Splunk.SPLK-3001.v2024-04-23.q108

試験コード:	SPLK-3001
試験名称:	Splunk Enterprise Security Certified Admin Exam
認定資格:	Splunk
無料問題数:	108
バージョン:	v2024-04-23
アクセス数:	1436
ページビュー数:	1080
https://www.jpnpdf.com/Splunk.SPLK-3001.v2024-04-23.q108-mondaishu.html	

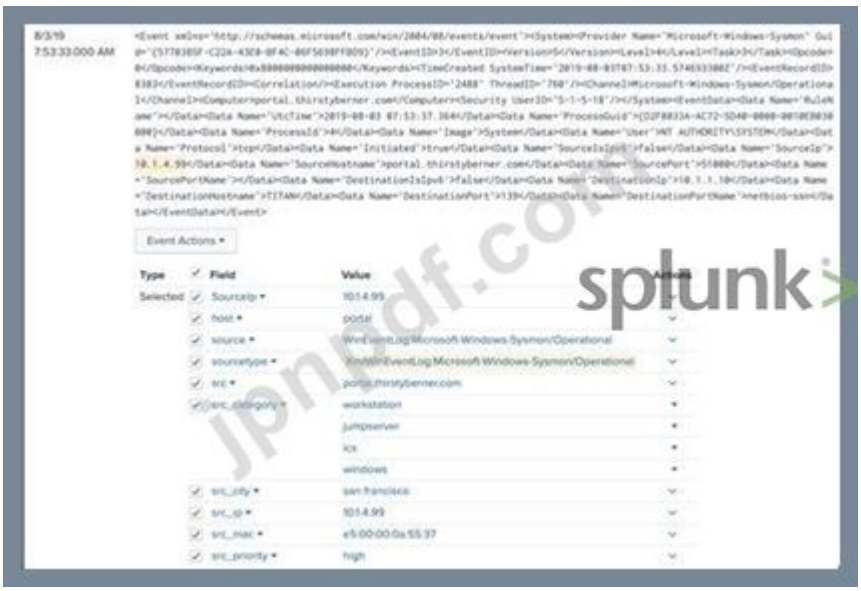
最新問題: **1**
ES は、次のどのオプションを使用してサーチヘッドにインストールする必要がありますか?
A. 他のアプリはありません。
B. インストールされている他のアプリ。
C. TA-* を除くすべてのアプリが削除されました。
D. デフォルトの組み込みアプリと CIM 準拠アプリのみ。
Answer: A (メーッセージを残す**)**
参照：
https://docs.splunk.com/Documentation/ES/6.1.0/Install/InstallEnterpriseSecurity

最新問題: **2**
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 エクスポーター
B. 設定メニュー -> ES -> エクスポート
C. コンテンツのエクスポート ダッシュボード
D. [設定] -> [コンテンツ管理]
Answer: D (メーッセージを残す**)**

最新問題: **3**
調査の添付ファイルはどこに保存されますか?
A. KV ストア
B. 注目すべきインデックス
C. attachments.csv ルックアップ
D. <splunk_home>/etc/apps/SA-Investigations/default/ui/views/attachments
Answer: A (メーッセージを残す**)**
参照：
https://docs.splunk.com/Documentation/ES/6.1.0/Admin/Manageinvestigations

最新問題: **4**
サイトには、CIM と非 CIM 準拠のアプリケーションの両方をホストする単一の既存の検索ヘッドがあります。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、優れた ES パフォーマンスも求めています。
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すか?
A. ES を既存のサーチヘッドにインストールします。
B. 新しいサーチヘッドを追加し、そこに ES をインストールします。
C. サーチヘッドの CPU 数とメモリ量を増やしてから、ES をインストールします。
D. CIM 非準拠のアプリを検索ヘッドから削除してから、ES をインストールします。
Answer: B (メーッセージを残す**)**
説明/参照: https://www.splunk.com/pdfs/technical-briefs/splunk-validated-architectures.pdf

最新問題: **5**
イベント内のアセットを識別するためにアセット ルックアップのどの列が使用されますか?
A. 送信元、DVC、宛先
B. cidr、ポート、netbios、saml
C. ip、mac、dns、nt_host
D. ホスト、ホスト名、URL、アドレス
Answer: C (メーッセージを残す**)**
説明
イベント内のアセットを識別するために使用されるアセット ルックアップの列は、ip、mac、dns、および nt_host です。
これらの列には、IP アドレス、MAC アドレス、DNS 名、NetBIOS 名などの資産のネットワーク識別子が含まれます。Splunk Enterprise Security は、これらの列を使用して、資産フィールドとイベント フィールド (src、dest、dvc、host、hostname など) を照合します。一致するものが見つかると、Splunk Enterprise Security は、カテゴリ、優先度、ビジネス ユニット、場所などの資産情報を使用してイベントを強化します。これにより、アセットの属性とコンテキストに基づいてイベントを検索および分析できます。参考 = アセット ルックアップ CSV ファイル アセットとアイデンティティの相関 Splunk Enterprise Security のアセットとアイデンティティ - パート 1 ...



最新問題: **6**
ES アセットの例は何ですか?
A. MAC アドレス
B. ユーザー名
C. サーバー
D. 人
Answer: (解答を表示する**)**
説明
Splunk Enterprise Security のドキュメントによると、資産とは、サーバー、ワークステーション、ルーター、ファイアウォールなどのネットワーク インフラストラクチャの一部である物理デバイスまたは論理デバイスです。資産には、IP アドレス、MAC アドレス、DNS 名、NT ホスト名、優先度、ビジネス ユニット、所有者などのさまざまな属性を持つことができます。Splunk Enterprise Security は、資産データを使用してセキュリティ イベントを強化および関連付け、分析のためのコンテキストを提供します。Splunk Enterprise Security の 資産とアイデンティティ管理」ページを使用して資産データを管理できます。詳細については、 Splunk Enterprise Security でのアセットと ID の管理」を参照してください。
他のオプションは ES アセットの例ではありませんが、他のタイプのデータに関連している可能性があります。MAC アドレスは資産の属性であり、資産そのものではありません。ユーザー名はアイデンティティの一例であり、資産またはイベントに関連付けられた個人またはグループです。Splunk Enterprise Security は、アイデンティティ データを使用してセキュリティ イベントを強化および関連付け、分析のためのコンテキストを提供します。Splunk Enterprise Security の 資産と ID 管理」ページを使用して ID データを管理できます。詳細については、 Splunk Enterprise Security でのアセットと ID の管理」を参照してください。People は、Splunk Common Information Model (CIM) のデータ モデルであり、さまざまなデータ ソース間でデータ フィールドを編成し、名前を付けるための共通標準を提供します。

Splunk Enterprise Security は CIM を使用して、クロスソース分析とセキュリティ イベントの相関付けを可能にします。
People データ モデルには、ユーザー名、電子メール アドレス、電話番号など、人に関連するイベントのフィールドとタグが含まれています。詳細については、 人物」を参照してください。したがって、正解はCです。
サーバ。参考文献
Splunk Enterprise Security で資産と ID を管理する
人々

最新問題: **7**
Splunk Enterprise Security が機能するために設定する必要があるデフォルトのポートは次のうちどれですか?
A. SplunkWeb (8043)、Splunk Management (8088)、KV ストア (8191)
B. SplunkWeb (8390)、Splunk Management (8323)、KV ストア (8672)
C. SplunkWeb (8068)、Splunk Management (8089)、KV ストア (8000)
D. SplunkWeb (8000)、Splunk Management (8089)、KV ストア (8191)
Answer: (解答を表示する**)**

最新問題: **8**
リスク分析ダッシュボードはどのようなツールを提供しますか?
A. リスク スコア別に表示される注目すべきイベント ドメイン。
B. 最もリスクの高い資産とアイデンティティの表示。
C. 高リスクの脅威。
D. 環境内で最も高い確率の相関検索を示す主要な指標。
Answer: B (メーッセージを残す**)**

