Splunk SPLK-5002試験の認証資格を逃さないで

P.S. MogiExamがGoogle Driveで共有している無料かつ新しいSPLK-5002ダンプ：https://drive.google.com/open?id=1mPrqQJUbjDCjbkzFtnFQkhlksrvBr6Y2

SplunkのSPLK-5002クイズトレントは無料の試用版を提供します。したがって、SPLK-5002テスト準備についてより深く理解し、この種の学習教材が購入に適しているかどうかを推定するのに役立ちます。 MogiExam試用版を使用すると、テストプラットフォームで利用可能な3つの異なるバージョンの選択からアフターサービスまで、さまざまな側面からのSPLK-5002試験トレントについてより深く理解できます。 SPLK-5002試験問題を試してみたら、Splunk Certified Cybersecurity Defense Engineer購入するのが大好きです。

Splunk SPLK-5002 認定試験の出題範囲：

トピック	出題範囲
トピック 1	• セキュリティプログラムの監査と報告：このセクションでは、監査担当者とセキュリティアーキテクトがプログラムの有効性を検証し、伝達する能力をテストします。セキュリティ指標の設計、コンプライアンスレポートの作成、そして関係者向けにプログラムのパフォーマンスと脆弱性を視覚化するダッシュボードの構築などが含まれます。
トピック 2	• 効果的なセキュリティプロセスとプログラムの構築：このセクションは、セキュリティプログラムマネージャーとコンプライアンス担当者を対象とし、セキュリティワークフローの運用化に焦点を当てています。脅威インテリジェンスの調査と統合、リスクと検知の優先順位付け手法の適用、そして堅牢なセキュリティ対策を維持するためのドキュメントや標準運用手順（SOP）の作成が含まれます。
トピック 3	• データエンジニアリング：このセクションでは、セキュリティアナリストとサイバーセキュリティエンジニアのスキルを測定し、基本的なデータ管理タスクを網羅します。データのレビューと分析の実行、効率的なデータインデックスの作成と維持、そしてSplunkメソッドを用いたデータ正規化を適用し、セキュリティ運用において構造化され利用可能なデータセットを確保することが含まれます。
トピック 4	• 検知エンジニアリング：このセクションでは、セキュリティ検知の開発と改良における脅威ハンターとSOCエンジニアの専門知識を評価します。トピックには、相関検索の作成と調整、検知へのコンテキストデータの統合、リスクベースの修飾子の適用、実用的な重要イベントの生成、進化する脅威に適応するための検知ルールのライフサイクル管理などが含まれます。
トピック 5	• 自動化と効率性：このセクションでは、セキュリティ運用の効率化における自動化エンジニアとSOARスペシャリストの能力を評価します。SOP（標準運用手順）の自動化の開発、ケース管理ワークフローの最適化、REST APIの活用、レスポンス自動化のためのSOARプレイブックの設計、Splunk Enterprise SecurityとSOARツールの統合の評価などを網羅します。

