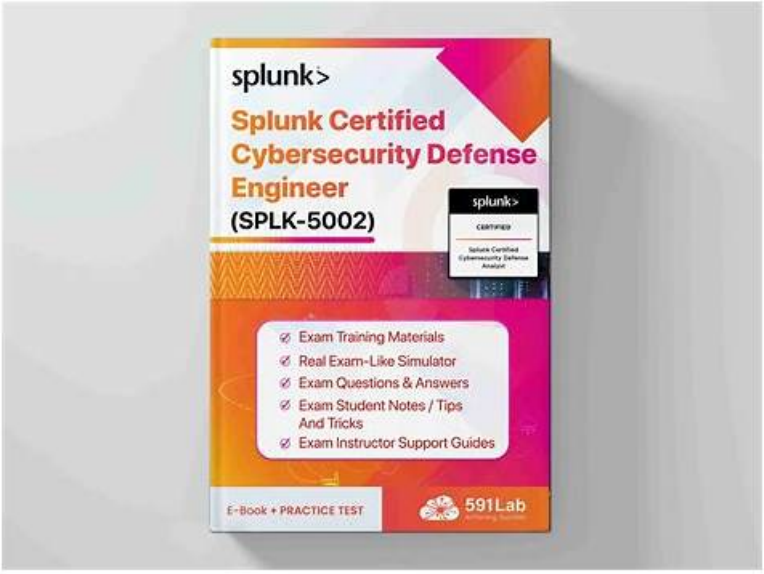
Splunk SPLK-5002최고품질시험덤프자료, SPLK-5002 시험덤프



참고: ExamPassdump에서 Google Drive로 공유하는 무료, 최신 SPLK-5002 시험 문제집이 있습니다: https://drive.google.com/open?id=1FPQZlk1Z8lm1TFZNVpZvouyXqsShkubb

Splunk SPLK-5002인증시험은 현재IT인사들 중 아주 인기 잇는 인증시험입니다.Splunk SPLK-5002시험패스는 여러분의 하시는 일과 생활에서 많은 도움을 줄뿐만 아니라 중요한 건 여러분의IT업계에서의 자기만의 자리를 지키실 수 잇습니다.이렇게 좋은 시험이니 많은 분들이 응시하려고 합니다,하지만 패스 율은 아주 낮습니다.

ExamPassdump 에서는 IT인증시험에 대비한 퍼펙트한Splunk 인증SPLK-5002덤프를 제공해드립니다. 시험공부할 시간이 충족하지 않은 분들은ExamPassdump 에서 제공해드리는Splunk 인증SPLK-5002덤프로 시험준비를 하시면 자격증 취득이 쉬워집니다. 덤프를 구매하시면 일년무료 업데이트서비스도 받을수 있습니다.

>> Splunk SPLK-5002최고품질 시험덤프자료 <<

높은 통과율 SPLK-5002최고품질 시험덤프자료 시험자료

경쟁율이 치열한 IT업계에서 아무런 목표없이 아무런 희망없이 무미건조한 생활을 하고 계시나요? 다른 사람들이 모두 취득하고 있는 자격증에 관심도 없는 분은 치열한 경쟁속에서 살아남기 어렵습니다. Splunk인증 SPLK-5002시험패스가 힘들다한들ExamPassdump덤프만 있으면 어려운 시험도 쉬워질수 밖에 없습니다. Splunk인증 SPLK-5002덤프에 있는 문제만 잘 이해하고 습득하신다면Splunk인증 SPLK-5002시험을 패스하여 자격증을 취득해 자신의 경쟁율을 업그레이드하여 경쟁시대에서 안전감을 보유할수 있습니다.

Splunk SPLK-5002 시험요강:

주제	소개
주제 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.
주제 2	• 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 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.
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.

최신 Cybersecurity Defense Analyst SPLK-5002 무료샘플문제 (Q42-Q47):

질문 # 42
A company wants to implement risk-based detection for privileged account activities.
Whatshould they configure first?

