Splunk.SPLK-3001.v2026-08-05.q122

試験コード：	SPLK-3001
試験名称：	Splunk Enterprise Security Certified Admin Exam
認証ベンダー：	Splunk
無料問題の数：	122
バージョン：	v2026-08-05
ページの閲覧量：	106
問題集の閲覧量：	1271

https://www.jpnshiken.com/shiken/Splunk.SPLK-3001.v2026-08-05.q122.html

質問: **1**
適応反応は何によって引き起こされるのでしょうか？
A. インシデントレビューダッシュボード上の相関検索とユーザーによる。
B. 相関検索とカスタム技術アドオンによる。
C. 脅威分析ダッシュボード上の相関検索とユーザーによる。
D. リスク分析ダッシュボード上のカスタム技術アドオンとユーザーによる。
正解: **(**正解を表示します**)**
説明
適応的対応とは、重大な出来事やその他のセキュリティインシデントに対応して実行できる行動のことである。
適応型対応は、相関検索やインシデントレビューダッシュボード上のユーザーによってトリガーされる可能性があります。
相関検索は、定期的に実行されるスケジュール検索であり、データ内の関心のあるパターンを検出し、検索条件が満たされたときに注目すべきイベントやその他のアクションを生成します。
ユーザーは、注目すべきイベントが作成されたときに適応型応答を自動的にトリガーするように相関検索を設定できます。また、注目すべきイベントとその詳細を表示するインシデントレビューダッシュボードから、適応型応答を手動で実行することもできます。ユーザーは、1つまたは複数の注目すべきイベントを選択し、メニューから適応型応答アクションを選択できます。
適応型レスポンスは、ユーザーが情報を収集したり、環境を変更したり、セキュリティインシデントを調査して対応するためのその他のアクションを実行したりするのに役立ちます。参照 = 適応型レスポンスフレームワークの概要 インシデントレビューダッシュボードから適応型レスポンスアクションを実行する

質問: **2**
誰が調査を削除できるのか？
A. ess_admin ユーザーのみ。
B. 調査の所有者のみ。
C. 調査の所有者とess-admin。
D. 調査の責任者および協力者。

正解: (正解を表示します)
https://docs.splunk.com/Documentation/ES/6.1.0/Admin/Manageinvestigations

質問: **3**
CIMデータモデルでは、デフォルトでどのインデックスが検索されますか？
A. 注目すべきデフォルト
B. 概要と注目すべき点
C. _内部および概要
D. すべてのインデックス
正解: (正解を表示します)
説明/参考資料 :https://answers.splunk.com/answers/600354/indexes-searched-by-cim-data-models.html

質問: **4**
以下の手順のうち、ESで脅威アクティビティダッシュボードをデフォルトのランディングページにするには、どれを実行すればよいですか？
A. 脅威アクティビティの表示設定を編集し、「デフォルトビュー」オプションにチェックマークを付けます。
B. [ナビゲーションの編集] ページから、[脅威アクティビティ] の [これを既定のビューとして設定] チェックマークをクリックします。
C. [ナビゲーションの編集] ページから、[脅威アクティビティ] ビューをページの一番上にドラッグアンドドロップします。
D. ユーザーの環境設定メニューから、既定のアプリケーションとしてエンタープライズセキュリティを選択します。
正解: (正解を表示します)
ページをタップ位置にドラッグしても、メニューバーに追加されるだけで、デフォルトのランディングページには設定されません。「これをデフォルトビューとして設定する」のチェックマークをクリックする必要があります。

質問: **5**
分散構成管理を使用してSplunk_TA_ForIndexersパッケージを作成する場合、どの3つのファイルを含めることができますか？
A. inputs.conf、props.conf、transforms.conf
B. web.conf、props.conf、transforms.conf
C. indexes.conf、props.conf、transforms.conf
D. eventtypes.conf、indexes.conf、tags.conf
正解: (正解を表示します)

質問: **6**

Splunk ESのどの機能が、アナリストがユーザー、システム、イベント間の関係を調査するのに役立ちますか？
A. 資産調査担当者は、コンテキストセキュリティ調査のためにエンティティ間の関係を効果的に視覚化します。
B. 相関検索スケジューラは、保存された検索をクラスタ化された検索ヘッドメンバーに分散します。
C. データオンボーディングウィザードは、外部データセットをCIM互換フォーマットに自動的に即座に正規化します。
D. 脅威インテリジェンスマネージャーは、外部リポジトリからのマルウェアシグネチャの同期を継続的に高速化します。
正解: **(**正解を表示します**)**
Asset Investigatorは、ID、システム、イベント間の文脈的な関係性を提示することで、アナリストが攻撃の範囲と影響を受ける組織資産を迅速に把握できるようにします。

質問: **7**
Enterprise Security の以下のルックアップタイプのうち、既知の悪意のある IP アドレスに関する情報が含まれているのはどれですか？
A. 資産。
B. ドメイン。
C. セキュリティドメイン。
D. 脅威情報。
正解: **(**正解を表示します**)**

質問: **8**
個人情報に関する詳細情報はどこに保存されていますか？
A. 身元調査官索引。
B. アクセス異常コレクション。
C. ユーザーアクティビティ指標。
D. 本人確認用CSVファイル。
正解: **(**正解を表示します**)**
https://docs.splunk.com/Documentation/ES/6.6.2/Admin/Formatassetoridentitylist

質問: **9**
Splunk Enterprise Securityにアドオンを自動的にインポートできるようにするには、次のうちどれを使用すればよいですか？
A. CIM_の接頭辞
B. .spl の接尾辞
C. TECH_の接頭辞
D. Splunk_TA_ の接頭辞
正解: **D (**コメントを発表する**)**

説明/参考資料：
https://dev.splunk.com/enterprise/docs/developapps/enterprisesecurity/planintegrationes/

質問: **10**
「デフォルトアカウント活動検出」相関検索は、既知のデフォルトアカウントを特定するために、どのルックアップテーブルを使用しますか？
A. 管理ID
B. ローカルユーザーインテル
C. アイデンティティ
D. 特権アカウント
正解: **(**正解を表示します**)**
説明
Splunk Enterprise Securityのドキュメントによると、Default Account Activity Detected相関検索は、Local User Intelルックアップテーブルを使用して既知のデフォルトアカウントを検出します。Local User Intelルックアップテーブルには、admin、root、guestなどのさまざまなシステムやアプリケーションのデフォルトのユーザー名とパスワードのリストが含まれています。相関検索は、Authenticationデータモデルの認証イベントをルックアップテーブルのユーザー名と比較し、一致するものがあれば注目すべきイベントを生成します。注目すべきイベントは、デフォルトアカウントがシステムまたはアプリケーションへのアクセスに使用されたことを示しており、ブルートフォース攻撃または設定ミスの兆候である可能性があります。したがって、正解はB. Local User Intelです。参照 = Default Account Activity Detected Local User Intel

質問: **11**
リスク分析ダッシュボードにはどのようなツールが用意されていますか？
A. 高リスクの脅威。
B. リスクスコア別に表示された注目すべきイベント領域。
C. 最もリスクの高い資産と身元情報の表示。
D. 環境内で最も高い確率で相関関係が見られる主要指標。
正解: **(**正解を表示します**)**
参照：
https://docs.splunk.com/Documentation/ES/6.1.0/User/RiskAnalysis

質問: **12**
アドオンビルダーはどこで入手できますか？
A. GitHub
B. SplunkBase
C. www.splunk.com
D. ESインストールパッケージ
正解: **(**正解を表示します**)**

説明/参考資料：
https://docs.splunk.com/Documentation/AddonBuilder/3.0.1/UserGuide/Installation

質問: **13**
Splunk ESが外部セキュリティツールでアクションを自動的にトリガーできるようにするフレームワークはどれですか？
A. 適応型対応フレームワークは、自動化されたアクションを外部セキュリティプラットフォームと統合します。
B. 脅威インテリジェンスフレームワークは、コミュニティインテリジェンスリポジトリから悪意のある指標を自動的に集約します。
C. 資産調査フレームワークは、ユーザーとシステムの関係調査のコンテキストを明確に視覚化します。
D. KVストアフレームワークは、Splunk環境内のアプリケーションレベルの構造化データを効率的に管理します。
正解: **A (**コメントを発表する**)**
適応型対応フレームワークは、外部ツールと統合することで、インシデント対応業務における封じ込め、チケット作成、通知、およびオーケストレーション活動を自動化します。

質問: **14**
セキュリティ態勢ダッシュボードには何が表示されますか？
A. 進行中の捜査とその状況。
B. 注目すべき出来事の概要。
C. SOCが現在追跡している脅威。
D. セキュリティツールの状態を表示します。
正解: **(**正解を表示します**)**
セキュリティ態勢ダッシュボードは、展開環境のすべてのドメインにおける注目すべきイベントに関する高度な情報を提供するように設計されており、セキュリティオペレーションセンター（SOC）での表示に適しています。このダッシュボードには、過去24時間のすべてのイベントと、過去24時間の傾向が表示され、リアルタイムのイベント情報と更新情報も提供されます。
参考資料：https://docs.splunk.com/Documentation/ES/6.1.0/User/SecurityPosturedashboard

質問: **15**
以下のうち、ESで使用されているデータモデルはどれですか？（該当するものをすべて選択してください。）
A. Web
B. 異常
C. 認証
D. ネットワークトラフィック
正解: **(**正解を表示します**)**

説明/参考資料：
https://dev.splunk.com/enterprise/docs/developapps/enterprisesecurity/datamodelsusedbyes/