最新問題: **9**
管理者は ES アプリを通じて新しいルックアップをどのように追加する必要がありますか?
A. ルックアップ ファイルを /etc/apps/SplunkEnterpriseSecuritySuite/lookups に追加します
B. [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ます。
C. [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。
D. [設定] -> [コンテンツ管理] -> [新しいコンテンツの作成] -> [管理されたルックアップ] 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。
Answer: D (メーッセージを残す**)**

最新問題: **10**
誰が調査を削除できますか?
A. ess_admin ユーザーのみ。

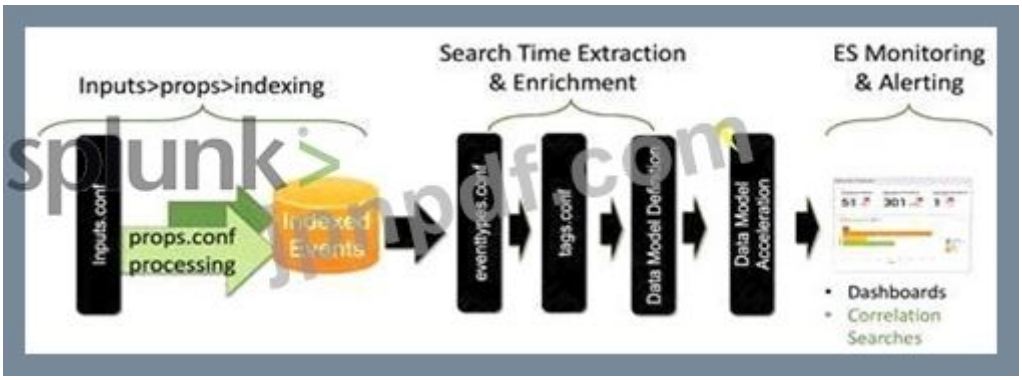
B. 調査所有者のみ。
C. 調査の所有者および ess 管理者。
D. 調査の所有者と協力者。
Answer: A (メーッセージを残す**)**
参照：
https://docs.splunk.com/Documentation/ES/6.1.0/Admin/Manageinvestigations

最新問題**: 11**
アドオン ビルダーはどこから入手できますか?
A. GitHub
B. SplunkBase
C. www.splunk.com
D. ES インストール パッケージ
Answer: (解答を表示する**)**
説明/参照:
https://docs.splunk.com/Documentation/AddonBuilder/3.0.1/UserGuide/installation

最新問題**: 12**
リスクの増加を示すために、リスク フレームワークはオブジェクト (ユーザー、サーバー、またはその他のタイプ) に何を追加しますか?
A. 数値スコア。
B. リスク プロファイル。
C. 集計。
D. 緊急性があります。
Answer: (解答を表示する**)**

最新問題**: 13**
データ正規化のメリットは次のうちどれですか?
A. 正規化されたデータ モデルを最適化してパフォーマンスを向上できるため、レポートの実行が速くなります。
B. ダッシュボードの構築には時間がかかります。
C. 正規化されたデータ型の特定のソース テクノロジに関係なく、検索を構築できます。
D. フォワーダーベースの入力はより効率的です。
Answer: (解答を表示する**)**
説明
Splunk Enterprise Security のドキュメントによると、データ正規化の利点の 1 つは、正規化されたデータ型の特定のソース テクノロジーに関係なく検索を構築できることです。データ正規化は、一貫性と効率性を高めるために共通の形式を使用して Splunk プラットフォームにデータを取り込み、保存する方法です。

データが正規化されると、異なるソースまたはベンダーからの同等のイベントに対して同じフィールド名とイベント タグに従います。これにより、データ形式の違いを気にすることなく、クロスソース分析とセキュリティ イベントの相関関係を実行できます。たとえば、Windows、Linux、および Mac OS システムからのデータがある場合、エンドポイント データ モデルを使用してデータを正規化し、同じフィールドを使用できます。
、および 、すべてのシステムにわたってエンドポイント イベントを検索します。したがって、正解は C です。正規化されたデータ型の特定のソース テクノロジに関係なく、検索を構築できます。参考 = データ ソースと正規化 Splunk Common Information Model アドオン Splunk Enterprise Security へのオンボーディング データ



最新問題: **14**
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 エクスポーター
B. [設定] -> [コンテンツ管理]
C. コンテンツのエクスポート ダッシュボード
D. 設定メニュー -> ES -> エクスポート
Answer: B (メーッセージを残す**)**
説明/参照: https://docs.splunk.com/Documentation/ES/6.1.0/Admin/Export

最新問題: **15**
アドオン ビルダーが新しいアドオンで構成できる機能は次のうちどれですか?
A. データを期限切れにします。
B. データを正規化します。
C. データを要約します。
D. データを変換します。
Answer: (解答を表示する**)**
参照：
https://docs.splunk.com/Documentation/AddonBuilder/3.0.1/UserGuide/Overview

最新問題: **16**
高速ストレージの代替場所を指定するために、indexes.conf でどの設定が使用されますか?
A. 解凍パス

B. tstatsHomePath
C. summaryHomePath
D. warmToColdScript
Answer: B (メーッセージを残す**)**
参照：
https://docs.splunk.com/Documentation/Splunk/8.0.2/Knowledge/Acceleratedatamodels

最新問題**: 17**
Enterprise Security のダッシュボードは主にどの種類のナレッジ オブジェクトからデータを取得しますか?
A. 統計情報
B. KV ストア
C. データモデル
D. 動的検索
Answer: C (メーッセージを残す**)**
参照：
https://docs.splunk.com/Splexicon:Knowledgeobject

最新問題**: 18**
アドオンを Splunk Enterprise Security に自動的にインポートできるのは次のうちどれですか?
A. CIM_ のプレフィックス
B. .spl の接尾辞
C. TECH_ の接頭辞
D. Splunk_TA_ のプレフィックス
Answer: D (メーッセージを残す**)**
参照：
https://dev.splunk.com/enterprise/docs/developapps/enterprisesecurity/planintegrationes/

最新問題**: 19**
推奨されるインストール前の手順は次のうちどれですか?

A. デフォルトの検索アプリを無効にします。
B. サーチヘッド転送を構成します。
C. MongoDB.com から KV ストアの最新バージョンをダウンロードします。
D. 最新の Python ディストリビューションをサーチヘッドにインストールします。
Answer: B (メーッセージを残す**)**

最新問題**: 20**
管理者は、ES をインストールする前に 1 つのサーチ ヘッドをプロビジョニングしています。そのマシンの OS、CPU、RAM の基準最小要件は何ですか?
A. OS: 64 ビット、RAM: 12 MB、CPU: 16 コア
B. OS: 64 ビット、RAM: 32 MB、CPU: 16 コア
C. OS: 32 ビット、RAM: 16 MB、CPU: 12 コア
D. OS: 64 ビット、RAM: 32 MB、CPU: 12 コア
Answer: (解答を表示する**)**

最新問題**: 21**
注目すべきイベントの短縮 ID を作成するオプションはどこにありますか?
A. 寄与するイベント。
B. 説明。
C. イベントの詳細。
D. 追加フィールド。
Answer: C (メーッセージを残す**)**

最新問題**: 22**
アドオン ビルダーは、何で始まる Splunk アプリを作成しますか?
A. だ-
B. SA-
C. た-
D. アプリ-
Answer: C (メーッセージを残す**)**
説明/参照:
https://dev.splunk.com/enterprise/docs/developapps/enterprisesecurity/abouttheessolution/

最新問題**: 23**
注目すべきイベントの短縮 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. 寄与するイベント。
D. 説明。
Answer: B (メーッセージを残す**)**

説明/参照:
https://docs.splunk.com/Documentation/ES/6.4.1/User/Takeactiononanotableevent