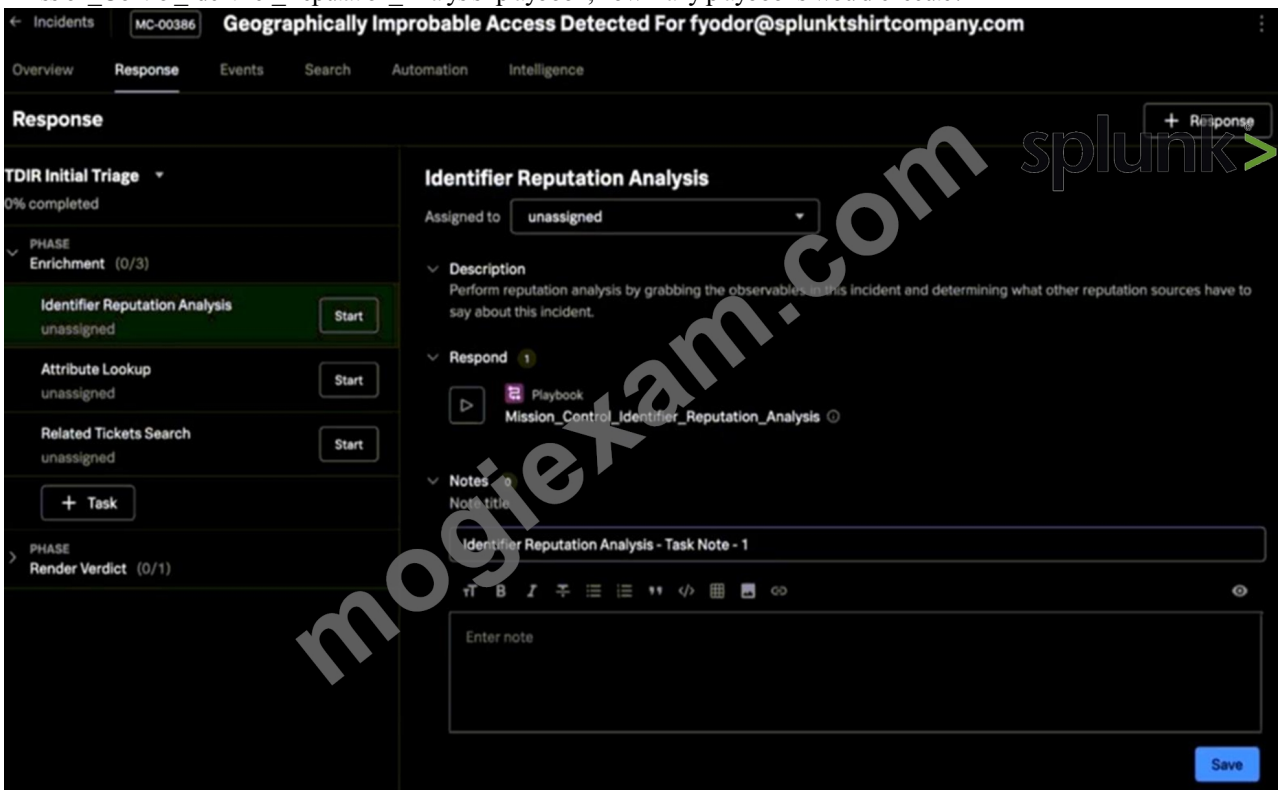
>> SPLK-5002復習解答例 <<

有効的なSPLK-5002復習解答例 & 合格スムーズSPLK-5002最新試験 |権威のあるSPLK-5002日本語版サンプル

さまざまな年齢層の研究条件に基づくさまざまな種類のアンケートによると、当社のSPLK-5002テスト準備はこれらの研究グループ向けに完全に設計されており、SPLK-5002試験の準備時の能力と効率を向上させ、目標とするSPLK-5002証明書が正常に作成されました。 SPLK-5002の質問トレントには多くの利点がありますので、ご紹介します。SplunkのSPLK-5002試験に合格することができます。

Splunk Certified Cybersecurity Defense Engineer 認定 SPLK-5002 試験問題 (Q79-Q84):

質問 # 79
While working in Mission Control, an analyst is looking to add enrichment and contextualize the finding that is being worked. If they were to click the execute icon next to the
"Mission_Control_Identifier_Reputation_Analysis" playbook, how many playbooks would execute?



- A. Unknown
- B. None
- C. 1 playbook
- D. At least 1 playbook

正解：C

解説：
Clicking the execute icon next to "Mission_Control_Identifier_Reputation_Analysis" triggers exactly 1 playbook. In Mission Control, each listed playbook is a discrete automation, so selecting it runs only that specific playbook for enrichment and contextualization.

質問 # 80
What is the main purpose of Splunk's Common Information Model (CIM)?