質問: **16**
ESのインストール後、管理者はLeersにss_usoロールを設定し、重要なイベントを閉じる権限を与えました。管理者は、これらのユーザーが解決済みの重要なイベントのステータスをクローズに変更できないようにするにはどうすればよいでしょうか？
A. ステータス設定ウィンドウから 解決済み」ステータスを選択します。クローズ済みステータスのステータス遷移からess_userを削除します。
B. Splunk アクセス制御から ess_user ロールを選択し、edit_notabie_events 機能を削除します。
C. エンタープライズセキュリティで、ess_userロールに独自のNotable Events権限を付与します。
D. ステータス設定ウィンドウから クローズ」ステータスを選択します。 解決済み」ステータスのステータス遷移からess_userを削除します。
正解: (正解を表示します)

質問: **17**
ネットワーク全体の活動において、どのようなネットワークサービスが使用されているかを把握するために、エンタープライズセキュリティの以下のダッシュボードのうち、どれが最も関連性の高いデータを含んでいますか？
A. 侵入検知センター
B. プロトコル分析
C. ユーザーインテリジェンス
D. 脅威インテリジェンス
正解: (正解を表示します)
説明／参考資料：
https://docs.splunk.com/Documentation/ES/6.1.0/User/NetworkProtectionDomaindashboards

質問: **18**
アドオンビルダーは、新しいアドオンで以下のどの機能を構成できますか？
A. 有効期限切れデータ。

B. データの正規化。
C. データを要約する。
D. データを翻訳します。
正解: **(**正解を表示します**)**
https://docs.splunk.com/Documentation/AddonBuilder/3.0.1/UserGuide/Overview

質問: **19**
適応応答アクションの履歴はどのインデックスに保存されますか？
A. cim_modactions
B. モジュール履歴
C. cim_adaptiveactions
D. モジュール式アクション履歴
正解: **(**正解を表示します**)**
説明/参考資料 :https://docs.splunk.com/Documentation/ES/6.1.0/Install/Indexes

質問: **20**
ESアプリとアドオン $SPLUNK_HOME/etc/apps）は、ステージングインスタンスからクラスタデプロイヤインスタンスのどの場所にコピーする必要がありますか？
A. $SPLUNK_HOME/etc/master-apps/
B. $SPLUNK_HOME/etc/system/local/
C. $SPLUNK_HOME/etc/shcluster/apps
D. $SPLUNK_HOME/var/run/searchpees/
正解: **(**正解を表示します**)**
ステージングインスタンスのアップグレードされたコンテンツはデプロイヤに移行され、検索ヘッドクラスタメンバーにデプロイされます。ステージングインスタンス
で、$SPLUNK_HOME/etc/apps をコピーします。
デプロイヤー上の $SPLUNK_HOME/etc/shcluster/apps で、ステージング環境でのアップグレード中に削除された、$SPLUNK_HOME/etc/shcluster/apps 内の非推奨のアプリまたはアドオンを削除します。ステージング環境で生成された ES アップグレード レポートを確認するか、移動されたアプリを調べて確認してください。
ステージング環境の $SPLUNK_HOME/etc/disabled-apps

質問: **21**
非標準のフィールド名をCIMフィールド名にマッピングするには、何を使用すればよいですか？
A. フィールドエイリアス。
B. 検索時間抽出。
C. 日。
D. イベントタイプ。
正解: **(**正解を表示します**)**
説明

質問: **22**
分散型configLradon管理を使用してspiunk_TA_Forindexersパッケージを作成する場合、vrfilchには3つのファイルを含めることができますか？
A. web.conf、props.conf、transforms.conf
B. eventtypes.conf、indexes.conf、tags.conf
C. inputs.conf、props.conf、transforms.conf
D. indexes.conf、props.conf、transforms.conf
正解: **(**正解を表示します**)**

質問: **23**
あるサイトには、CIM準拠アプリケーションと非CIM準拠アプリケーションが混在する既存の検索ヘッドが1つあります。すべてのアプリケーションはミッションクリティカルです。顧客はコストを慎重に管理したいと考えていますが、ESのパフォーマンスも良好にしたいと考えています。ESをインストールするためのベストプラクティスは何でしょうか？
A. 既存の検索ヘッドにESをインストールします。
B. 新しい検索ヘッドを追加し、そこにESをインストールします。
C. 検索ヘッドのCPU数とメモリ容量を増やしてからESをインストールします。
D. 検索ヘッドからCIMに準拠していないアプリを削除してから、ESをインストールします。
正解: **(**正解を表示します**)**
説明／参考資料 :https://www.splunk.com/pdfs/technical-briefs/splunk-validated-architectures.pdf

質問: **24**
Enterprise Securityのどの機能が、Webサーバーから脅威インテリジェンスデータをダウンロードしますか？
A. 脅威サービスマネージャー
B. 脅威ダウンロードマネージャー
C. 脅威インテリジェンスパーサー
D. 脅威インテリジェンスの執行
正解: **(**正解を表示します**)**
脅威インテリジェンスフレームワークは、インテリジェンスファイルとデータのダウンロードに通常必要となる設定の大部分を処理するモジュール式の入力（脅威インテリジェンスのダウンロード）を提供します。
このモジュール入力にアクセスするには、Inputs.conf ファイルに次のスタンザを作成するだけで済みます。
脅威リスト」

質問: **25**
注目すべき出来事の緊急性を生み出すために、どのような2つの分野が組み合わさるのでしょうか？

A. 重要度と深刻度。
B. 優先度と重要度。
C. 優先順位と時間。
D. 優先度と重要度。
正解: **(**正解を表示します**)**

質問: **26**
ESのインストール準備における最初のステップは何ですか？
A. 必要なハードウェアを決定します。
B. 使用するデータソースを特定する。
C. ESをインストールします。
D. 設置の規模と範囲を決定する。
正解: **D (**コメントを発表する**)**

質問: **27**
現在有効になっているES相関検索の一覧に移動するにはどうすればよいですか？
A. 設定→相関検索→ステータスを「有効」に選択
B. 設定 -> 検索、レポート、アラート -> 「相関関係」の名前でフィルタリング
C. 設定→コンテンツ管理→タイプ「相関」、ステータス「有効」を選択
D. 設定 -> 検索、レポート、アラート -> 「SplunkEnterpriseSecuritySuite」アプリを選択し、「ルール」でフィルタリングします
正解: **A (**コメントを発表する**)**
参照：
https://docs.splunk.com/Documentation/ES/6.1.0/Admin/Listcorrelationsearches

質問: **28**
ESコンテンツをエクスポートすると、拡張子が.splのアプリが自動的に作成されます。ESコンテンツの更新をエクスポートおよびインポートする際のベストプラクティスは何ですか？
A. コンテンツをエクスポートするたびに、新しいアプリ名を使用してください。
B. エクスポートに名前を付ける際に、.spl 拡張子を使用しないでください。
C. 新しいアプリ名を使用するか、既存のコンテンツと新しいコンテンツの両方を常に含めるようにしてください。
D. エクスポートの際には、既存コンテンツと新規コンテンツを必ず含めてください。
正解: **C (**コメントを発表する**)**
毎回新しいアプリ名を使用するか（管理が難しくなる可能性がある）、エクスポートするたびに必ずすべてのコンテンツ（古いコンテンツと新しいコンテンツの両方）を含めるようにしてください。

質問: **29**

インシデントレビューダッシュボードの 注目すべきイベント」テーブルに新しい列を追加する手順を教えてください。
A. 設定 -> インシデント管理 -> インシデントレビュー設定 -> イベント管理
B. 設定 -> インシデント管理 -> 注目すべきイベントステータス
C. 設定 -> コンテンツ管理 -> タイプ：相関検索
D. 設定 -> インシデント管理 -> インシデントレビュー設定 -> テーブル属性
正解: **(**正解を表示します**)**

質問: **30**
調査を行う際、新たに発見されたIOC（侵害指標を保管する最良の方法は何ですか？
A. 「アーティファクトを追加」ボタンをクリックします。
B. 「IOCを追加」ボタンをクリックします。
C. メモ帳に貼り付けてください。
D. 調査のテキストメモに追加してください。
正解: **B (**コメントを発表する**)**

質問: **31**
注目すべき事象の緊急度はどのように算出されるのですか？
A. 資産の優先順位と脅威の重み。
B. 相関検索によって検出されたアラートの深刻度。
C. 相関検索によって検出された資産または身元リスクと深刻度。
D. 相関検索によって設定された深刻度と、関連する資産またはIDに割り当てられた優先度。
正解: **D (**コメントを発表する**)**
参照：
https://docs.splunk.com/Documentation/ES/6.1.0/User/Howurgencyisassigned

質問: **32**
データモデルノードにイベントタイプを含めるには、適切なフィールドを抽出した後、次にどのような手順を踏む必要がありますか？
A. 設定を保存します。
B. 正しいタグを適用してください。
C. 正しい検索を実行してください。

D. CIMダッシュボードにアクセスしてください。
正解: **(**正解を表示します**)**
参照：
https://docs.splunk.com/Documentation/CIM/4.15.0/User/UsetheCIMtonormalizeOSSECdata

質問: **33**
分散構成管理の自動展開機能を使用して indexes.conf を配布する場合、次のうちどれがリスクとなりますか？
A. インデクサーがクラッシュする可能性があります。
B. インデクサーが処理中である可能性があります。
C. インデクサーにアクセスできない可能性があります。
D. インデクサーには異なる設定があります。
正解: **(**正解を表示します**)**
https://community.splunk.com/t5/Splunk-Enterprise-Security/Splunk-Enterprise-Security-requires- a-deployment-client-but/mp/279749