最新問題: **24**
ES に対してデフォルトで設定されている適応アクションは次のうちどれですか?
A. 新しいアセットを作成します
B. 注目すべきイベントを作成する
C. 調査を作成します
D. 新しい相関検索を作成します
Answer: D (メーッセージを残す**)**
説明/参照:

最新問題: **25**
ソース タイプを管理し、フィールドを抽出した後、アドオン ビルダーで次の重要なステップはどれですか?
A. データ収集を構成します。
B. データ モデルにマッピングします。
C. アラート アクションを作成します。
D. 検証してパッケージ化します
Answer: B (メーッセージを残す**)**

最新問題: **26**
注目すべきイベントの緊急性はどのように計算されますか?
A. 資産の優先順位と脅威の重み。
B. 相関検索によって見つかった資産またはアイデンティティのリスクと重大度。
C. 相関検索によって見つかったアラートの重大度。
D. 相関検索によって設定された重大度、および関連する資産または ID に割り当てられた優先度。
Answer: D (メーッセージを残す**)**

最新問題: **27**
プロパティ正規化データ モデルをテストする方法は次のうちどれですか?
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. | を実行します。データモデルの検索、結果をデータモデルの CIM ドキュメントと比較します。
C. | を実行します。ロードジョブ検索では、タグ値を確認し、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. | を実行します。datamodel を検索し、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。
Answer: (解答を表示する**)**

説明
適切に正規化されたデータ モデルをテストする 1 つの方法は、| を実行することです。datamodel データ モデルまたはデータ モデル内のデータセットに対して検索し、結果をデータモデルの CIM ドキュメントと比較します。CIM ドキュメントには、各データ モデルとデータセットの予期されるフィールド、タグ、制約、および正規化されたイベントの例が記載されています。| を実行することにより、データモデル検索を使用すると、データ モデルまたはデータセットの JSON 出力を調べて、それが CIM 仕様と一致していることを確認できます。| の検索モード オプションを使用することもできます。datamodel コマンドを使用して、さらに検査または変更できる結果または検索文字列を返します。詳細については、データモデル - Splunk ドキュメント 1 および Splunk Common Information Model の概要 2 を参照してください。参照 = 1: データモデル - Splunk ドキュメント 2: Splunk 共通情報モデルの概要

最新問題: **28**
管理者は、ES をインストールする前に 1 つのサーチ ヘッドをプロビジョニングしています。そのマシンの OS、CPU、RAM の基準最小要件は何ですか?
A. OS: 32 ビット、RAM: 16 MB、CPU: 12 コア
B. OS: 64 ビット、RAM: 32 MB、CPU: 12 コア
C. OS: 64 ビット、RAM: 12 MB、CPU: 16 コア
D. OS: 64 ビット、RAM: 32 MB、CPU: 16 コア
Answer: D (メーッセージを残す**)**
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 の実行以外に他のタスクを実行しないという前提に基づいています。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も推奨しています。
参考文献 = Splunk Enterprise Security Admin ドキュメント

最新問題: **29**
ES は、次のどのオプションを使用してサーチヘッドにインストールする必要がありますか?
A. デフォルトの組み込みアプリと CIM 準拠アプリのみ。
B. インストールされている他のアプリ。
C. TA-* を除くすべてのアプリが削除されました。
D. 他のアプリはありません。
Answer: (解答を表示する**)**

最新問題: **30**
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. インデックス、conf で tstatsHomePath 設定を使用します。

B. props、conf で 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 のホーム パス設定を更新します。
Answer: B (メーッセージを残す**)**

最新問題**: 31**
非クラウド (オンプレミス) ES 導入の場合、インデクサーごとの 1 日あたりのインデックス作成の最大推奨量はどれくらいですか?
A. 50 GB
B. 100 GB
C. 300 GB
D. 500 MB
Answer: B (メーッセージを残す**)**
参照：
https://docs.splunk.com/Documentation/ITSI/4.4.2/Install/Plan

最新問題**: 32**
データを高速化するには、1 日当たりのデータ量の年間約何倍の追加ストレージ スペースが必要ですか?
A. 3.4
B. 5.7
C. 1.0
D. 2.5
Answer: (解答を表示する**)**
説明
Enterprise Security でのデータ モデルの管理に関する Splunk Lantern の記事によると、データを高速化するには、1 日あたりのデータ量の約 3.4 倍の追加ストレージ スペースが年間で必要になります1。これは、毎日の入力量が 100 GB の場合、年間のアクセラレーション データ モデル ストレージは 100 GB x 3.4 = 340 GB になることを意味します。この推定値は、データ モデル構成、データ保持ポリシー、およびインデクサー クラスターのレプリケー

ション係数によって異なる場合があります。参考 = Enterprise Security でのデータ モデルの管理

最新問題: **33**
ES に対してデフォルトで設定されている適応アクションは次のうちどれですか?
A. 調査を作成します
B. 新しい相関検索を作成します
C. 新しいアセットを作成します
D. 注目すべきイベントを作成する
Answer: (解答を表示する**)**

最新問題: **34**
脅威生成検索では何が生成されますか?
A. 注目すべきインデックス内の注目すべき脅威。
B. threat_activity インデックス内のイベント。
C. KV ストア コレクション内のインテルの脅威。
D. 脅威相関検索。
Answer: (解答を表示する**)**

最新問題: **35**
サイトには、CIM と非 CIM 準拠のアプリケーションの両方をホストする単一の既存の検索ヘッドがあります。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、優れた ES パフォーマンスも求めています。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すか?
A. ES を既存のサーチヘッドにインストールします。
B. サーチヘッドの CPU 数とメモリ量を増やしてから、ES をインストールします。
C. CIM 非準拠のアプリを検索ヘッドから削除してから、ES をインストールします。
D. 新しいサーチヘッドを追加し、そこに ES をインストールします。
Answer: D (メーッセージを残す**)**

最新問題: **36**
エンドポイント セキュリティ ドメイン ダッシュボードのイベントのソースの例は次のうちどれですか?
A. REST API の呼び出し。
B. 調査の最終結果ステータス。
C. ワークステーション、ノートブック、および POS システム。
D. 割り当てから解決までのインシデントのライフサイクル監査。
Answer: D (メーッセージを残す**)**
説明/参照:
https://docs.splunk.com/Documentation/ES/6.1.0/User/EndpointProtectionDomaindashboards

最新問題: **37**
ES 申請書は次のどれにアップロードする必要がありますか?
A. インデクサー。
B. KV ストア。
C. 検索ヘッド。
D. 専用フォワーダー。
Answer: (解答を表示する**)**
説明
ES アプリケーションは、ES ユーザー インターフェイスを実行し、検索、アラート、レポートを実行するコンポーネントである検索ヘッドにアップロードする必要があります。サーチヘッドは ES 専用にする必要があり、他のアプリケーションは実行しないでください。インデクサーは、データにインデックスを付けてバケットに保存するコンポーネントです。KV ストアは、データをキーと値のペアとして保存および管理する機能です。専用フォワーダーは、さまざまなソースからデータを収集し、それをインデクサーに転送するコンポーネントです。これらのコンポーネントはいずれも ES アプリケーションを実行できません。参考文献
[Splunk Enterprise Securityのインストール]
[Splunk Enterprise アーキテクチャ]

最新問題: **38**
管理者は、ES インデックス付きデータが改ざんによって侵害される可能性がないことを確認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. インデックスのアクセス権限。
B. インデックスの一貫性。
C. インデクサーの確認応答。
D. データ整合性制御。
Answer: D (メーッセージを残す**)**

最新問題: **39**
ネットワーク アクティビティ全体で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観察するには、Enterprise Security の次のダッシュボードのどれに最も関連性の高いデータが含まれますか?
A. 脅威インテリジェンス
B. プロトコル分析
C. 侵入センター
D. ユーザー インテリジェンス
Answer: (解答を表示する**)**

