SPLK-5002높은통과율시험대비덤프공부 - SPLK-5002 인기덤프공부

EMC DEP-3CR1 PowerProtect Cyber Recovery Exam 3

질문 # 26
An enterprise customer needs a Cyber Recovery solution to be implemented. As an outcome from a previous workshop, the following backup environment needs to be protected to the CR Vault.
Location 1: 4 PowerProtect DDs
Location 2: 4 PowerProtect DDs
Location 3: 2 PowerProtect DDs
Location 4: 2 PowerProtect DDs
The customer wants to implement a CR Vault in a 5th location.
How many Cyber Recovery systems must be installed at a minimum level?

- A. 0
- B. 1
- C. 2
- D. 3

정답□B

질문 # 27
What vault status is displayed if none of the PowerProtect DD systems in the CR Vault are able to communicate with the Cyber Recovery software?

- A. Unknown
- B. Unlocked
- C. Locked
- D. Degraded

정답□B

질문 # 28
.....

DEP-3CR1높은 통과율 시험대비 덤프공부:
https://www.koreadumps.com/DEP-3CR1_exam-braindumps.html

- DEP-3CR1시험문제집 □ DEP-3CR1시험대비 덤프데모 다운 □ DEP-3CR1시험덤프 □ 무료 다운로드를 위해 지금 www.itdumpskr.com 에서 □ DEP-3CR1 □검색DEP-3CR1높은 통과율 인기 덤프문제
- DEP-3CR1최신버전 덤프공부 □ DEP-3CR1높은 통과율 인기 덤프문제 □ DEP-3CR1시험대비 덤프데모문제 □ 지금□ www.itdumpskr.com □에서▶ DEP-3CR1 ◀를 검색하고 무료로 다운로드하세요DEP-3CR1높은 통과율 인기 덤프문제
- DEP-3CR1덤프문제 □ DEP-3CR1시험패스 가능 덤프 □ DEP-3CR1시험대비 공부하기 □ 검색만 하면□ www.itdumpskr.com □에서 ★ DEP-3CR1 ★무료 다운로드DEP-3CR1최신기출자료
- 최신버전 DEP-3CR1시험대비 덤프 최신자료 덤프문제 □ 검색만 하면□ www.itdumpskr.com □에서▷ DEP-3CR1 ◁무료 다운로드DEP-3CR1시험패스 가능한 인증공부자료
- DEP-3CR1최신버전 덤프공부 □ DEP-3CR1합격보장 가능 덤프공부 □ DEP-3CR1시험대비 덤프데모 다운 □ 지금□ www.itdumpskr.com □을(를) 열고 무료 다운로드를 위해▶ DEP-3CR1 ◀를 검색하십시오DEP-3CR1시험패스 가능 덤프
- DEP-3CR1최신버전 덤프공부 □ DEP-3CR1시험대비 공부하기 □ DEP-3CR1덤프문제 □I

DEP-3CR1시험대비덤프최신자료 & DEP-3CR1높은통과율시험대비덤프공부

참고: KoreaDumps에서 Google Drive로 공유하는 무료, 최신 SPLK-5002 시험 문제집이 있습니다: https://drive.google.com/open?id=1hiK1EYwFuvuc95foJnVx8B6p8ppSwqze

Splunk SPLK-5002인증시험패스에는 많은 방법이 있습니다. 먼저 많은 시간을 투자하고 신경을 써서 전문적으로 과련 지식을 터득한다거나; 아니면 적은 시간투자와 적은 돈을 들여 KoreaDumps의 인증시험덤프를 구매하는 방법 등이 있습니다.

KoreaDumps는 몇년간 최고급 덤프품질로 IT인증덤프제공사이트중에서 손꼽히는 자리에 오게 되었습니다. Splunk SPLK-5002 덤프는 많은 덤프들중에서 구매하는 분이 많은 인기덤프입니다. Splunk SPLK-5002시험준비중이신 분이시라면Splunk SPLK-5002한번 믿고 시험에 도전해보세요. 좋은 성적으로 시험패스하여 자격증 취득할것입니다.

>> SPLK-5002높은 통과율 시험대비 덤프공부 <<

Splunk SPLK-5002인기덤프공부 & SPLK-5002인증문제

Splunk인증SPLK-5002시험은 현재 치열한 IT경쟁 속에서 열기는 더욱더 뜨겁습니다. 응시자들도 더욱더 많습니다. 하지만 난이도난 전혀 낮아지지 않고 이지도 어려운 시험입니다. 어쨌든 개인적인 지식 장악도 나 정보기술 등을 테스트하는 시험입니다. 보통은Splunk인증SPLK-5002시험을 넘기 위해서는 많은 시간과 신경이 필요합니다.