質問: **34**
ESをインストールする前に、以下のどの操作が必要になる可能性がありますか？
A. 分散検索接続をリダイレクトします。
B. KVストアをパージします。
C. 追加のインデクサーを追加します。
D. 追加の転送業者を追加します。
正解: **(**正解を表示します**)**
説明
Splunk Enterprise Security のドキュメントによると、ES をインストールする前に必要となる場合があるアクションの 1 つは、分散検索接続のリダイレクトです。このアクションは、検索ヘッド クラスタや検索ヘッド プールなど、既に分散検索環境に接続されている検索ヘッドに ES をインストールする場合に必要です。既存の検索ヘッドから、ES を実行する新しい検索ヘッドに分散検索接続をリダイレクトする必要があります。これは、ES が他のアプリやユーザーと共有されない専用の検索ヘッドを必要とするためです。分散構成管理ツールを使用して、分散検索接続をリダイレクトし、インデクサー用の Splunk Enterprise Security アプリを作成できます。詳細については、 分散検索接続のリダイレクト」を参照してください。
その他の操作は ES のインストール前に必須ではありませんが、ES のパフォーマンスとスケーラビリティを最適化するのに役立つ場合があります。KV ストアをパージすると、ディスク領域を解放し、古いデータを削除できますが、ES のインストール前に必須ではありません。詳細については、 KV ストアのパージ」を参照してください。追加のインデクサを追加すると、ES のインデックス作成と検索機能を向上させることができますが、ES のインストール前に必須ではありません。詳細については、 展開計画」を参照してください。追加のフォワーダーを追加すると、ES のデータ取り込みと転送機能を向上させることができますが、ES のインストール前に必

須ではありません。詳細については、「Splunk Enterprise Security へのデータの転送」を参照してください。参照 = 分散検索接続のリダイレクト KV ストアのページ 展開計画 Splunk Enterprise Security へのデータの転送

質問: **35**
CIMデータモデルでは、デフォルトでどのインデックスが検索されますか？
A. 注目すべきデフォルト
B. 概要と注目すべき点
C. _内部および概要
D. すべてのインデックス
正解: **D (コメントを発表する)**
参照：
https://answers.splunk.com/answers/600354/indexes-searched-by-cim-data-models.html

質問: **36**
適応応答アクションの履歴はどのインデックスに保存されますか？
A. cim_modactions
B. モジュール式アクション履歴
C. モジュール履歴
D. cim_adaptiveactions
正解: **(正解を表示します)**

質問: **37**
管理者は、ESにインデックス付けされたデータが改ざんによって侵害されることがないようにしたいと考えている。
この要件を満たす機能は何でしょうか？
A. 指標の一貫性。
B. インデックスへのアクセス権限。
C. データ整合性管理。
D. 索引作成者への謝辞。
正解: **(正解を表示します)**

質問: **38**
以下のうち、プロパティ正規化データモデルをテストする方法はどれですか？
A. データモデル検索を実行し、結果をES正規化ガイドのデータモデルのリストと比較します。
B. データモデル検索を実行し、結果をデータモデルの CIM ドキュメントと比較します。
C. 監査 -> 正規化監査を使用して、エラー パネルを確認します。
D. loadjob search を実行し、タグ値を調べて、エンコーディングに基づいて既知のタグと比較します。
正解: **(正解を表示します)**

質問: **39**
誰が調査を削除できるのか？
A. ess_admin ユーザーのみ。
B. 調査の所有者のみ。
C. 調査の所有者とess-admin。
D. 調査の責任者および協力者。
正解: **(**正解を表示します**)**
参照：
https://docs.splunk.com/Documentation/ES/6.1.0/Admin/Manageinvestigations

質問: **40**
資産検索画面のどの列が、イベント内の資産を識別するために使用されますか？
A. 送信元、DVC、宛先
B. ホスト、ホスト名、URL、アドレス
C. cidr、port、netbios、saml
D. IPアドレス、MACアドレス、DNS、NT_ホスト
正解: **(**正解を表示します**)**

質問: **41**
高速ストレージの代替場所を指定するにはどうすればよいですか？
A. indexes、conf の Home Path 設定を更新します
B. props、conf の tstatsHomePath 設定を使用します
C. インデックスのストレージ最適化設定を構成します。
D. インデックス、conf で tstatsHomePath 設定を使用します
正解: **(**正解を表示します**)**

質問: **42**
Enterprise Securityのどの機能が、Webサーバーから脅威インテリジェンスデータをダウンロードしますか？
A. 脅威サービスマネージャー
B. 脅威ダウンロードマネージャー
C. 脅威インテリジェンスパーサー
D. セラト情報執行
正解: **B (**コメントを発表する**)**
説明
脅威インテリジェンスフレームワークは、インテリジェンスファイルとデータのダウンロードに必要な設定の大部分を処理するモジュール式入力（脅威インテリジェンスのダウンロード）を提供します。このモジュール式入力にアクセスするには、Inputs.confファイルに「threatlist」という名前のセクションを作成するだけです。」

質問: **43**
アドオンビルダーで、ソースタイプの管理とフィールドの抽出を行った後、次に行う重要なステップは何ですか？
A. データモデルへのマッピング。
B. 検証とパッケージ化
C. データ収集を設定します。
D. アラートアクションを作成します。
正解: **(**正解を表示します**)**

質問: **44**
管理者は、ESにインデックス付けされたデータが改ざんによって侵害されることがないようにしたいと考えている。
この要件を満たす機能は何でしょうか？
A. 指標の一貫性。
B. データ整合性管理。
C. インデクサーへの謝辞。
D. インデックスへのアクセス権限。
正解: **(**正解を表示します**)**
https://answers.splunk.com/answers/790783/anti-tampering-features-to-protect-splunk-logs-the.html

質問: **45**
Splunk Enterprise Security環境において、相関検索が重要な理由は何ですか？
A. 不審な行動を検知し、対応が必要な重要なセキュリティ調査イベントを自動的に生成します。
B. 地理的に分散したクラスタ化されたストレージインフラストラクチャ間で、インデックス付きデータのレプリケーションを効率的に高速化します。
C. エンドポイントテレメトリを、定義済みの共通情報モデルフィールドマッピング構造に自動的に正規化します。
D. 期限切れのコンプライアンスレポートを、長期保存用の規制保管リポジトリに安全にアーカイブします。
正解: **(**正解を表示します**)**
相関検索は、正規化されたデータを継続的に分析し、アナリストによる調査と対応のために注目すべきイベントを自動的に生成することで、疑わしい活動パターンを特定します。

質問: **46**
エンドポイントセキュリティドメインダッシュボードにおけるイベントの発生源の例としては、次のうちどれが該当しますか？
A. ワークステーション、ノートパソコン、POSシステム。
B. 調査最終結果の状況。

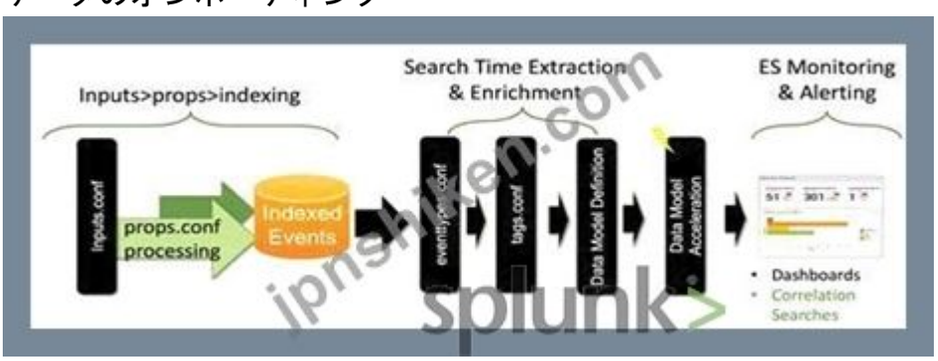
C. インシデントのライフサイクル監査（割り当てから解決まで）。
D. REST API呼び出し。
正解: **C** (コメントを発表する)

質問: **47**
管理者がESをインストールする前に、検索ヘッドを1台プロビジョニングしています。そのマシンに必要なOS、CPU、RAMの最小要件は何ですか？
A. OS :64ビット、RAM :32MB、CPU :16コア
B. OS :64ビット、RAM :12MB、CPU :16コア
C. OS :64ビット、RAM :32MB、CPU :12コア
D. OS :32ビット、RAM :16MB、CPU :12コア
正解: (正解を表示します)

質問: **48**
ESコンテンツをエクスポートすると、拡張子が.splのアプリが自動的に作成されます。ESコンテンツの更新をエクスポートおよびインポートする際のベストプラクティスは何ですか？
A. コンテンツをエクスポートするたびに、新しいアプリ名を使用してください。
B. エクスポートに名前を付ける際に、.spl 拡張子を使用しないでください。
C. エクスポートの際には、既存コンテンツと新規コンテンツを必ず含めてください。
D. 新しいアプリ名を使用するか、既存のコンテンツと新しいコンテンツの両方を常に含めるようにしてください。
正解: (正解を表示します)
説明
ES コンテンツへの更新をエクスポートおよびインポートする際は、Splunk Enterprise Security 管理者ドキュメント 1 に記載されているベスト プラクティスに従う必要があります。ベスト プラクティスの 1 つは、宛先システムの既存のコンテンツを上書きしないことです。これを行うには、2 つのオプションがあります。コンテンツをエクスポートするたびに新しいアプリ名を使用するか、常に既存のコンテンツと新しいコンテンツの両方を各エクスポートに含めるかのいずれかです。この方法で、元のコンテンツを保持し、競合やデータ損失を回避できます。その他のオプション A、B、C は正しくありません。コンテンツをエクスポートするたびに新しいアプリ名を使用することは、オプションの 1 つにすぎず、唯一のオプションではありません。エクスポートに名前を付ける際に .spl 拡張子を使用しても問題ありません。これは Splunk アプリのデフォル