- A. Event sampling for raw data
- B. Asset and identity information for privileged accounts
- C. Automated dashboards for all accounts
- D. Correlation searches with low thresholds

정답： B

설명:
Why Configure Asset & Identity Information for Privileged Accounts First?
Risk-based detection focuses on identifying and prioritizing threats based on the severity of their impact. For privileged accounts (admins, domain controllers, finance users), understanding who they are, what they access, and how they behave is critical.
#Key Steps for Risk-Based Detection in Splunk ES:1##Define Privileged Accounts & Groups - Identify high- risk users (Admin, HR, Finance, CISO).2##Assign Risk Scores - Apply higher scores to actions involving privileged users.3##Enable Identity & Asset Correlation - Link users to assets for better detection.
4##Monitor for Anomalies - Detect abnormal login patterns, excessive file access, or unusual privilege escalation.
#Example in Splunk ES:
A domain admin logs in from an unusual location # Trigger high-risk alert A finance director downloads sensitive payroll data at midnight # Escalate for investigation Why Not the Other Options?
#B. Correlation searches with low thresholds - May generate excessive false positives, overwhelming the SOC.#C. Event sampling for raw data - Doesn't provide context for risk-based detection.#D. Automated dashboards for all accounts - Useful for visibility, but not the first step for risk-based security.
References & Learning Resources
#Splunk ES Risk-Based Alerting (RBA): https://www.splunk.com/en_us/blog/security/risk-based-alerting.
html#Privileged Account Monitoring in Splunk: https://docs.splunk.com/Documentation/ES/latest/User
/RiskBasedAlerting#Implementing Privileged Access Security (PAM) with Splunk: https://splunkbase.splunk.
com

질문 # 43
How can Splunk engineers monitor indexing performance effectively?(Choosetwo)

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

정답： C,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 # 44
Which sourcetype configurations affect data ingestion?(Choosethree)

- A. Event breaking rules
- B. Timestamp extraction
- C. Line merging rules
- D. Data retention policies

정답: A,B,C

설명:
The sourcetype in Splunk defines how incoming machine data is interpreted, structured, and stored. Proper sourcetype configurations ensure accurate event parsing, indexing, and searching.
#1. Event Breaking Rules (A)
Determines how Splunk splits raw logs into individual events.
If misconfigured, a single event may be broken into multiple fragments or multiple log lines may be combined incorrectly.
Controlled using LINE_BREAKER and BREAK_ONLY_BEFORE settings.
#2. Timestamp Extraction (B)
Extracts and assigns timestamps to events during ingestion.
Incorrect timestamp configuration leads to misplaced events in time-based searches.
Uses TIME_PREFIX, MAX_TIMESTAMP_LOOKAHEAD, and TIME_FORMAT settings.
#3. Line Merging Rules (D)
Controls whether multiline events should be combined into a single event.
Useful for logs like stack traces or multi-line syslog messages.
Uses SHOULD_LINEMERGE and LINE_BREAKER settings.
C: Data Retention Policies #
Affects storage and deletion, not data ingestion itself.
#Additional Resources:
Splunk Sourcetype Configuration Guide
Event Breaking and Line Merging

질문 # 45
A Detection Engineer works closely with SOC leads to define expected analyst workflows, often documented as a Standard Operating Procedure (SOP). Which capability can be used to document expected analyst actions in an investigation?

- A. Correlation Search Editor
- B. Adaptive response actions
- C. Response templates
- D. Investigation notes

정답: C

설명:
Response templates in Splunk Mission Control can be used to document and standardize expected analyst actions during an investigation. They align with SOPs and ensure analysts follow consistent workflows when responding to findings.

질문 # 46
An effective method for building automation workflows is to follow the OODA (Observe, Orient, Decide, Act) loop stages. When transitioning between the Decide and Act stages, what additional work should be included before automating the Act stage?

- A. Validate if the asset, identity, or service has an exemption.
- B. Create a new automation playbook.
- C. Create a new response template.
- D. Validate response data paths from Decide stage.

정답：A

설명:
Before automating the Act stage of the OODA loop, it is essential to validate whether the asset, identity, or service has an exemption. This ensures that automated actions do not negatively impact business-critical systems or users who are intentionally excluded from automated remediation.

질문 # 47
.....