最新問題: **40**
サイトには、CIM と非 CIM 準拠のアプリケーションの両方をホストする単一の既存の検索ヘッドがあります。
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、優れた ES パフォーマンスも求めています。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すか?
A. ES を既存のサーチヘッドにインストールします。
B. 新しいサーチヘッドを追加し、そこに ES をインストールします。
C. サーチヘッドの CPU 数とメモリ量を増やしてから、ES をインストールします。
D. CIM 非準拠のアプリを検索ヘッドから削除してから、ES をインストールします。
Answer: B (メーッセージを残す**)**
説明
これは、ES がリソースを大量に消費するアプリケーションであり、十分な CPU とメモリを備えた専用の検索ヘッドを必要とするためです。既存のサーチヘッドに ES をインストールすると、パフォーマンスの問題や他のアプリケーションとの競合が発生する可能性があります。CIM に準拠していないアプリはサイトにとってミッションクリティカルであるため、検索ヘッドから削除することはお勧めできません。サーチヘッド上の CPU の数とメモリの量を増やしても、ES やその他のアプリケーションの負荷を処理するには十分ではない可能性があります。したがって、選択肢 B が最も適切な答えです。ES のインストールに関する詳細は、この Web ページで参照できます1。

最新問題: **41**
調査の添付ファイルはどこに保存されますか?
A. KV ストア
B. 注目すべきインデックス
C. attachments.csv ルックアップ
D. <splunk_home>/etc/apps/SA-Investigations/default/ui/views/attachments
Answer: A (メーッセージを残す**)**
説明
調査への添付ファイルは、investigation_attachment という名前の KV ストア コレクションに保存されます。KV ストアは、データをキーと値のペアとして保存および管理する機能です。Splunk Enterprise Security は、KV ストアを使用して、調査、調査イベント、調査リード、調査添付などの複数のコレクションに調査情報を保存します。KV ストア API エンドポイントを使用して、KV ストア コレクションを表示または変更できます。KV ストア API エンドポイントの使用の詳細については、『Splunk Enterprise REST API リファレンス マニュアル』1 の KV ストア エンドポイントの説明を参照してください。他のオプション B、C、D は正しくありません。
調査への添付ファイルは、注目すべきインデックス、attachments.csv ルックアップ、または

<splunk_home>/etc/apps/SA-Investigations/default/ui/views/attachments ディレクトリ。参考 = Splunk Enterprise Security で調査を管理する

最新問題: **42**
調査の添付ファイルはどこに保存されますか?
A. attachments.csv ルックアップ
B. <splunk_home>/etc/apps/SA-Investigations/default/ui/views/attachments
C. 注目すべきインデックス
D. KV ストア
Answer: D (メーッセージを残す**)**

最新問題: **43**
推奨されるインストール前の手順は次のうちどれですか?
A. サーチヘッド転送を構成します。
B. 最新の Python ディストリビューションをサーチヘッドにインストールします。
C. MongoDBxom から KV ストアの最新バージョンをダウンロードします。
D. デフォルトの検索アプリを無効にします。
Answer: A (メーッセージを残す**)**

最新問題: **44**
デフォルト アカウント アクティビティの検出相関検索では、既知のデフォルト アカウントにフラグを立てるためにどのルックアップ テーブルが使用されますか?
A. 管理 ID
B. ローカル ユーザー Intel
C. アイデンティティ
D. 特権アカウント
Answer: B (メーッセージを残す**)**
説明
Splunk Enterprise Security のドキュメントによると、デフォルト アカウント アクティビティの検出相関検索では、ローカル ユーザー Intel ルックアップ テーブルを使用して既知のデフォルト アカウントにフラグを立てます。ローカル ユーザー Intel ルックアップ テーブルには、admin、root、guest など、さまざまなシステムおよび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。相関検索では、認証データ モデルからの認証イベントとルックアップ テーブル内のユーザー名が比較され、一致する場合は注目すべきイベントが生成されます。この注目すべきイベントは、システムまたはアプリケーションへのアクセスにデフォルトのアカウントが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構成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. ローカル ユーザー Intel です。参照 = デフォルト アカウント アクティビティが検出されたローカル ユーザー Intel

最新問題: **45**
ガラステーブルの主な特徴は次のうちどれですか?
A. カスタマイズ。
B. 後で取得できる強力なデータ。
C. インタラクティブな調査。
D. 剛性。
Answer: (解答を表示する**)**

最新問題: **46**
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. インデックスのストレージ最適化設定を構成します。
B. インデックス、conf のホーム パス設定を更新します。
C. props、conf で tstatsHomePath 設定を使用します。
D. インデックス、conf で tstatsHomePath 設定を使用します。
Answer: D (メーッセージを残す**)**
説明
Indexes.conf の tstatsHomePath 設定を使用すると、高速ストレージの代替場所を指定できます。
高速ストレージは、Splunk Enterprise が高速化されたデータモデルの概要データを保存する場所です。
概要データは、データ モデルを使用する検索とレポートを高速化するために使用されます。デフォルトでは、高速化されたストレージは、データ モデルによって参照されるイベントを含むインデックスと同じボリュームに配置されます。ただし、tstatsHomePath 設定を使用して、高速ストレージの場所を別のボリュームまたはパスに変更できます。これは、Splunk Enterprise 導入環境のパフォーマンスとディスク領域の使用量を最適化するのに役立ちます。参考 = 高速ストレージの代替の場所を指定する必要がある場合は、indexes.conf.spec の tstatsHomePath 設定を使用します。

最新問題: **47**
Enterprise Security をインストールした後、分散構成管理ツールを使用して、インデクサーを構成するアプリを作成できますか?

A. Splunk_DS_ForIndexers.spl
B. Splunk_ES_ForIndexers.spl
C. Splunk_SA_ForIndexers.spl
D. Splunk_TA_ForIndexers.spl
Answer: D (メーッセージを残す)
説明
説明/参照: https://docs.splunk.com/Documentation/ES/6.1.0/Install/InstallTechnologyAdd-ons

最新問題**: 48**
次のアクションのうち、全体的な検索パフォーマンスを向上させることができるのはどれですか?
A. インデックス付きリアルタイム検索を無効にします。
B. すべての相関検索の優先順位を上げます。
C. 優先度の低い相関検索の頻度 (スケジュール) を減らします。
D. 誤検知の数が多い相関検索に注目すべきイベントの抑制を追加します。
Answer: C,D (メーッセージを残す)
説明
相関検索は、セキュリティ インシデントやその他の注目すべきイベントを検出するために Splunk Enterprise Security で実行されるスケジュールされた検索です。大量のリソースを消費し、全体的な検索パフォーマンスに影響を与える可能性があります。検索パフォーマンスを向上させるために、次のアクションを実行できます。
優先度の低い相関検索の頻度 (スケジュール) を減らします。これにより、同時に実行される検索の数が減り、一部のリソースが他の検索のために解放されます。相関検索のスケジュールは、Splunk Enterprise Security のコンテンツ管理ページで編集できます。詳細については、 Splunk Enterprise Security での相関検索の編集」を参照してください。
誤検知の数が多い相関検索に対して、注目すべきイベントの抑制を追加します。これにより、相関検索によって関連性のない、または実行不可能な注目すべきイベントが生成されることがなくなり、注目すべきイベント フレームワークの負荷が軽減されます。Splunk Enterprise Security のコンテンツ管理ページで相関検索の抑制ルールを追加できます。詳細については、 Splunk Enterprise Security での重要なイベントの抑制」を参照してください。
他の 2 つのアクションは、検索パフォーマンスやセキュリティ体制に悪影響を与える可能性があるため、推奨されません。インデックス付きリアルタイム検索を無効にすると、一部のダッシュボードやパネルでデータが正しく表示されなくなる可能性があり、すべての相関検索の優先順位を上げると、リソースの競合が発生して他の検索のパフォーマンスが低下する可能性があります。詳細については、 ピークパフォーマンスを実現するための Splunk Enterprise の最適化」および 検索タイプが Splunk Enterprise のパフォーマンスに与える影響」を参照してください。参考 = Splunk Enterprise Security で相関検索を編集する Splunk Enterprise Security で注目すべきイベントを抑制する ピークパフォーマンスを実現するた