トの拡張子です。各エクスポートに新しいコンテンツのみを含めることは、宛先システムの既存のコンテンツを上書きする可能性があるため、良いプラクティスではありません。
参考文献
Splunk Enterprise Security のコンテンツをアプリとしてエクスポートする

質問: **49**
非標準のフィールド名をCIMフィールド名にマッピングするには、何を使用すればよいですか？
A. フィールドエイリアス。
B. 検索時間抽出。
C. 日。
D. イベントタイプ。
正解: **(**正解を表示します**)**
説明
フィールドエイリアスは、標準以外のフィールド名を CIM フィールド名にマッピングする知識オブジェクトです。フィールドエイリアスを使用すると、データソースが同じ種類のデータに対して異なるフィールド名を使用している場合でも、同じ検索文字列を使用して異なるデータソースからデータを取得できます。たとえば、ソース IP アドレスに src_ip、source_ip、sip など、異なるフィールド名を使用するデータソースがある場合、これらのフィールド名を CIM フィールド名 src にマッピングするフィールドエイリアスを作成できます。これにより、検索やレポートで src を共通のフィールド名として使用でき、Splunk は各データソースに適したフィールド名に自動的に置き換えます。フィールドエイリアスは検索時に適用されるため、元のデータやインデックス作成時のフィールド抽出には影響しません。参照 = 共通情報モデル (CIM) フィールドエイリアスを使用した共通フィールド名への値の正規化、Splunk Enterprise Security へのデータのオンボーディング



質問: **50**
Enterprise Securityをインストールする際、データの正規化に必要なアドオンをインストールした後、何をすべきでしょうか？
A. いいえ、アドオンのための追加手順はありません。
B. コンテンツ管理ダッシュボードからアドオンを設定します。
C. アドオンを使用する準備が整うまでアドオンを無効にし、その後アドオンを有効にします。
D. README またはドキュメントに従ってアドオンを設定してください。
正解: **D (**コメントを発表する**)**

説明/参考資料 :https://docs.splunk.com/Documentation/ES/6.4.1/Install/Planyourdatainputs

質問: **51**
分散構成管理を使用して Splunk_TA_ForIndexers パッケージを作成する場合、どの 3 つのファイルを含めることができますか？
A. indexes.conf、props.conf、transforms.conf
B. web.conf、props.conf、transforms.conf
C. inputs.conf、props.conf、transforms.conf
D. eventtypes.conf、indexes.conf、tags.conf
正解: **(**正解を表示します**)**
https://docs.splunk.com/Documentation/ES/6.4.1/Install/InstallTechnologyAdd-ons

質問: **52**
以下のうち、プロパティ正規化データモデルをテストする方法はどれですか？
A. 監査 -> 正規化監査を使用して、エラー パネルを確認します。
B. | datamodelsearch を実行し、結果をデータモデルの CIM ドキュメントと比較します。
C. | loadjobsearch を実行し、タグ値を調べて、エンコーディングに基づいて既知のタグと比較します。
D. | datamodelsearch を実行し、結果を ES 正規化ガイドのデータ モデルのリストと比較します。
正解: **B (**コメントを発表する**)**
説明/参考資料:
https://docs.splunk.com/Documentation/CIM/4.15.0/User/UsetheCIMtonormalizedataatsearchtime

質問: **53**
アドオンビルダーは、新しいアドオンで以下のどの機能を構成できますか？
A. 有効期限切れデータ。
B. データの正規化。
C. データを要約する。
D. データを翻訳します。
正解: **B (**コメントを発表する**)**
説明
正解はBです。データの正規化。アドオンビルダーは、データフィールドを共通情報モデル（CIM）にマッピングすることでデータを正規化する新しいアドオンを構成できます。CIMは、ドメインやテクノロジーを横断してデータを記述するための共通言語を提供します。データを正規化することで、Splunk Enterprise SecurityやSplunk IT Service Intelligenceなどの他のSplunkアプリでデータを使用できるようになります。アドオンビルダーは、さまざまなソースからのデータの収集、データからのフィールドの抽出、アラートアクションと適応型応答アクションの作成、アドオンのテストと検証など、新しいアドオンの他の機能も構成できます。

ただし、アドオンビルダーでは、アドオンにデータの有効期限切れ、データの集計、データの翻訳などの設定を行うことはできません。
これらはアドオンビルダーの機能ではありません。参照
Splunkアドオンビルダー
[Splunk Webで共通情報モデルを使用する]

質問: **54**
以下のうち、ESで使用されているデータモデルはどれですか？（該当するものをすべて選択してください）
A. Web
B. 異常
C. 認証
D. ネットワークトラフィック
正解: **(**正解を表示します**)**
説明
Splunk Enterprise Security で使用されるデータ モデルは、共通情報モデル アドオン (Splunk_SA_CIM) および Enterprise Security 固有のデータ モデルによって定義および提供されるものです。共通情報モデル アドオンには、Web、認証、ネットワーク トラフィック、変更、DLP、電子メール、エンドポイント、侵入検知、マルウェア、パフォーマンス、チケット管理、脆弱性 1 など、セキュリティ データのさまざまなドメインをカバーする 12 のデータ モデルが含まれています。Enterprise Security 固有のデータ モデルは、異常、監査、ビジネス コンテキスト、データ損失防止、ID 管理、リスク、脅威インテリジェンス、Web プロキシ 2 です。したがって、ES で使用されるデータ モデルは、Web、認証、ネットワーク トラフィック、異常などです。
参照 = 1: Splunk 共通情報モデルの概要 - Splunk ドキュメント - Splunk 共通情報モデル アドオンに含まれるデータ モデル。2: Splunk Enterprise Security のデータ モデル - Splunk ドキュメント - Enterprise Security 固有のデータ モデル。

質問: **55**
ESデータモデルの高速化におけるデフォルトのスケジュールは何ですか？
A. 1分
B. 5分
C. 15分
D. 1時間
正解: **(**正解を表示します**)**
説明／参考資料：
https://docs.splunk.com/Documentation/Splunk/8.0.2/Knowledge/Acceleratedatamodels

質問: **56**
分散構成管理の自動展開機能を使用して indexes.conf を配布する場合、次のうちどれがリスクとなりますか？

A. インデクサーがクラッシュする可能性があります。
B. インデクサーが処理中である可能性があります。
C. インデクサーにアクセスできない可能性があります。
D. インデクサーには異なる設定があります。
正解: **(**正解を表示します**)**
説明/参考資料: https://docs.splunk.com/Documentation/Splunk/8.0.2/Admin/Indexesconf

質問: **57**
ダッシュボード要件マトリックス文書の主な目的は何ですか？
A. 各ダッシュボードが依存するデータモデルを識別します。
B. ローカルデータモデルに合わせて各ダッシュボードをカスタマイズするための手順を提供します。
C. ダッシュボードで使用される検索を識別します。
D. 各ダッシュボードに依存するデータモデルを特定します。
正解: **(**正解を表示します**)**
説明
ダッシュボード要件マトリックス文書の主な目的は、Splunk Enterprise Security の各ダッシュボードが依存するデータモデルを特定することです。ダッシュボード要件マトリックス文書は、Splunk Enterprise Security のすべてのダッシュボードと、それらを構成するデータモデルデータセットを一覧表示する Web ページです。データモデルデータセットは、共通情報モデル (CIM) ドキュメントにリンクされており、イベントが CIM に準拠するために使用する必要があるタグ、フィールド名、およびフィールド値が説明されています。ダッシュボード要件マトリックス文書は、Splunk Enterprise Security の展開で有効化および高速化する必要のあるデータモデルと、テクノロジーアドオンを使用してデータモデルにマッピングする必要のあるデータソースを判断するのに役立ちます。参照 = Splunk Enterprise Security のダッシュボード要件マトリックス、Splunk 共通情報モデルのデータモデル

質問: **58**
ユーザーアクティビティダッシュボード内のリモートアクセスパネルに、直近1時間分のデータが表示されません。
検索漏れなどの潜在的なエラーがないか、どのデータモデルをチェックすべきでしょうか？
A. Web
B. リスク
C. パフォーマンス
D. 認証
正解: **(**正解を表示します**)**
https://docs.splunk.com/Documentation/ES/6.6.0/Admin/Dashboardrequirements - ユーザーアクティビティダッシュボード、リモートアクセスパネルを確認してください

質問: **59**

推奨アクション」と 適応的対応アクション」はどちらも適応的対応を利用していますが、両者の違いは何でしょうか？
A. 推奨アクションはアナリストにテキストによる説明を表示し、適応型応答アクションはエンコードされた形で表示します。
B. 推奨アクションはアナリストに適応型レスポンスのリストを表示し、適応型レスポンスアクションはそれらを自動的に実行します。
C. 推奨アクションには、既に実行された適応型応答のリストが表示され、適応型応答アクションはそれらを自動的に実行します。
D. 推奨アクションは、アナリストに適応型応答のリストを表示します。適応型応答アクションは、アナリストの介入により手動で実行されます。
正解: **B** (コメントを発表する)
推奨される適応型対応策を特定すると、アナリストが利用可能な対応策のリストを確認する際に、それらの対応策が強調表示されるため、利用可能な対応策の長いリストの中から簡単に見つけることができます。

質問: **60**
データ処理の高速化には、年間で1日あたりのデータ量のおよそ何倍の追加ストレージ容量が必要になりますか？
A. 3.4
B. 5.7
C. 1.0
D. 2.5
正解: **A** (コメントを発表する)
https://docs.splunk.com/Documentation/ES/6.4.1/Install/Datamodels