- A. To compress data during indexing

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

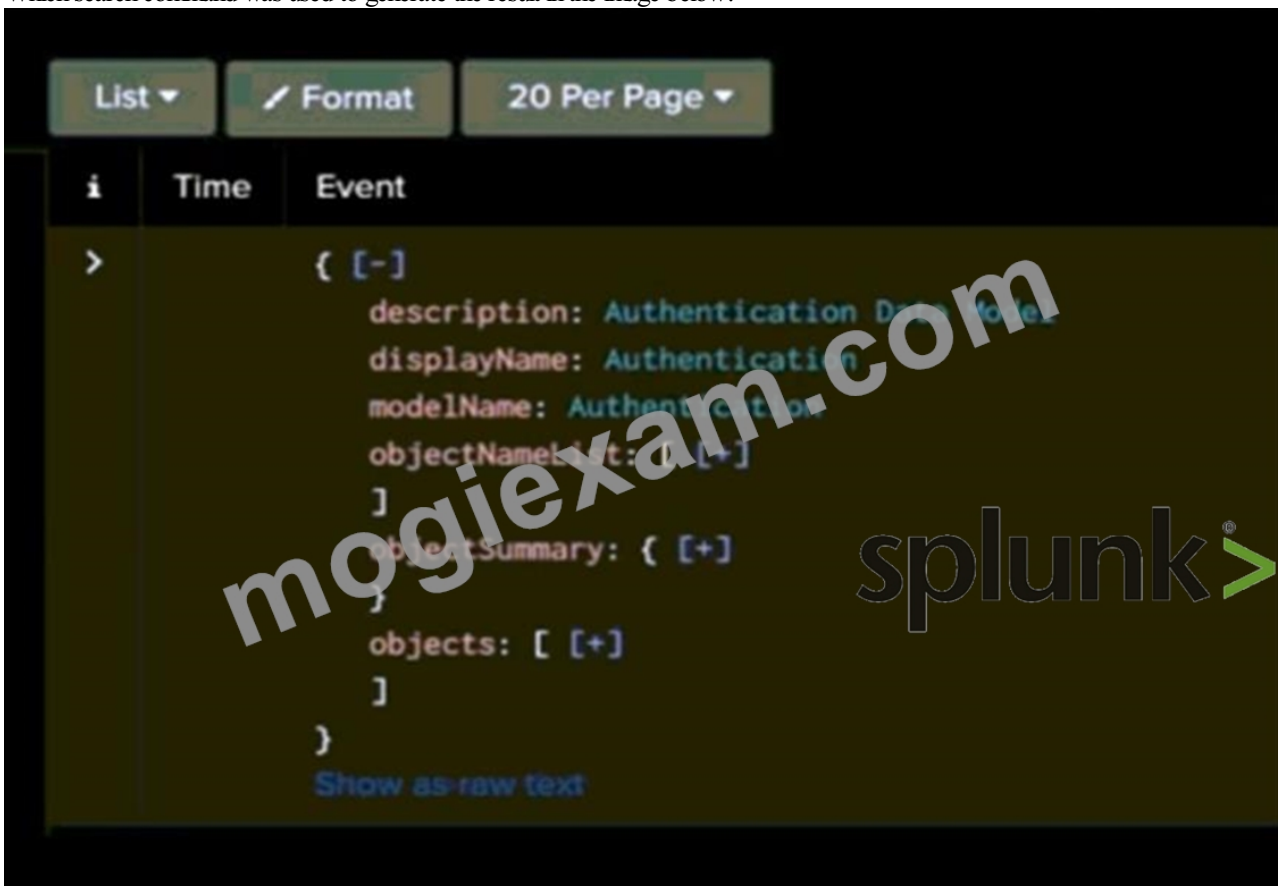
正解：C

質問 # 81
What does Splunk's term "bucket" refer to in data indexing?

- A. A directory containing indexed data
- B. A collection of events with a specific retention policy
- C. A storage unit for archived data
- D. A database table for search results

正解：A

質問 # 82
Which search command was used to generate the result in the image below?



- A. datamodel
- B. datatype
- C. cim
- D. metadata

正解：A

解説：
The result in the image shows details of the Authentication Data Model (description, displayName, modelName, objectNameList, etc.). This output is generated by the datamodel search command, which is used to list and inspect available data models in Splunk.

質問 # 83
What Splunk process ensures that duplicate data is not indexed?

- A. Metadata tagging
- B. Data deduplication
- C. Indexer clustering
- D. Event parsing

正解：D

解説：
Splunk prevents duplicate data from being indexed through event parsing, which occurs during the data ingestion process.
How Event Parsing Prevents Duplicate Data:
Splunk's indexer parses incoming data and assigns unique timestamps, metadata, and event IDs to prevent reindexing duplicate logs.
CRC Checks (Cyclic Redundancy Checks) are applied to avoid duplicate event ingestion.
Index-time filtering and transformation rules help detect and drop repeated data before indexing.

質問 # 84
.....

SPLK-5002準備試験では、国内および海外の専門家と学者を取り入れた専門家のチームを集めて、関連する試験銀行の調査と設計を行い、受験者がSPLK-5002試験に合格するのを支援します。ほとんどの専門家は長年プロの分野で勉強しており、SPLK-5002練習問題で多くの経験を蓄積しています。当社は才能の選択にかなり慎重であり、夢のSPLK-5002認定の取得を支援するために、専門知識とスキルを備えた従業員を常に雇用しています。