めに Splunk Enterprise を最適化する 検索タイプが Splunk Enterprise のパフォーマンスに与える影響

最新問題: **49**
ES コンテンツがエクスポートされると、拡張子 .spl を持つ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場合のベスト プラクティスは何ですか?
A. エクスポートごとに常に既存のコンテンツと新しいコンテンツを含めます。
B. 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ます。
C. コンテンツがエクスポートされるたびに、新しいアプリ名を使用します。
D. エクスポートに名前を付けるときに .spl 拡張子を使用しないでください。
Answer: C (メーッセージを残す)

最新問題: **50**
ES データモデルを高速化するためのデフォルトのスケジュールは何ですか?
A. 15 分
B. 1 分
C. 1 時間
D. 5 分
Answer: D (メーッセージを残す)

最新問題: **51**
ガラス テーブルには、静止画像とテキスト、アドホック検索の結果、および次のオブジェクトのうちどれを表示できますか?
A. ルックアップ検索。
B. 要約されたデータ。
C. セキュリティ指標。
D. メトリクス ストアの検索。
Answer: C (メーッセージを残す)

最新問題: **52**
ブルート フォース アクセス動作が検出された相関検索が有効になっており、多くの誤検知が発生しています。入力データはすでに検証されていると仮定します。相関検索の感度を下げるにはどうすればよいでしょうか?
A. 検索を編集し、注目すべきイベントのステータス フィールドを変更して、注目すべきイベントの緊急性を低くします。
B. 検索を編集し、where または xswhere ステートメントを探し、しきい値と比較して一致を少なくします。

C. 検索を編集し、where または xswhere ステートメントを探し、より一般的な一致となるように比較されるしきい値を変更します。
D. この相関検索の緊急度テーブルを変更し、新しい重大度レベルを追加して、この検索からの注目すべきイベントの緊急性を低くします。
Answer: (解答を表示する**)**
参照：
https://docs.splunk.com/Documentation/ES/6.1.0/User/Howurgencyisassigned

最新問題**: 53**
ES をインストールする前に、次のアクションのうちどれが必要ですか?
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. インデクサーを追加します。
D. フォワーダーを追加します。
Answer: A (メーッセージを残す**)**
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なアクションの 1 つは、分散検索接続をリダイレクトすることです。このアクションは、サーチ ヘッド クラスターやサーチ ヘッド プールなどの分散検索環境にすでに接続されているサーチ ヘッドに ES をインストールする場合に必要です。分散検索接続を既存のサーチ ヘッドから ES を実行する新しいサーチ ヘッドにリダイレクトする必要があります。これは、ES には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が必要であるためです。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。
ES をインストールする前に他のアクションは必要ありませんが、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、ディスク領域が解放され、古いデータが削除されますが、ES をインストールする前に行う必要はありません。詳細については、「KV ストアのパージ」を参照してください。インデクサーを追加すると、ES のインデックス作成および検索能力が向上しますが、ES をインストールする前に追加する必要はありません。詳細については、「展開計画」を参照してください。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が向上しますが、ES をインストールする前は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 ストアの展開計画のパージ データを Splunk Enterprise Security に転送します。

最新問題**: 54**

ネットワーク アクティビティ全体で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観察するには、Enterprise Security の次のダッシュボードのどれに最も関連性の高いデータが含まれますか?
A. 侵入センター
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
セクション: (なし)
説明
Answer: A (メッセージを残す**)**
参照：
https://docs.splunk.com/Documentation/ES/6.1.0/User/NetworkProtectionDomaindashboards

最新問題**: 55**
現在有効になっている ES 相関検索のリスト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] [有効] を選択します。
B. [設定] -> [検索、レポート、およびアラート] -> [相関] の名前でフィルターします。
C. [設定] -> [コンテンツ管理] -> タイプ 「相関」およびステータス 「有効」を選択します。
D. 設定 -> 検索、レポート、およびアラート -> 「SplunkEnterpriseSecuritySuite」のアプリを選択し、「ルール」でフィルターします。
Answer: A (メッセージを残す**)**
参照：
https://docs.splunk.com/Documentation/ES/6.1.0/Admin/Listcorrelationsearches

最新問題**: 56**
誰が調査を削除できますか?
A. ess_admin ユーザーのみ。
B. 調査の所有者と協力者。
C. 調査所有者のみ。
D. 調査の所有者および ess 管理者。
Answer: (解答を表示する**)**

最新問題**: 57**
非クラウド (オンプレミス) ES 導入の場合、インデクサーごとの 1 日あたりのインデックス作成の最大推奨量はどれくらいですか?
A. 50 GB
B. 100 GB
C. 300 GB
D. 500 MB
Answer: B (メッセージを残す**)**

説明
Splunk リファレンス アーキテクチャのドキュメント 1 によると、ES の場合、Splunk はインデクサーごとに 1 日あたり 80 ～ 100 GB の取り込みに基づいてサイジングを推奨しています。つまり、毎日 2 TB の取り込みを行う ES 展開には、最大で
20 のインデクサー。この推奨事項は、非クラウド (オンプレミス) ES 展開を対象としています。クラウドベースの ES 展開の場合、インデクサーごとに 1 日あたり推奨されるインデックス作成量は 50 GB2 です。他のオプションである 300 GB と 500 MB は、Splunk では ES 導入には推奨されません。参考文献 = Splunk リファレンス アーキテクチャ Splunk Enterprise Security のパフォーマンス リファレンス

最新問題: **58**
新しいイベントのインデックス作成時に相関検索が実行されることを示す設定はどれですか?
A. 常時オン
B. リアルタイム
C. スケジュール済み
D. 連続
Answer: (解答を表示する**)**
説明/参照:
https://docs.splunk.com/Documentation/ES/6.1.0/Admin/Configurecorrelationsearches

最新問題: **59**
調査の添付ファイルはどこに保存されますか?
A. KV ストア
B. 注目すべきインデックス
C. attachments.csv ルックアップ
D. <splunk_home>/etc/apps/SA-Investigations/default/ui/views/attachments
Answer: A (メッセージを残す**)**
説明/参照: https://docs.splunk.com/Documentation/ES/6.1.0/Admin/Manageinvestigations

最新問題: **60**
管理者は ES アプリを通じて新しいルックアップをどのように追加する必要がありますか?
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ます。
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] -> [新しいコンテンツの作成] -> [管理されたルックアップ] 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。
Answer: D (メッセージを残す**)**

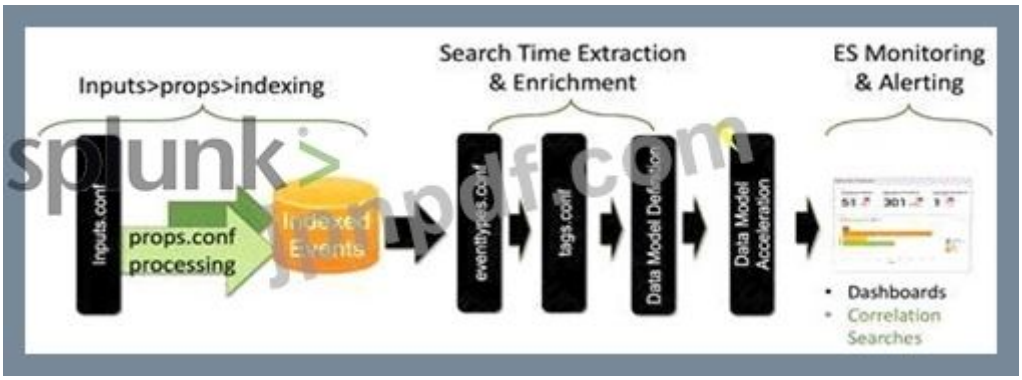
参照：
https://docs.splunk.com/Documentation/ES/6.1.0/Admin/Createlookups