質問: **61**
当該サイトには、CIM準拠アプリケーションと非CIM準拠アプリケーションが混在して動作する、既存の検索ヘッドが1つ存在する。
すべてのアプリケーションはミッションクリティカルです。顧客はコストを慎重に管理したいと考えていますが、ESのパフォーマンスも良好にしたいと考えています。ESをインストールする際のベストプラクティスは何でしょうか？
A. 既存の検索ヘッドにESをインストールします。
B. 新しい検索ヘッドを追加し、そこにESをインストールします。
C. 検索ヘッドのCPU数とメモリ容量を増やしてからESをインストールします。
D. 検索ヘッドからCIMに準拠していないアプリを削除してから、ESをインストールします。
正解: (正解を表示します)

質問: **62**
管理者は、ESインデックス化されたデータが改ざんによって侵害されることがないようにしたいと考えています。この要件を満たす機能は何でしょうか？
A. 指標の一貫性。
B. データ整合性管理。
C. インデクサーへの謝辞。
D. インデックスへのアクセス権限。
正解: **B** (コメントを発表する)
参照：
.html

質問: **63**
Splunk Enterprise Securityにアドオンを自動的にインポートできるようにするには、次のうちどれを使用すればよいですか？
A. CIM_の接頭辞
B. .spl の接尾辞
C. TECH_の接頭辞
D. Splunk_TA_ の接頭辞
正解: **D** (コメントを発表する)
https://dev.splunk.com/enterprise/docs/developapps/enterprisesecurity/planintegrationes/

質問: **64**
CIMデータモデルでは、デフォルトでどのインデックスが検索されますか？
A. 注目すべきデフォルト
B. 概要と注目すべき点
C. _内部および概要
D. すべてのインデックス
正解: (正解を表示します)
説明
デフォルトでは、CIM データ モデルは Splunk Enterprise Security のすべてのインデックスを検索します。つまり、データ モデルのタグとフィールドに一致するイベントは、それが格納されているインデックスに関係なく、データ モデルに含めることができます。ただし、これは、特にデータ モデルに関連するデータを含まないインデックスが多数ある場合、データ モデルの検索

のパフォーマンスと効率にも影響を与える可能性があります。そのため、CIM アドオンの indexes allow list 設定を使用して、各データ モデルが検索するインデックスを制限することをお勧めします。indexes allow list は、データ モデルの検索に含めるインデックスをカンマで区切ったリストです。インデックス名またはインデックス マクロを指定できます。たとえば、Authentication データ モデルの indexes allow list を index=main、index=security、index=auth に設定して、検索を 3 つのインデックスのみに制限できます 12。参照 = 1: Enterprise Security でのデータ モデルの管理 - Splunk Lantern - Indexes allow list。2: Splunk Common Information Model の概要 - Splunk ドキュメント - CIM が存在する理由。

質問: **65**
ESをインストールする前に、以下のどの操作が必要になる可能性がありますか？
A. 追加のインデクサーを追加します。
B. 追加の転送業者を追加してください。
C. KVストアをパージします。
D. 分散検索接続をリダイレクトします。
正解: **A (**コメントを発表する**)**

質問: **66**
ネットワーク全体の活動において、どのようなネットワークサービスが使用されているかを把握するために、エンタープライズセキュリティの以下のダッシュボードのうち、どれが最も関連性の高いデータを含んでいますか？
A. 侵入検知センター
B. プロトコル分析
C. ユーザーインテリジェンス
D. 脅威インテリジェンス
正解: **(**正解を表示します**)**
説明

質問: **67**
データ処理の高速化には、年間で1日あたりのデータ量のおよそ何倍の追加ストレージ容量が必要になりますか？
A. 3.4
B. 5.7
C. 1.0
D. 2.5
正解: **(**正解を表示します**)**
説明
Splunk Lanternの記事 「エンタープライズセキュリティにおけるデータモデルの管理」によると、高速データには、年間で1日のデータ量の約3.4倍の追加ストレージ容量が必要となります[1]。つま

り、1日の入力量が100GBの場合、高速データモデルの年間ストレージ容量は100GB × 3.4 = 340GBとなります。この推定値は、データモデルの構成、データ保持ポリシー、およびインデクサクラスタのレプリケーション係数によって異なる場合があります。参考文献 = エンタープライズセキュリティにおけるデータモデルの管理

質問: **68**
セキュリティアナリストがネットワーク異常を調査する際に使用するES機能は次のうちどれですか？
A. 相関エディタ。
B. 主要指標の検索。
C. 脅威ダウンロードダッシュボード。
D. プロトコルインテリジェンスダッシュボード。
正解: **D** (コメントを発表する)
説明／参考資料 :https://www.splunk.com/en_us/products/premium-solutions/splunk-enterprise-security/features.html

質問: **69**
ESのインストール後、管理者はess_userロールを持つユーザーに、注目すべきイベントを閉じる権限を設定しました。
管理者は、これらのユーザーが解決済みの注目すべきイベントのステータスを 「クローズ済み」に変更できないようにするには、どのように制限すればよいでしょうか？
A. Splunkアクセス制御からess_userロールを選択し、edit_notable_events機能を削除します。
B. エンタープライズセキュリティで、ess_userロールに 「注目すべきイベントを所有する」権限を付与します。
C. ステータス設定ウィンドウから 「解決済み」ステータスを選択します。 「クローズ済み」ステータスのステータス遷移からess_userを削除します。
D. ステータス設定ウィンドウから 「クローズ」ステータスを選択します。 「解決済み」ステータスのステータス遷移からess_userを削除します。
正解: **C** (コメントを発表する)

質問: **70**
以下のうち、プロパティ正規化データモデルをテストする方法はどれですか？
A. 監査 -> 正規化監査を使用して、エラー パネルを確認します。
B. データモデル検索を実行し、結果をデータモデルの CIM ドキュメントと比較します。
C. loadjob検索を実行し、タグ値を調べて、エンコーディングに基づいて既知のタグと比較します。
D. データモデル検索を実行し、結果をES正規化ガイドのデータモデルのリストと比較します。
正解: (正解を表示します)
https://docs.splunk.com/Documentation/CIM/4.15.0/User/UsetheCIMtonormalizedataatsearchtime

質問: **71**
ソースタイプの管理とフィールドの抽出が終わったら、アドオンビルダーで次に行う重要なステップは何ですか？
A. データ収集を設定します。
B. 検証とパッケージ化。
C. アラートアクションを作成します。
D. データモデルへのマッピング。
正解: **D** (コメントを発表する)
この手順により、データが適切に構造化され、共通情報モデル（CIM）に準拠していることが保証され、Splunk環境内での統合と使いやすさが向上します。

質問: **72**
どの機能に、ESの実装時に役立つシナリオが含まれていますか？
A. 適応反応
B. 相関検索
C. ユースケースライブラリ
D. 予測分析
正解: (正解を表示します)
説明／参考資料 :https://www.splunk.com/pdfs/professional-services/2019/splunk-enterprise-security-implementation-success.pdf

質問: **73**
ESウィンドウの下部にある横棒は何ですか？
A. 捜査官作業台。
B. 捜査弁護士。
C. コンプライアンスバー。
D. アナリストバー。
正解: (正解を表示します)
https://docs.splunk.com/Documentation/ES/6.4.1/User/Startaninvestigation

質問: **74**
ES検索ヘッドはどこに設置すべきですか？
A. Splunkを新規インストールしたサーバー上。
B. Splunk DB Connect を実行している Splunk サーバー上。
C. 任意のSplunkサーバー上。
D. 最上位レベルの可視性を持つSplunkサーバー上。
正解: **C** (コメントを発表する)

質問: **75**

ESのインストール後、管理者はess_userロールを持つユーザーに、注目すべきイベントを閉じる権限を設定しました。
管理者は、これらのユーザーが解決済みの注目すべきイベントのステータスを クローズ済み」に変更できないようにするには、どのように制限すればよいでしょうか？
A. エンタープライズセキュリティで、ess_userロールに 注目すべきイベントを所有する」権限を付与します。
B. ステータス設定ウィンドウから クローズ」ステータスを選択します。 解決済み」ステータスのステータス遷移からess_userを削除します。
C. ステータス設定ウィンドウから 解決済み」ステータスを選択します。 クローズ済み」ステータスのステータス遷移からess_userを削除します。
D. Splunkアクセス制御からess_userロールを選択し、edit_notable_events機能を削除します。
正解: (正解を表示します)
説明
Splunk Enterprise Security のステータス設定ウィンドウでは、注目すべきイベントの調査ステータスとステータス遷移を管理およびカスタマイズできます。注目すべきイベントのステータスをあるステータスから別のステータスに変更できるロールを指定できます。たとえば、ess_user ロールを 解決済み」の注目すべきイベントのステータスを クローズ済み」に変更できないようにするには、 クローズ済み」ステータスのステータス遷移から ess_user ロールを削除します。これにより、 クローズ済み」ステータスに変更する権限を持つロールのみが、 解決済み」の注目すべきイベントをクローズできるようになります。参照 = Splunk Enterprise Security での調査ステータスの管理とカスタマイズ

質問: **76**
注目すべきイベントのショートIDを作成するオプションはどこにありますか？
A. 追加フィールド。
B. イベントの詳細。
C. 関連イベント。
D. 説明。
正解: (正解を表示します)
説明/参考資料：
https://docs.splunk.com/Documentation/ES/6.4.1/User/Takeactiononanotableevent

