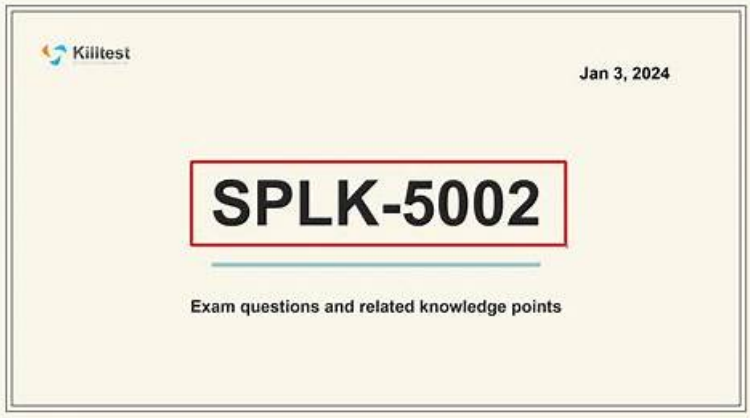
완벽한SPLK-5002인증시험대비공부자료시험덤프로시험패스가능



그 외, ITDumpsKR SPLK-5002 시험 문제집 일부가 지금은 무료입니다: https://drive.google.com/open?id=1fw41-b-MdfCGzbodMCGUmJlpCjxFivKN

Splunk SPLK-5002 덤프가 고객님의 기대를 가득 채워드릴수 있도록 정말로 노력하고 있는 ITDumpsKR랍니다. Splunk SPLK-5002 덤프는 pdf버전과 소프트웨어버전으로만 되어있었는데 최근에는 휴대폰에서가 사용가능한 온라인버전까지 개발하였습니다. 날따라 새로운 시스템을 많이 개발하여 고객님께 더욱 편하게 다가갈수 있는 ITDumpsKR가 되겠습니다.

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	• 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 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.
주제 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.
주제 5	• 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.

SPLK-5002인증시험대비 공부자료 완벽한 시험자료

ITDumpsKR는 고객님께서 첫번째Splunk SPLK-5002시험에서 패스할수 있도록 최선을 다하고 있습니다. 만일 어떤 이유로 인해 고객이 첫 번째 시도에서 실패를 한다면, ITDumpsKR는 고객에게Splunk SPLK-5002덤프비용 전액을 환불 해드립니다.환불보상은 다음의 필수적인 정보들을 전제로 합니다.

최신 Cybersecurity Defense Analyst SPLK-5002 무료샘플문제 (Q105-Q110):

질문 # 105
What methods can improve Splunk's indexing performance?(Choosetwo)

- A. Use universal forwarders for data ingestion.
- B. Optimize event breaking rules.
- C. Create multiple search heads.
- D. Enable indexer clustering.

정답：B,D

설명：
Improving Splunk's indexing performance is crucial for handling large volumes of data efficiently while maintaining fast search speeds and optimized storage utilization.
Methods to Improve Indexing Performance:
Enable Indexer Clustering (A)
Distributes indexing load across multiple indexers.
Ensures high availability and fault tolerance by replicating indexed data.
Optimize Event Breaking Rules (D)
Defines clear event boundaries to reduce processing overhead.
Uses correctLINE_BREAKERandTRUNCATEsettings to improve parsing speed.

질문 # 106
Which components are necessary to develop a SOAR playbook in Splunk?(Choosethree)

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

정답：C,D,E

설명：
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

질문 # 107
What are essential steps in developing threat intelligence for a security program?(Choosethree)

- A. Operationalizing intelligence through workflows
- B. Collecting data from trusted sources
- C. Creating dashboards for executives
- D. Conducting regular penetration tests
- E. Analyzing and correlating threat data

정답： A,B,E

설명:
Threat intelligence in Splunk Enterprise Security (ES) enhances SOC capabilities by identifying known attack patterns, suspicious activity, and malicious indicators.
Essential Steps in Developing Threat Intelligence:
Collecting Data from Trusted Sources (A)
Gather data from threat intelligence feeds (e.g., STIX, TAXII, OpenCTI, VirusTotal, AbuseIPDB).
Include internal logs, honeypots, and third-party security vendors.
Analyzing and Correlating Threat Data (C)
Use correlation searches to match known threat indicators against live data.
Identify patterns in network traffic, logs, and endpoint activity.
Operationalizing Intelligence Through Workflows (E)
Automate responses using Splunk SOAR (Security Orchestration, Automation, and Response).
Enhance alert prioritization by integrating intelligence into risk-based alerting (RBA).