最新問題: **61**
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は何ですか?
A. [設定] -> [インシデント管理] -> [重要なイベント ステータス]
B. [設定] -> [コンテンツ管理] -> [タイプ]: 相関検索
C. 構成 -> 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
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]
Answer: C (メーッセージを残す)
説明/参照: https://docs.splunk.com/Documentation/ES/6.1.0/Admin/Customizenotables

最新問題: **62**
ES の実装時に役立つシナリオはどの機能に含まれていますか?
A. 相関検索
B. 適応応答
C. ユースケース ライブラリ
D. 予測分析
Answer: A (メーッセージを残す)

最新問題: **63**
イベントを正規化するコンポーネントはどれですか?
A. SA-CIM。
B. SA-注目に値します。
C. ES アプリケーション。
D. テクノロジー アドオン。
Answer: (解答を表示する)
説明
テクノロジー アドオン (TA) は、特定のデータ ソースまたはベンダーからデータを取り込み、正規化するための設定を含む Splunk アプリです。TA には、ソースタイプの定義、イン

デックス時および検索時のフィールド抽出、イベント タイプ、タグ、ルックアップ、およびデータを Splunk Common Information Model (CIM) にマッピングするのに役立つその他の設定を含めることができます。CIM は、さまざまなデータ ソース間でデータ フィールドを編成し、名前を付けるための共通の標準を提供する、事前定義されたデータ モデルのセットです。Splunk Enterprise Security は CIM を使用して、セキュリティ イベントのクロスソース分析と相関付けを可能にします。したがって、正解は D です。
テクノロジーのアドオン。参考文献
テクノロジーアドオンの概要
Splunk 共通情報モデル アドオン
テクノロジーアドオンを使用したエンタープライズセキュリティデータの正規化
Splunk Enterprise Security へのデータのオンボーディング



最新問題: **64**
脅威生成検索では何が生成されますか?
A. KV ストア コレクション内のインテルの脅威。
B. 脅威相関検索。
C. 注目すべきインデックス内の注目すべき脅威。
D. threat_activity インデックス内のイベント。
Answer: (解答を表示する)
説明
https://docs.splunk.com/Documentation/ES/6.4.1/Admin/Createthreatmatchspecs

最新問題: **65**
アドオン ビルダーは、何で始まる Splunk アプリを作成しますか?
A. アプリ-
B. TA-
C. だ-
D. SA-
Answer: (解答を表示する)

最新問題: **66**
ID に関する詳細情報はどこに保存されますか?

A. Identity Investigator インデックス。
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 インデックス。
D. ID ルックアップ CSV ファイル。
Answer: D (メーッセージを残す)
説明
ユーザー名、電子メール アドレス、電話番号、ロールなどのアイデンティティに関する詳細情報は、Splunk Enterprise Security のアイデンティティ ルックアップ CSV ファイルに保存されます。ID ルックアップ CSV ファイルは、Active Directory、LDAP、カスタム ID リストなどのさまざまなデータ 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。ID ルックアップ CSV ファイルは、ID 情報でイベントを強化し、ID 相関検索に基づいて注目すべきイベントを生成するために使用されます。Splunk Enterprise Security の [資産とアイデンティティ管理] ページを使用して、アイデンティティ ルックアップ CSV ファイルを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
ID ルックアップ CSV ファイル

最新問題**: 67**
ES インストール プロセスのどの時点で Splunk_TA_ForIndexes.splbe をインデクサーにデプロイする必要がありますか?
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.splis が最初にインストールされます。
C. サーチ 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 applycluster-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。
Answer: (解答を表示する)
説明/参照: https://docs.splunk.com/Documentation/ES/6.1.0/Install/InstallTechnologyAdd-ons

最新問題**: 68**
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. Therat Intelligence の施行
Answer: (解答を表示する)
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通常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 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 ファイル内に " という名前のスタンザを作成するだけです。脅威リスト」。

最新問題: **69**
ユーザー名が ID リストの「ID」列と一致しない場合、次にどの列がチェックされますか?
A. 電子メール。
B. ニックネーム
C. IP アドレス。
D. 姓と名の組み合わせ。
Answer: A (メーッセージを残す**)**
説明
ユーザー名が ID リストの「ID」列と一致しない場合、Splunk Enterprise Security は次は「メール」列です。「電子メール」列には、ID に関連付けられた電子メール アドレスが含まれます。電子メールアドレスがユーザー名と一致する場合、Splunk Enterprise Security はユーザーに ID を割り当てます。電子メールアドレスが一致しない場合、Splunk Enterprise Security は次に「nickname」列をチェックし、次に「ip」列、最後に「last_name」列と「first_name」列をチェックします。列の順序は、identity_manager.conf ファイルの identity_match設定によって決まります。参照 = ID 相関identity_manager.conf

最新問題: **70**
注目すべきイベントの緊急性はどのように計算されますか?
A. 資産の優先順位と脅威の重み。
B. 相関検索によって見つかったアラートの重大度。
C. 相関検索によって見つかった資産またはアイデンティティのリスクと重大度。
D. 相関検索によって設定された重大度、および関連する資産または ID に割り当てられた優先度。
Answer: (解答を表示する**)**
参照：
https://docs.splunk.com/Documentation/ES/6.1.0/User/Howurgencyisassigned

最新問題: **71**
次の手順のどれを実行すると、脅威アクティビティ ダッシュボードが ES のデフォルトのランディング ページになりますか?
A. [ナビゲーションの編集] ページから、[脅威アクティビティ] ビューをページの上部にドラッグ アンド ドロップします。
B. ユーザーの [設定] メニューから、デフォルトのアプリケーションとして Enterprise Security を選択します。

C. [ナビゲーションの編集] ページで、脅威アクティビティの [これをデフォルト ビューとして設定する] チェックマークをクリックします。
D. [脅威アクティビティ] ビュー設定を編集し、[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。
Answer: C (メーッセージを残す**)**
説明
Splunk Enterprise Security のドキュメントによると、脅威アクティビティ ダッシュボードを ES のデフォルトのランディング ページにするには、ナビゲーションの編集ページを使用して、脅威アクティビティの [デフォルト ビューとして設定する] チェックマークをクリックします。[ナビゲーションの編集] ページでは、ES のメニュー バーをカスタマイズし、カスタム ダッシュボード、レポート、またはその他のビューへのリンクを追加できます。各アプリ コンテキストのデフォルト ビューを設定することもできます。これにより、アプリを開いたときのランディング ページが決まります。脅威アクティビティ ダッシュボードをデフォルト ビューとして設定するには、次の手順を実行する必要があります。
Enterprise Security メニュー バーで、[構成] > [一般] > [ナビゲーション] を選択します。
[ナビゲーションの編集] ページで、ドロップダウン メニューから Enterprise Security アプリ コンテキストを選択します。
「ナビゲーション XML」セクションで、ビュー名「threat_activity」を含む行を見つけます。
属性default="true"を行に追加し、同じアプリコンテキスト内の他の行から同じ属性を削除します。
「変更を保存」をクリックして、変更を「ナビゲーションの編集」ページに適用します。
これにより、Enterprise Security アプリを開いたときのデフォルトのランディング ページが脅威アクティビティ ダッシュボードになります。詳細については、「ナビゲーション バーのカスタマイズ」を参照してください。
他のオプションは、脅威アクティビティ ダッシュボードを ES のデフォルトのランディング ページにするための正しい方法ではありません。「脅威アクティビティ」ビューをページの上部にドラッグ アンド ドロップしても、デフォルトのビューは変更されません。メニュー項目の順序のみが変更されます。Enterprise Security をデフォルトのアプリケーションとして選択すると、アプリ内のデフォルトのビューは変更されず、Splunk にログインしたときに開くアプリのみが変更されます。脅威アクティビティのビュー設定を編集しても、デフォルトのビューは変更されず、ダッシュボードのタイトル、説明、権限、スケジュールのみが変更されます。したがって、正解は C です。「ナビゲーションの編集」ページで、「脅威アクティビティ」の「これをデフォルトのビューとして設定する」チェックマークをクリックします。参考 = ナビゲーション バーをカスタマイズします。