質問: **77**
| tstats コマンドのどの引数を使用すると、検索対象を要約データのみに制限できますか？
A. 要約=t
B. 要約=すべて
C. summariesonly=t
D. summariesonly=all
正解: **(正解を表示します)**
説明
tstats コマンドの検索対象を要約データのみに制限する引数は summariesonly=t です。
要約データは、データモデルの高速化プロセスによって生成されるデータであり、データモデルの要約インデックス（TSIDX ファイル）を作成します。summariesonly=t を使用すると、tstats コマンドは要約インデックスのみを検索するため、検索のパフォーマンスと効率が向上します。ただし、これは、データモデルの高速化でカバーされていないイベント（高速化の時間範囲外のイベントや、データモデルの制約に一致しないイベントなど）は検索結果に返されないことも意味します。12. 参照 = 1:
tstats - Splunk ドキュメント - 要約のみ。2: エンタープライズ セキュリティでのデータ モデルの管理 - Splunk Lantern - インデックスはリストを許可します。
Splunk Tstatsで楽しく または苦痛を軽減して）| Deductiv

質問: **78**
以下のどの操作が、相関検索における偽陽性の数を減らすことにはつながらないでしょうか？
A. 重症度を軽減する。
B. スロットリングフィールドの削除。

C. スロットリングウィンドウを拡大します。
D. 閾値感度の向上。
正解: **B** (コメントを発表する)
説明
スロットリング フィールドを削除しても、相関検索による誤検出の数は減りません。スロットリング フィールドとは、イベントをグループ化し、重複するアラートを抑制するために使用されるフィールドです。たとえば、src と dest をスロットリング フィールドとして使用すると、相関検索では、スロットリング ウィンドウ内の src と dest の値の一意のペアごとに 1 つのアラートのみが生成されます。これにより、同じ問題に対するアラートの繰り返しを回避し、誤検出の数を減らすことができます。スロットリング フィールドを削除すると、相関検索によって生成されるアラートの数が増え、誤検出が増える可能性があります。その他の操作は、相関検索の感度を下げたり、頻度を減らしたりすることで、誤検出の数を減らすのに役立ちます。深刻度を下げると、アラートの優先度が下がり、目立たなくなります。スロットリング ウィンドウを広げると、同じ問題に対するアラート間の時間間隔が長くなります。しきい値の感度を上げると、相関検索の選択性が高くなり、アラートをトリガーするためにより多くの証拠が必要になります。参考資料 = Splunk Enterprise Security での相関検索の設定 Enterprise Security での相関検索の最適化

質問: **79**
ESデータモデルの高速化におけるデフォルトのスケジュールは何ですか？
A. 1分
B. 5分
C. 15分
D. 1時間
正解: **B** (コメントを発表する)
https://docs.splunk.com/Documentation/Splunk/8.0.2/Knowledge/Acceleratedatamodels

質問: **80**
新しいESインストール環境で一連の相関検索が有効になり、結果が監視されています。そのうちの1つの相関検索で多数の注目すべきイベントが発生しましたが、評価の結果、それらは誤検出であることが判明しました。
この問題の解決策は何ですか？
A. その相関検索から注目すべきイベントを除外します。
B. 相関検索のデフォルトの状態と重要度を変更します。
C. ストレージ要件を削減するために、相関検索の高速化を無効にします。
D. サイトの相関スケジュールと感度を変更します。
正解: (正解を表示します)

質問: **81**
個人情報に関する詳細情報はどこに保存されていますか？
A. 身元調査官索引。

B. アクセス異常コレクション。
C. ユーザーアクティビティ指標。
D. 本人確認用CSVファイル。
正解: **(**正解を表示します**)**
説明
Splunk Enterprise Security の Identity Lookup CSV ファイルには、ユーザー名、メールアドレス、電話番号、役割などの ID に関する詳細情報が格納されています。Identity Lookup CSV ファイルは、Active Directory、LDAP、カスタム ID リストなど、さまざまなデータ ソースから収集および抽出された ID データを含むルックアップ ファイルです。Identity Lookup CSV ファイルは、イベントに ID 情報を付加したり、ID 相関検索に基づいて注目すべきイベントを生成したりするために使用されます。Identity Lookup CSV ファイルは、Splunk Enterprise Security の [資産および ID 管理] ページを使用して表示および管理できます。
参考文献
Splunk Enterprise Securityで資産とIDを管理する
本人確認用CSVファイル

質問: **82**
データ正規化の利点は次のうちどれですか？
A. 正規化されたデータタイプであれば、特定のソース技術に関係なく検索を構築できます。
B. フォワーダーベースの入力の方が効率的です。
C. 正規化されたデータモデルはパフォーマンス向上のために最適化できるため、レポートの実行速度が向上します。
D. ダッシュボードの構築には時間がかかります。
正解: **(**正解を表示します**)**
データ正規化により、異なるソースからのデータが共通のスキーマにマッピングされ、一貫性があり、技術に依存しない検索と分析が可能になります。

質問: **83**
カスタム相関検索を作成する際、注目すべきイベントのタイトル、説明、およびドリルダウンフィールドにフィールド値を埋め込むには、どのような形式が使用されますか？
A. %fieldname%
B. "フィールド名"
C. _フィールド名_
D. $fieldname$
正解: **(**正解を表示します**)**

質問: **84**
管理者は、ESをインストールする前に、検索ヘッドを1つプロビジョニングしています。
そのマシンに必要なOS、CPU、RAMの最小要件は何ですか？
A. OS :32ビット、RAM :16MB、CPU :12コア

B. OS :64ビット、RAM :32MB、CPU :12コア
C. OS :64ビット、RAM :12MB、CPU :16コア
D. OS :64ビット、RAM :32MB、CPU :16コア
正解: **D** (コメントを発表する)
https://docs.splunk.com/Documentation/ES/6.4.0/Install/DeploymentPlanning

質問: **85**
注目すべき事象の緊急度はどのように算出されるのですか？
A. 資産の優先順位と脅威の重み。
B. 相関検索によって検出されたアラートの深刻度。
C. 相関検索によって検出された資産または身元リスクと深刻度。
D. 相関検索によって設定された深刻度と、関連する資産またはIDに割り当てられた優先度。
正解: (正解を表示します)
説明/参考資料 :https://docs.splunk.com/Documentation/ES/6.1.0/User/Howurgencyisassigned

質問: **86**
Splunk_TA_ForIndexes.splは、ESのインストールプロセスのどの段階でインデクサーにデプロイされるべきですか？
A. デプロイメントサーバーにアプリを追加するとき。
B. Splunk_TA_ForIndexers.spl が最初にインストールされます。
C. 検索ヘッドにESをインストールし、分散構成管理ツールを実行した後。
D. Splunk_TA_ForIndexers.spl は、クラスターマスターと splunk apply cluster-bundle コマンドを使用してインデクサー クラスター サイトにのみインストールされます。
正解: (正解を表示します)
参照：
https://docs.splunk.com/Documentation/ES/6.1.0/Install/InstallTechnologyAdd-ons

質問: **87**
リスク分析ダッシュボードにはどのようなツールが用意されていますか？
A. リスクスコア別に表示された注目すべきイベント領域。
B. 最もリスクの高い資産と身元情報の表示。
C. 高リスクの脅威。
D. 環境内で最も高い確率で相関関係が見られる主要指標。
正解: (正解を表示します)

質問: **88**
注目すべき出来事の緊急性を生み出すために、どのような2つの分野が組み合わさるのでしょうか？
A. 優先度と深刻度。
B. 優先度と重要度。

C. 重要度と深刻度。
D. 優先順位と時間。
正解: **(**正解を表示します**)**
https://docs.splunk.com/Documentation/ES/6.4.1/User/Howurgencyisassigned

質問: **89**
ESアプリとアドオン $SPLUNK_HOME/etc/apps）は、ステージングインスタンスからクラスタデプロイヤインスタンスのどの場所にコピーする必要がありますか？
A. $SPLUNK_HOME/etc/system/local/
B. $SPLUNK_HOME/var/run/searchpees/
C. $SPLUNK_HOME/etc/shcluster/apps
D. $SPLUNK_HOME/etc/master-apps/
正解: **(**正解を表示します**)**
ステージングインスタンスのアップグレードされたコンテンツはデプロイヤに移行され、検索ヘッドクラスタメンバーにデプロイされます。ステージングインスタンスで、$SPLUNK_HOME/etc/apps をコピーします。
デプロイヤー上の $SPLUNK_HOME/etc/shcluster/apps で、ステージング環境でのアップグレード中に削除された、$SPLUNK_HOME/etc/shcluster/apps 内の非推奨のアプリまたはアドオンを削除します。ステージング環境で生成された ES アップグレード レポートを確認するか、移動されたアプリを調べて確認してください。
ステージング環境の $SPLUNK_HOME/etc/disabled-apps

質問: **90**
ESアプリとアドオン $SPLUNK_HOME/etc/apps）は、ステージングインスタンスからクラスタデプロイヤインスタンスのどの場所にコピーする必要がありますか？
A. $SPLUNK_HOME/etc/master-apps/
B. $SPLUNK_HOME/etc/system/local/
C. $SPLUNK_HOME/etc/shcluster/apps
D. $SPLUNK_HOME/var/run/searchpees/
正解: **(**正解を表示します**)**
説明
ES アプリとアドオンは $SPLUNK_HOME/etc/apps からステージング インスタンスにコピーする必要があります。
クラスターデプロイヤインスタンス上の $SPLUNK_HOME/etc/shcluster/apps の場所。これは、デプロイヤが検索ヘッドクラスターメンバーに配布する構成バンドルを格納するディレクトリです。構成バンドルは、クラスターによって複製されないアプリやその他の構成ファイルで構成されます。デプロイヤは、インデクサークラスターのマスターノードで使用される $SPLUNK_HOME/etc/master-apps/ ディレクトリを使用しません。デプロイヤは、デプロイヤインスタンス自体のローカル構成ファイルを格納するために使用される $SPLUNK_HOME/etc/system/local/ ディレクトリを使用しません。デプロイヤは、