질문 # 108
What is the main purpose of Splunk's Common Information Model (CIM)?

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

정답： C

설명:
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

질문 # 109
How can Splunk engineers monitor indexing performance effectively?(Choosetwo)

- A. Create correlation searches on indexed data.
- B. Use the Monitoring Console.
- C. Enable detailed event logging for indexers.
- D. Track indexer queue size and throughput.

정답： B,D

설명：
Monitoring indexing performance in Splunk is crucial for ensuring efficient data ingestion, search performance, and resource utilization.
Methods to Monitor Indexing Performance Effectively:
Use the Monitoring Console (A)
Provides real-time visibility into indexing performance.
Displays resource utilization, indexing rate, queue health, and disk usage.
Track Indexer Queue Size and Throughput (D)
Monitoring queue sizes prevents indexing bottlenecks.
Ensures data is processed efficiently without delays.

질문 # 110
.....

- Splunk SPLK-5002최신버전덤프, 는 모든 SPLK-5002시험내용을 커버합니다! □ ⇒ www.exampassdump.com ⇐ 을(를) 열고 （ SPLK-5002 ）를 검색하여 시험 자료를 무료로 다운로드하십시오SPLK-5002최신 업데이트 덤프문제
- SPLK-5002합격보장 가능 시험덤프 □ SPLK-5002시험패스 가능한 공부 □ SPLK-5002최신 시험 최신 덤프자료 □ □ www.itdumpskr.com □의 무료 다운로드“ SPLK-5002 ”페이지가 지금 열립니다SPLK-5002시험패스 덤프공부자료
- Splunk SPLK-5002최신버전덤프, 는 모든 SPLK-5002시험내용을 커버합니다! □ 검색만 하면（ www.dumptop.com ）에서▷ SPLK-5002 ◁무료 다운로드SPLK-5002최신 업데이트 덤프문제
- 시험준비에 가장 좋은 SPLK-5002인증시험대비 공부자료 공부 □ 검색만 하면□ www.itdumpskr.com □에서▷ SPLK-5002 ◁무료 다운로드SPLK-5002최고덤프공부
- SPLK-5002인증시험대비 공부자료 기출문제 □ 무료 다운로드를 위해➡ SPLK-5002 □□□를 검색하려면[www.dumptop.com]을(를) 입력하십시오SPLK-5002최고품질 시험대비자료
- SPLK-5002최고품질 시험대비자료 □ SPLK-5002최신 시험 최신 덤프자료 □ SPLK-5002시험대비 덤프 최신버전 □ 검색만 하면✔ www.itdumpskr.com □✔□에서《 SPLK-5002 》무료 다운로드SPLK-5002퍼펙트 덤프 최신자료
- SPLK-5002인증시험대비 공부자료 시험준비에 가장 좋은 인기시험 기출문제자료 □ 무료로 다운로드하려면➥ www.pass4test.net □로 이동하여⇛ SPLK-5002 ⇚를 검색하십시오SPLK-5002퍼펙트 덤프 샘플문제 다운
- jakubgxja529679.onzeblog.com, 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, totalbookmarking.com, sashaxbiq316777.shoutmyblog.com, kbookmarking.com, majaldox634757.jasperwiki.com, anitaokpw597814.blog-eye.com, socialmediaentry.com, kallumzyjq056267.homewikia.com, mindsplushearts.com, Disposable vapes

그리고 ITDumpsKR SPLK-5002 시험 문제집의 전체 버전을 클라우드 저장소에서 다운로드할 수 있습니다: https://drive.google.com/open?id=1fw41-b-MdfCGzbodMCGUmJlpCjxFivKN