最新問題**: 72**
注目すべきイベントの短縮 ID を作成するオプションはどこにありますか?
A. 寄与するイベント。
B. イベントの詳細。

C. 追加フィールド。
D. 説明。
Answer: B (メーッセージを残す**)**
https://docs.splunk.com/Documentation/ES/6.4.1/User/Takeactiononanotableevent

最新問題**: 73**
コンテンツ管理ページを使用して ES から何をエクスポートできますか?
A. 相関検索、マネージド ルックアップ、およびガラス 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リストされている任意のコンテンツ タイプ。
D. 相関検索、ガラス テーブル、およびワークベンチ パネルのみ。
Answer: (解答を表示する**)**
説明
Splunk Enterprise Security のコンテンツ管理ページでは、ページにリストされているあらゆるコンテンツ タイプをアプリとしてエクスポートできます。コンテンツ タイプには、相関検索、ガラス テーブル、ダッシュボード、レポート、保存された検索、キー インジケーター、ワークベンチ パネル、および管理されたルックアップが含まれます。エクスポート オプションを使用すると、カスタマイズされた検索を開発環境またはテスト環境から運用環境に移行するなど、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。[コンテンツ管理] ページを使用して、他の ES インスタンスまたは Splunkbase からコンテンツをインポートすることもできます。参考 = Splunk Enterprise Security からコンテンツをアプリとしてエクスポートする コンテンツを Splunk Enterprise Security にアプリとしてインポートする

最新問題**: 74**
ブルート フォース アクセス動作が検出された相関検索が有効になっており、多くの誤検知が発生しています。入力データはすでに検証されていると仮定します。相関検索の感度を下げるにはどうすればよいでしょうか?
A. 検索を編集し、注目すべきイベントのステータス フィールドを変更して、注目すべきイベントの緊急性を低くします。
B. 検索を編集し、where または xswhere ステートメントを探し、しきい値と比較して一致を少なくします。
C. 検索を編集し、where または xswhere ステートメントを探し、より一般的な一致となるように比較されるしきい値を変更します。
D. この相関検索の緊急度テーブルを変更し、新しい重大度レベルを追加して、この検索からの注目すべきイベントの緊急性を低くします。
Answer: B (メーッセージを残す**)**
説明
失敗したログインの数がしきい値以上の場合、検索によって注目すべきイベントがトリガーされます。

検索の感度を低くするには、しきい値を大きくして、より頻繁に失敗したログインのみが注目すべきイベントをトリガーするようにすることができます。たとえば、デフォルトのしきい値は 4 です。これは、1 分間に 4 回以上ログインが失敗すると、重要なイベントがトリガーされることを意味します。しきい値を 10 に変更すると、1 分間に 10 回以上失敗したログインのみが重要なイベントをトリガーします。参照 = Splunk Enterprise Security 管理者マニュアル ブルート フォース アクセス動作の検出

最新問題: **75**
新しい ES インストールの相関検索の調整の一部は次のうちどれですか?
A. 相関適応応答を構成します。
B. 相関結果のストレージを構成します。
C. 相関権限を構成しています。
D. 相関関係の注目すべきイベントのインデックスを設定します。
Answer: D (メーッセージを残す**)**

最新問題: **76**
カスタム相関検索を作成する場合、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. $フィールド名$
B. "フィールド名"
C. %フィールド名%
D. _フィールド名_
Answer: C (メーッセージを残す**)**
参照：
https://docs.splunk.com/Documentation/ITSI/4.4.2/Configure/Createcorrelationsearch

最新問題: **77**
summariesonly=true オプションは相関検索に対して何をしますか?
A. 高速化されたデータのみを検索します。
B. サマリー インデックスをインデックス層に転送します。
C. デフォルトの要約時間範囲を使用します。

D. サマリー インデックスのみを検索します。
Answer: A (メーッセージを残す**)**
説明/参照: https://community.splunk.com/t5/Splunk-Enterprise-Security/Why-do-correlation-searches-in-Enterprise-Security-not-use-quot/mp/262622

最新問題**: 78**
適応応答アクション履歴はどのインデックスに保存されますか?
A. cim_modactions
B. modular_history
C. cim_adaptiveactions
D. modular_action_history
Answer: A (メーッセージを残す**)**
参照：
https://docs.splunk.com/Documentation/ES/6.1.0/Install/Indexes

最新問題**: 79**
新しく構築されたカスタム ダッシュボードは、ES のセキュリティ アナリストのチームが利用できる必要があります。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すか?
A. ES ホーム ページのリンクを新しいダッシュボードに追加します。
B. es_analyst から継承された新しいロールを作成し、ダッシュボード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。
C. es_analysts によるアクセスを許可するようにダッシュボードの権限を設定し、ナビゲーション エディターを使用してメニューに追加します。
D. 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。
Answer: C (メーッセージを残す**)**
説明
Splunk Enterprise Security のドキュメントによると、新しく構築されたカスタム ダッシュボードを ES のセキュリティ アナリストのチームに統合する最良の方法は、es_analysts によるアクセスを許可するようにダッシュボードの権限を設定し、ナビゲーション エディターを使用してメニューに追加することです。これにより、ES のセキュリティ アナリストのデフォルトのロールである es_analyst ロールを持つユーザーがダッシュボードを表示し、アクセスできるようになります。ナビゲーション エディターを使用すると、ES のメニュー バーをカスタマイズし、カスタム ダッシュボード、レポート、またはその他のビューへのリンクを追加できます。詳細については、「ユースケースに合わせて Splunk Enterprise Security ダッシュボードをカスタマイズする」および「ナビゲーション バーをカスタマイズする」を参照してください。
他のオプションは、ダッシュボードが適切に統合されないか、不必要な複雑さが生じるため、推奨されません。ES ホームページのリンクを新しいダッシュボードに追加することは、ダッシュボードがメニュー バーに統合されず、ホームページが乱雑になる可能性があるた

め、良い選択肢ではありません。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することは、冗長なロールが作成され、デフォルトのビューとしての Security Posture ダッシュボード。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 にインストールすることは、別個のアプリの作成と維持が必要であり、ES との競合やパフォーマンスの問題が発生する可能性があるため、良い選択肢ではありません。したがって、正解は C です。es_analysts によるアクセスを許可するようにダッシュボードの権限を設定し、ナビゲーション エディターを使用してメニューに追加します。参考 = ナビゲーション バーをカスタマイズする Splunk Enterprise Security コンテンツ管理の役割と機能 ユースケースに合わせて Splunk Enterprise Security ダッシュボードをカスタマイズする カスタム ダッシュボードと Achi へのアラートを作成する方法 - Splunk Community

最新問題: **80**
注目すべきイベントの短縮 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. 寄与するイベント。
D. 説明。
Answer: B (メーッセージを残す**)**
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短縮 ID を作成するオプションは、注目すべきイベントの [イベントの詳細] セクションにあります。「イベントの詳細」セクションには、タイトル、説明、緊急度、所有者、ステータスなど、注目すべきイベントに関する基本情報が表示されます。また、注目すべきイベントを識別して共有するために使用できる 6 桁の英数字コードを生成するショート ID の作成へのリンクも提供されます。短縮 ID はインシデント レビュー ダッシュボードの URL に追加され、短縮 ID フィールドで注目すべきイベントをフィルターするために使用できます。詳細については、Splunk

Enterprise Security で注目すべきイベントを手動で作成する」を参照してください。したがって、正解は B. イベントの詳細です。参考文献
= Splunk Enterprise Security で注目すべきイベントを手動で作成します。