$SPLUNK_HOME/var/run/searchpeers/ ディレクトリは、検索ヘッドがインデクサークラスタピアに関する情報を保存するために使用します。参照 :デプロイヤを使用してアプリと構成の更新を配布する - Splunk ドキュメント、検索ヘッドクラスタ環境に Splunk Enterprise Security をインストールする - Splunk ドキュメント

質問: **91**
「推奨される行動」と「適応的対応行動」はどちらも適応的対応を採用していますが、両者の違いは何でしょうか？
A. 推奨アクションはアナリストにテキストによる説明を表示し、適応型応答アクションはエンコードされた形で表示します。
B. 推奨アクションはアナリストに適応型レスポンスのリストを表示し、適応型レスポンスアクションはそれらを自動的に実行します。
C. 推奨アクションには、既に実行された適応型応答のリストが表示され、適応型応答アクションはそれらを自動的に実行します。
D. 推奨アクションは、アナリストに適応型応答のリストを表示します。適応型応答アクションは、アナリストの介入により手動で実行されます。
正解: **D** (コメントを発表する)
参照：
https://docs.splunk.com/Documentation/ES/latest/Admin/Configureadaptiveresponse

質問: **92**
| tstats コマンドのどの引数を使用すると、検索対象を要約データのみに制限できますか？
A. summariesonly=all
B. summariesonly=t
C. 要約=t
D. 要約=すべて
正解: **B** (コメントを発表する)

質問: **93**
アドオンビルダーは、何から始まるSplunkアプリを作成しますか？
A. で-
B. IN-

C. TA-
D. アプリ-
正解: **(**正解を表示します**)**
説明
Splunk アドオンビルダーは、テクノロジーアドオンを作成するのに役立ちます。テクノロジーアドオンは、環境内の特定のソースからのデータフィードを収集、変換、正規化するのに役立つ特殊なアドオンです。テクノロジーアドオンは、TA と呼ばれることが多く、TA-12 という接頭辞で始まります。参考資料 = 1: Splunk アドオンビルダーユーザーガイド - Splunk アドオンビルダーについて 2: Splunk 開発者ポータル - Splunk アプリの開発

質問: **94**
調査に添付されたファイルはどこに保存されますか？
A. KVストア
B. 注目すべき指標
C. attachments.csv の検索
D. <splunk_home>/etc/apps/SA-Investigations/default/ui/views/attachments
正解: **(**正解を表示します**)**
https://docs.splunk.com/Documentation/ES/6.1.0/Admin/Manageinvestigations

質問: **95**
ガラス製のテーブルには、静止画像やテキスト、アドホック検索の結果、そして次のうちどのオブジェクトを表示できますか？
A. 検索を実行します。
B. 要約データ。
C. セキュリティ指標。
D. メトリクスストア検索。
正解: **C (**コメントを発表する**)**
説明
グラステーブルには、静止画像やテキスト、アドホック検索の結果、およびセキュリティメトリックを表示できます。セキュリティメトリックは、KPI、サービス健全性スコア、または注目すべきイベントの値を表示する視覚化です。グラステーブルエディタの [セキュリティメトリック] メニューを使用して、グラステーブルにセキュリティメトリックを追加できます。また、セキュリティメトリックの外観、動作、およびドリルダウンオプションを設定することもできます。グラステーブルは、ルックアップ検索、集計データ、またはメトリックストア検索を直接表示することはできませんが、これらのタイプの検索をアドホック検索のデータソースとして使用し、その結果をグラステーブルに表示することは可能です。参照 = Splunk Enterprise Security でグラステーブルにセキュリティメトリックを追加する Splunk Enterprise Security でグラステーブルを作成および管理する

質問: **96**

次のうち、ESでデフォルトで設定されている適応アクションはどれですか？
A. 新しいアセットを作成する
B. 注目すべきイベントを作成する
C. 調査を作成する
D. 新しい相関検索を作成する
正解: **(**正解を表示します**)**
説明／参考資料：

質問: **97**
次のうち、ESでデフォルトで設定されている適応アクションはどれですか？
A. 注目すべきイベントを作成する
B. 新しい相関検索を作成する
C. 調査を作成する
D. 新しいアセットを作成する
正解: **A (**コメントを発表する**)**
説明
Splunk Enterprise Securityのドキュメントによると、「注目すべきイベントの作成」アダプティブレスポンスアクションは、ESにデフォルトで設定されているアダプティブレスポンスアクションの1つです。このアクションを使用すると、相関検索の結果、または他の注目すべきイベントの詳細から、注目すべきイベントを作成できます。注目すべきイベントのタイトル、説明、緊急度、所有者、その他のフィールドをカスタマイズできます。「注目すべきイベントの作成」アクションは、特定の条件や基準に基づいてアラートやタスクを作成する場合に便利です。
したがって、正解はAです。注目すべきイベントを作成します。参照 = 注目すべきイベントを作成します。

質問: **98**
コンテンツ管理ページを使用してESからエクスポートできるものは何ですか？
A. 相関検索、管理ルックアップ、およびグラステーブルのみ。
B. 相関検索、ガラステーブル、作業台パネルのみ。
C. コンテンツ管理ページに記載されているすべてのコンテンツタイプ。
D. 相関検索のみ。
正解: **C (**コメントを発表する**)**

質問: **99**
Splunk Enterprise Securityが機能するために、デフォルトで設定する必要があるポートは次のうちどれですか？
A. SplunkWeb (8000)、Splunk Management (8089)、KV Store (8191)
B. SplunkWeb (8088)、Splunk Management (8089)、KV Store (8000)
C. SplunkWeb (8043)、Splunk Management (8088)、KV Store (8191)
D. SplunkWeb (8386)、Splunk Management (8926)、KV Store (8106)

正解: (正解を表示します)
https://docs.splunk.com/Documentation/Splunk/8.1.2/Security/SecureSplunkonyournetwork

質問: **100**
ESコンテンツをエクスポートすると、拡張子が.splのアプリが自動的に作成されます。ESコンテンツの更新をエクスポートおよびインポートする際のベストプラクティスは何ですか？
A. コンテンツをエクスポートするたびに、新しいアプリ名を使用してください。
B. エクスポートに名前を付ける際に、.spl 拡張子を使用しないでください。
C. エクスポートの際には、既存コンテンツと新規コンテンツを必ず含めてください。
D. 新しいアプリ名を使用するか、既存のコンテンツと新しいコンテンツの両方を常に含めるようにしてください。
正解: **A** (コメントを発表する)

質問: **101**
コンテンツ管理ページを使用してESからエクスポートできるものは何ですか？
A. 相関検索、管理ルックアップ、およびグラステーブルのみ。
B. 相関検索のみ。
C. コンテンツ管理ページに記載されているすべてのコンテンツタイプ。
D. 相関検索、ガラステーブル、作業台パネルのみ。
正解: (正解を表示します)
コンテンツ管理ページで、カスタム検索リストから該当するコンテンツタイプを選択し、「エクスポート」を選択することで、任意のコンテンツタイプをエクスポートできます。

質問: **102**
注目すべき出来事の緊急性を生み出すために、どのような2つの分野が組み合わさるのでしょうか？
A. 優先度と深刻度。
B. 優先度と重要度。
C. 重要度と深刻度。
D. 優先順位と時間。
正解: (正解を表示します)
説明/参考資料 :https://docs.splunk.com/Documentation/ES/6.4.1/User/Howurgencyisassigned

質問: **103**
適応反応は何によって引き起こされるのでしょうか？
A. インシデントレビューダッシュボード上の相関検索とユーザーによる。
B. 相関検索とカスタム技術アドオンによる。
C. 脅威分析ダッシュボード上の相関検索とユーザーによる。
D. リスク分析ダッシュボード上のカスタム技術アドオンとユーザーによる。
正解: (正解を表示します)

これらの対応は、相関検索の結果に基づく自動アクションである場合もあれば、インシデントレビュープロセス中にユーザーが手動でトリガーする場合もある。

質問: **104**
資産またはIDリストのどの列がイベントセキュリティと組み合わされて、注目すべきイベントの緊急度を決定しますか？
A. VIP
B. 優先
C. 重要性
D. 臨界性
正解: **(**正解を表示します**)**
参照：
https://docs.splunk.com/Documentation/ES/6.1.0/User/Howurgencyisassigned

質問: **105**
管理者はESアプリを通じて新しいルックアップを追加するにはどうすればよいですか？
A. 設定 -> ルックアップ -> ルックアップ定義でルックアップファイルをアップロードしてください
B. 設定 -> ルックアップ -> ルックアップテーブルファイルでルックアップファイルをアップロードします。
C. ルックアップファイルを /etc/apps/SplunkEnterpriseSecuritySuite/lookups に追加します。
D. 設定 -> コンテンツ管理 -> 新規コンテンツの作成 -> 管理ルックアップを使用してルックアップファイルをアップロードします。
正解: **(**正解を表示します**)**
説明
ESアプリで新しいルックアップを追加する正しい方法は、設定 > コンテンツ管理 > 新規コンテンツの作成 > 管理ルックアップを使用してルックアップファイルをアップロードすることです。これにより、ユーザーは既存のルックアップファイルと定義を作成または選択し、ルックアップの種類、ラベル、説明を指定して、ルックアップファイルの編集を有効にできます。また、ルックアップファイルはアプリケーションレベルで保存されるため、編集や共有が容易になります。
その他のオプションは、正しくないか、ES では推奨されません。設定 > ルックアップ > ルックアップ テーブル ファイルでルックアップ ファイルをアップロードしても、ルックアップ定義やルックアップのラベルと説明は作成されません。
設定 > ルックアップ > ルックアップ定義でルックアップファイルをアップロードしても、ルックアップファイル自体はアップロードされず、既存のファイルの定義が作成されるだけです。
/etc/apps/SplunkEnterpriseSecuritySuite/lookups はファイルシステムの編集を手動で行う必要があり、ES では推奨されません。参照 = Splunk Enterprise Security でのルックアップの作成と管理

