurity Defense Analyst SPLK-5002 무료샘플문제 (Q13-Q18):

질문 # 13
What elements are critical for developing meaningful security metrics? (Choose three)

- A. Consistent definitions for key terms
- B. Regular data validation
- C. Avoiding integration with third-party tools
- D. Visual representation through dashboards
- E. Relevance to business objectives

정답： A,B,E

설명:
Key Elements of Meaningful Security Metrics
Security metrics shouldalign with business goals, be validated regularly, and have standardized definitionsto ensure reliability.
#1. Relevance to Business Objectives (A)
Security metrics should tie directly tobusiness risks and priorities.
Example:
A financial institution might trackfraud detection ratesinstead of genericmalware alerts.
#2. Regular Data Validation (B)
Ensures data accuracy byremoving false positives, duplicates, and errors.
Example:
Validatingphishing alert effectivenessby cross-checking withuser-reported emails.
#3. Consistent Definitions for Key Terms (E)
Standardized definitions preventmisinterpretation of security metrics.
Example:
Clearly definingMTTD (Mean Time to Detect) vs. MTTR (Mean Time to Respond).
#Incorrect Answers:
C: Visual representation through dashboards# Dashboards help, butdata quality matters more.
D: Avoiding integration with third-party tools# Integrations withSIEM, SOAR, EDR, and firewallsarecrucial for effective metrics.
#Additional Resources:
NIST Security Metrics Framework

Splunk

질문 # 14
Which of the following should be the primary reference when designing a new playbook in Splunk SOAR?

- A. Existing Standard Operating Procedure
- B. MITRE ATT&CK framework
- C. Existing investigation actions
- D. CIS Framework

정답：A

설명：
When designing a new playbook in Splunk SOAR, the existing Standard Operating Procedure (SOP) should be the primary reference. SOPs define the approved steps and workflows for analysts, ensuring that automated playbooks align with organizational processes and compliance requirements.

질문 # 15
Consider the following series of events:
4:00 GMT Detection runs for interval 3:30-4:00
4:30 GMT Detection runs for interval 4:00-4:30
4:35 GMT Event 1 occurs on an endpoint
4:45 GMT Event 1 is indexed
5:00 GMT Detection runs for interval 4:30-5:00
5:05 GMT Event 1 finding is added to ES with timestamp 4:35
5:24 GMT Event 2 occurs on an endpoint
5:30 GMT Detection runs for interval 5:00-5:30
5:35 GMT Event 2 is indexed
6:00 GMT Detection runs for interval 5:30-6:00
What is the problem with the detection schedule chosen and how can it be solved?

- A. The logs are delayed so the detection time window needs to be decreased.
- B. The time window for the detection is too large, causing duplicate alerts.
- C. The logs are delayed so the detection time window needs to be increased.
- D. The time window for the detection is too small, causing duplicate alerts.

정답：C

설명：
In this scenario, events are indexed after the scheduled detection window has already executed, meaning detections miss relevant events. This happens due to log ingestion delay. The solution is to increase the detection time window (or use a delay offset) so that detections account for delayed logs, ensuring events like Event 1 and Event 2 are included in the proper detection run.

질문 # 16
What is the role of aggregation policies in correlation searches?

- A. To group related notable events for analysis
- B. To index events from multiple sources
- C. To automate responses to critical events
- D. To normalize event fields for dashboards

정답：A

설명：
Aggregation policies in Splunk Enterprise Security (ES) are used to group related notable events, reducing alert fatigue and improving incident analysis.
Role of Aggregation Policies in Correlation Searches:
Group Related Notable Events (A)

Helps SOC analysts see a single consolidated event instead of multiple isolated alerts.
Uses common attributes like user, asset, or attack type to aggregate events.
Improves Incident Response Efficiency
Reduces the number of duplicate alerts, helping analysts focus on high-priority threats.

질문 # 17
A company wants to create a dashboard that displays normalized event data from various sources.
Whatapproach should they use?

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

정답：C

설명：
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.

질문 # 18
.....

- SPLK-5002높은 통과율 덤프문제 □ SPLK-5002최신 시험대비자료 □ SPLK-5002인기시험자료 □ 시험 자료를 무료로 다운로드하려면➥ www.itdumpskr.com □을 통해➤ SPLK-5002 □를 검색하십시오SPLK-5002시험문제모음
- 시험대비 SPLK-5002완벽한 덤프공부자료 덤프데모문제 다운 □▶ www.itdumpskr.com◀은⇛ SPLK-5002 ⇚무료 다운로드를 받을 수 있는 최고의 사이트입니다SPLK-5002인증 시험덤프
- amierpob454710.bloggip.com, brontebyfj369380.theisblog.com, marchzsh151574.blogripley.com, getidealist.com, sachinvajc971701.eveowiki.com, www.stes.tyc.edu.tw, haarispgph464492.answerblogs.com, saulbria159955.wannawiki.com, mariahafte609955.blogdosaga.com, roywouv526052.hazeronwiki.com, Disposable vapes

그 외, ExamPassdump SPLK-5002 시험 문제집 일부가 지금은 무료입니다: https://drive.google.com/open?id=1FPQZlk1Z8lm1TFZNVpZvouyXqsShkubb