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	• 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	• 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 4	• 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 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 (Q78-Q83):

질문 # 78
An engineer is examining a correlation search as a part of a detection review, and sees that it is configured in the following fashion:
Which of the following is true about this configuration?

- A. The search will run as prescribed without issue every 30 minutes.
- B. The risk modifiers should be adjusted for an hour of data.
- C. There could be missing data as the search schedule is not ingesting data properly.
- D. There could be missing findings as the search frequency and time range are improperly configured.

정답：D

설명:
The correlation search is scheduled to run every 2 minutes (*/2 * * * *) but is querying a 60-minute window (earliest = -60m@m). This large mismatch between the time range and the execution frequency is considered an improper configuration for ES correlation searches.
Such a configuration can lead to inconsistent detection behavior, including missed or duplicate findings, because the search continually reprocesses a very large window using a very short execution interval.

질문 # 79
Based on a recent red team exercise, an organization is highly concerned about pass the hash attacks especially including tools like Empire. Which Eventcode associated to PowerShell Script Block Logging would be used to detect this activity?

- A. EventCode=4168
- B. EventCode=4126
- C. EventCode=4624
- D. EventCode=4104

정답：D

설명：
EventCode=4104 is associated with PowerShell Script Block Logging, which records the full content of executed PowerShell scripts. This is critical for detecting malicious frameworks like Empire that rely on PowerShell for pass-the-hash and other attack techniques.

질문 # 80
What is the primary purpose of correlation searches in Splunk?

- A. To store pre-aggregated search results
- B. To extract and index raw data
- C. To create dashboards for real-time monitoring
- D. To identify patterns and relationships between multiple data sources

정답：D

설명：
Correlation searches in Splunk Enterprise Security (ES) are a critical component of Security Operations Center (SOC) workflows, designed to detect threats by analyzing security data from multiple sources.
Primary Purpose of Correlation Searches:
Identify threats and anomalies: They detect patterns and suspicious activity by correlating logs, alerts, and events from different sources.
Automate security monitoring: By continuously running searches on ingested data, correlationsearches help reduce manual efforts for SOC analysts.
Generate notable events: When a correlation search identifies a security risk, it creates a notable event in Splunk ES for investigation.
Trigger security automation: In combination with Splunk SOAR, correlation searches can initiate automated response actions, such as isolating endpoints or blocking malicious IPs.
Since correlation searches analyze relationships and patterns across multiple data sources to detect security threats, the correct answer is B. To identify patterns and relationships between multiple data sources.
References:
Splunk ES Correlation Searches Overview
Best Practices for Correlation Searches
Splunk ES Use Cases and Notable Events

질문 # 81
Below is an example of a sysmon process create log. Which EventCode would be associated to this log entry?

- A. EventCode=1
- B. EventCode=4
- C. EventCode=3
- D. EventCode=2

정답：A

설명：
In Sysmon, EventCode=1 corresponds to a Process Create event. The log provided shows details of a new process creation (powershell.exe) including ProcessGuid, ProcessId, CommandLine, ParentProcessId, and ParentImage, which are all fields specific to a Process Create event.

질문 # 82
Which syntax is correct to create two new rows on an existing threat intelligence collection?

- A. curl -k -u admin:pass https://localhost:8089/services/data/threat_intel/item/email_intel -d item='[{"src_user": "user_new", "subject":"click this"}]' -G -X
- B. curl -k -u admin:pass https://localhost:8089/services/data/threat_intel/item/email_intel -d item='[{"src_user": "user_new", "subject":"click this"}]'

- C. curl -k -u admin:pass https://localhost:8089/services/data/threat_intel/item/email_intel -d item='[{"src_user": "user_new", "subject":"click this"},{"src_user": "user2_new", "subject":"click this"}]' -G -X
- D. curl -k -u admin:pass https://localhost:8089/services/data/threat_intel/item/email_intel -d item="[{"src_user": "user_new", "subject":"click this"},{"src_user": "user2_new", "subject":"click this"}]'

정답：D

설명：
This syntax is valid because it passes multiple JSON objects inside a single array for the item parameter, ensuring both new rows are added to the collection in one request.

질문 # 83
.....