質問: **106**
ESのインストール準備における最初のステップは何ですか？
A. ESをインストールします。
B. 使用したデータソースを特定する。
C. 必要なハードウェアを決定します。
D. 設置規模と範囲を決定する。
正解: **(**正解を表示します**)**
説明／参考資料：

質問: **107**
データ処理の高速化には、年間で1日あたりのデータ量のおよそ何倍の追加ストレージ容量が必要になりますか？
A. 3.4
B. 5.7
C. 2.5
D. 1.0
正解: **(**正解を表示します**)**

質問: **108**
分散構成管理の自動展開機能を使用して indexes.conf を配布する場合、次のうちどれがリスクとなりますか？
A. インデックスが暴落する可能性があります。
B. インデックスが処理中である可能性があります。
C. インデックスにアクセスできない可能性があります。
D. インデックスには異なる設定があります。
正解: **A (**コメントを発表する**)**
参照：
https://docs.splunk.com/Documentation/Splunk/8.0.2/Admin/Indexesconf

質問: **109**
管理者がESをインストールする前に、検索ヘッドを1台プロビジョニングしています。そのマシンに必要なOS、CPU、RAMの最小要件は何ですか？

A. OS :32ビット、RAM :16MB、CPU :12コア
B. OS :64ビット、RAM :32MB、CPU :12コア
C. OS :64ビット、RAM :12MB、CPU :16コア
D. OS :64ビット、RAM :32MB、CPU :16コア
正解: **(**正解を表示します**)**
説明
Splunk Enterprise Security Admin ドキュメントによると、ES を実行する専用サーチヘッドの最小ハードウェア要件は次のとおりです。OS: 64 ビット、RAM: 32 GB、CPU: 16 コア。これらの要件は、サーチヘッドが ES の実行以外のタスクを実行しないことを前提としています。また、ドキュメントでは、サーチヘッド用に少なくとも 500 GB のディスク容量を確保することを推奨しています。
参考資料 = Splunk Enterprise Security 管理者向けドキュメント

質問: **110**
この写真の赤い枠の中には、どのような値が含まれていますか？

A. 情報源のランキング。
B. イベントの優先順位。
C. リスクスコア。
D. IPアドレスの評価。
正解: **(**正解を表示します**)**

質問: **111**
次のうち、Web Intelligenceダッシュボードはどれですか？
A. エンドポイントセンター
B. ストリーム:httpプロトコルダッシュボード
C. HTTPカテゴリ分析
D. ネットワークセンター
正解: **C (**コメントを発表する**)**

質問: **112**
セキュリティ態勢ダッシュボードには何が表示されますか？

A. 進行中の捜査とその状況。
B. 注目すべき出来事の概要。
C. SOCが現在追跡している脅威。
D. セキュリティツールの状態を表示します。
正解: **(**正解を表示します**)**
説明
セキュリティ態勢ダッシュボードは、展開環境のすべてのドメインにおける注目すべきイベントの概要を、セキュリティオペレーションセンター（SOC）での表示に適した形で表示します。このダッシュボードには、過去24時間のすべてのイベントと、過去24時間の傾向が表示され、リアルタイムのイベント情報と更新情報も提供されます。ダッシュボードは、主要指標、緊急度別の注目すべきイベント、時間の経過に伴う注目すべきイベント、最も注目すべきイベント、および最も注目すべきイベントソース1を表示する複数のパネルで構成されています。参照 :セキュリティ態勢ダッシュボード - Splunkドキュメント

質問: **113**
クラウド環境ではない（オンプレミスの）ESデプロイメントにおいて、インデクサー1台あたり、1日あたりの推奨インデックス作成量の最大値はどれくらいですか？
A. 500 MB
B. 50GB
C. 300GB
D. 100 GB
正解: **(**正解を表示します**)**

質問: **114**
インシデントレビューダッシュボードで注目すべきイベントを担当するセキュリティチームメンバーには、どのような役割を割り当てるべきですか？
A. ess_user
B. ess_admin
C. ess_analyst
D. ess_reviewer
正解: **C (**コメントを発表する**)**
説明
インシデントレビューダッシュボードで注目すべきイベントを担当するセキュリティチームメンバーに割り当てるべき役割は、ess_analyst 役割です。ess_analyst 役割は、Splunk Enterprise Security で定義済みの役割であり、ユーザーに注目すべきイベントの表示、編集、コメント、ステータスと所有者の変更権限を付与します。ess_analyst 役割では、セキュリティ分析と調査に関連するダッシュボード、レポート、検索にもアクセスできます 12。参照 = 1: Splunk Enterprise Security の役割と機能の概要 - Splunk ドキュメント - ess_analyst 役割。2: インシデントレビュー - Splunk ドキュメント - インシデントレビューダッシュボードで注目すべきイベントをトリアージする。

質問: **115**
ダッシュボード要件マトリックス文書の主な目的は何ですか？
A. ダッシュボードで使用される検索を識別します。
B. ローカルデータモデルに合わせて各ダッシュボードをカスタマイズするための手順を提供します。
C. 各ダッシュボードが依存するデータモデルを識別します。
D. 各ダッシュボードに依存するデータモデルを特定します。
正解: **(正解を表示します)**

質問: **116**
リスクフレームワークは、リスクの増加を示すために、オブジェクト（ユーザー、サーバー、その他のタイプ）にどのような情報を追加するのでしょうか？
A. 緊急です。
B. リスクプロファイル。
C. 集合体。
D. 数値スコア。
正解: **(正解を表示します)**
参照：
https://docs.splunk.com/Documentation/ES/6.1.0/User/RiskScoring

質問: **117**
新しく構築したカスタムダッシュボードを、ES（European Security）のセキュリティアナリストチームが利用できるようにする必要があります。新しいダッシュボードを統合するにはどうすればよいでしょうか？
A. ダッシュボードの権限をes_analystsによるアクセスを許可するように設定し、ナビゲーションエディタを使用してメニューに追加します。
B. ESのホームページに新しいダッシュボードへのリンクを追加します。
C. ダッシュボードをカスタムアドインアプリに追加し、コンテンツマネージャーを使用してESにインストールします。
D. es_analyst から継承した新しいロールを作成し、ダッシュボードの権限を読み取り専用にして、このダッシュボードを新しいロールのデフォルト ビューにします。
正解: **(正解を表示します)**

質問: **118**
データモデルノードにイベントタイプを含めるには、適切なフィールドを抽出した後、次にどのような手順を踏む必要がありますか？
A. 設定を保存します。
B. 正しいタグを適用してください。
C. 正しい検索を実行してください。

D. CIMダッシュボードにアクセスしてください。
正解: **(**正解を表示します**)**
順序は次のようになります: イベントタイプ -> タグ -> データモデル定義 -> データモデルの高速化 -> 検索

質問: **119**
ESから相関検索などのコンテンツをエクスポートできる場所はどこですか？
A. コンテンツエクスポートツール
B. 設定→コンテンツ管理
C. エクスポートコンテンツダッシュボード
D. 設定メニュー→ES→エクスポート
正解: **(**正解を表示します**)**
説明
Splunk Enterprise Security のコンテンツをアプリとしてエクスポートするには、コンテンツ管理ページを使用します。エクスポートオプションを使用すると、カスタムコンテンツを他の ES インスタンスと共有できます。たとえば、開発環境やテスト環境から本番環境にカスタム検索を移行する場合などです。コンテンツ管理ページでは、Splunk Enterprise Security のコンテンツを表示、編集、有効化、無効化、エクスポートできます。また、他の ES インスタンスまたは Splunk Security Essentials アプリからコンテンツをインポートすることもできます。参照 = Splunk Enterprise Security のコンテンツをアプリとしてエクスポートする コンテンツ管理

質問: **120**
適応応答アクションの履歴はどのインデックスに保存されますか？
A. cim_modactions
B. モジュール履歴
C. cim_adaptiveactions
D. モジュール式アクション履歴
正解: **A (**コメントを発表する**)**
https://docs.splunk.com/Documentation/ES/6.1.0/Install/Indexes

質問: **121**
ガラス製のテーブルには、静止画像やテキスト、アドホック検索の結果、そして次のうちどのオブジェクトを表示できますか？
A. 検索を実行します。
B. 要約データ。
C. セキュリティ指標。
D. メトリクスストア検索。
正解: **(**正解を表示します**)**
説明/参考資料: https://docs.splunk.com/Documentation/ES/6.1.0/User/CreateGlassTable

質問: **122**
以下のうち、ESで使用されているデータモデルはどれですか？（該当するものをすべて選択してください）
A. Web
B. 異常
C. 認証
D. ネットワークトラフィック
正解: **(**正解を表示します**)**
参照：
https://dev.splunk.com/enterprise/docs/developapps/enterprisesecurity/datamodelsusedbyes/

有効的な**SPLK-3001**問題集はJPNTest.com提供され、**SPLK-3001**試験に合格することに役に立ちます！JPNTest.comは今最新**SPLK-3001**試験問題集を提供します。JPNTest.com SPLK-3001試験問題集はもう更新されました。ここで**SPLK-3001**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/SPLK-3001-mondaishu
「**118**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」