最新問題: **81**
ES は、次のどのオプションを使用してサーチヘッドにインストールする必要がありますか?
A. 他のアプリはありません。
B. TA-* を除くすべてのアプリが削除されました。
C. デフォルトの組み込みアプリと CIM 準拠アプリのみ。
D. インストールされている他のアプリ。
Answer: C (メーッセージを残す)

最新問題: **82**
Web Intelligence ダッシュボードは次のうちどれですか?
A. ストリーム :http プロトコル ダッシュボード
B. エンドポイント センター
C. ネットワーク センター
D. HTTP カテゴリ分析
Answer: D (メーッセージを残す)

最新問題: **83**
注目すべきイベントの緊急性を高めるために、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いますか?
A. VIP
B. 優先度
C. 重要性
D. 重大度
Answer: B (メーッセージを残す)
説明
アセットまたは ID リストの優先度列はイベントの重大度と組み合わされて、Splunk Enterprise Security での注目すべきイベントの緊急度が決まります。緊急度は、注目すべきイベントに対処することがどの程度重要かを示す尺度であり、イベントに関係する資産またはアイデンティティの優先順位とイベントの重大度をマッピングするマトリックスに基づいて計算されます。緊急度は、低、中、高、クリティカルのいずれかの値になります12。たとえば、デフォルトでは、中、高、およびクリティカルの優先度をクリティカル重大度と組み合わせると、クリティカル緊急度ランキングが生成されます3。参照 = 1: インシデントのレビュー - Splunk ドキュメント - 緊急性。2:
重要なイベントの緊急性を設定する - Splunk のドキュメント。3: 解決済み: Splunk Enterprise Security: 強制する方法はありますか? - Splunk コミュニティ。

最新問題: **84**
ES がダウンロードできる脅威インテリジェンスのタイプは次のうちどれですか? (該当するものをすべて選択してください)
A. テキスト
B. STIX/TAXII
C. VulnScanSPL
D. Splunk Enterprise Threat Generator
Answer: B (メーッセージを残す**)**
説明
Splunk Enterprise Security は、STIX/TAXII サーバーからの脅威インテリジェンスのダウンロードをサポートしています。STIX はサイバー脅威情報を記述するための構造化言語であり、TAXII は STIX データを交換するためのプロトコルです。Splunk Enterprise Security は、TAXII をサポートする任意のサーバーから STIX/TAXII フィードをダウンロードできます
1.1 仕様と STIX 1.1.1 または 1.2 仕様。Splunk Enterprise Security は、テキスト、VulnScanSPL、または Splunk Enterprise Threat Generator ソースからの脅威インテリジェンスのダウンロードをサポートしていません。
参考 = Splunk Enterprise Security への脅威インテリジェンスの追加、STIX または OpenIOC 構造化脅威インテリジェンス ファイルのアップロード

最新問題: **85**
ES アセットの例は何ですか?
A. サーバー
B. MAC アドレス
C. 人
D. ユーザー名
Answer: B (メーッセージを残す**)**

最新問題: **86**
管理者は、アナリストがインシデント レビュー ダッシュボードで作業しているときに、注目すべきイベントのアクション メニューに選択可能なオプションとして表示されるように、「Nslookup」適応応答アクションを構成するように求められます。管理者はこのオプションを構成するためにどのような手順を実行しますか?
A. 構成 -> コンテンツ管理 -> タイプ: 相関検索 -> 注目 -> Nslookup
B. 構成 -> タイプ: 相関検索 -> 注目 -> 推奨アクション -> Nslookup
C. 構成 -> コンテンツ管理 -> タイプ: 相関検索 -> 注目 -> 次のステップ -> Nslookup
D. 設定 -> コンテンツ管理 -> タイプ: 相関検索 -> 注目 -> 推奨アクション -> Nslookup
Answer: (解答を表示する**)**
説明

「Nslookup」適応応答アクションを構成して、アナリストがインシデント レビュー ダッシュボードで作業しているときに、注目すべきイベントのアクション メニューに選択可能なオプションとして表示されるようにするには、管理者は次の手順を実行します。
Splunk Enterprise Security メニュー バーで、[設定] > [コンテンツ] > [コンテンツ管理] をクリックします。
「タイプ: 相関検索」でコンテンツをフィルターし、Nslookup アクションを追加する相関検索を選択します。
「編集」をクリックして「注目」タブに移動します。
[推奨されるアクション] で、[新しいアクションの追加] をクリックし、ドロップダウン メニューから [Nslookup] を選択します。
Nslookup アクションに必要なフィールド (ホスト フィールド、DNS サーバー、出力インデックスなど) を入力します。
「保存」をクリックして、相関検索への変更を保存します。
Nslookup アクションは、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のアクション メニューにオプションとして表示されます。参考 = Splunk Enterprise Security でのアダプティブ レスポンス アクションのセットアップ Splunk Enterprise Security に含まれるアダプティブ レスポンス アクション

最新問題**: 87**
Splunk Enterprise Security が機能するために設定する必要があるデフォルトのポートは次のうちどれですか?
A. SplunkWeb (8068)、Splunk Management (8089)、KV ストア (8000)
B. SplunkWeb (8390)、Splunk Management (8323)、KV ストア (8672)
C. SplunkWeb (8000)、Splunk Management (8089)、KV ストア (8191)
D. SplunkWeb (8043)、Splunk Management (8088)、KV ストア (8191)
Answer: (解答を表示する**)**
説明
https://docs.splunk.com/Documentation/Splunk/8.1.2/Security/SecureSplunkonyournetwork

最新問題**: 88**
Enterprise Security のダッシュボードは主にどの種類のナレッジ オブジェクトからデータを取得しますか?
A. 統計情報
B. KV ストア
C. データモデル
D. 動的検索
Answer: C (メーッセージを残す**)**
説明

データ モデルは、エンタープライズ セキュリティ ダッシュボードの主要なデータ ソースです。データ モデルは、インデックスからデータを定義し、取得するための構造化された一貫した方法を提供します。データ モデルは、事前に構築されたデータの概要を使用することで検索を高速化します。データ モデルでは、データ モデルの概要に対して統計分析を実行できる tstats コマンドの使用も可能になります。データ モデルは Common Information Model (CIM) にマッピングされ、ドメインやテクノロジー全体でデータを記述するための共通言語を提供します。参考 = データ モデルについて Splunk Web で共通情報モデルを使用する

最新問題: **89**
ES サーチヘッドはどこに設置すればよいですか?
A. Splunk DB Connect を実行している Splunk サーバー上。
B. トップレベルの可視性を持つ Splunk サーバー上。
C. 任意の Splunk サーバー上。
D. Splunk が新規にインストールされたサーバー上。
Answer: C (メーッセージを残す**)**

最新問題: **90**
ES グラフィカル ナビゲーション バー エディターに移動するにはどうすればよいですか?
A. 設定 -> ユーザー インターフェース -> ナビゲーション メニュー -> SplunkEnterpriseSecuritySuite の横にある 「デフォルト」をクリックします
B. [設定] -> [ユーザー インターフェイス] -> [ナビゲーション] -> [エンタープライズ セキュリティ] をクリックします。
C. [設定] -> ナビゲーション メニュー
D. [設定] -> [一般] -> [ナビゲーション]
Answer: D (メーッセージを残す**)**

最新問題: **91**
デフォルト アカウント アクティビティの検出相関検索では、既知のデフォルト アカウントにフラグを立てるためにどのルックアップ テーブルが使用されますか?
A. ローカル ユーザー Intel
B. 管理者 ID
C. ID
D. 特権アカウント
Answer: C (メーッセージを残す**)**

最新問題: **92**
ES インストール プロセスのどの時点で Splunk_TA_ForIndexes.spl をインデクサーにデプロイする必要がありますか?
A. Splunk_TA_ForIndexers.spl が最初にインストールされます。
B. Splunk_TA_ForIndexers.spl は、クラスターマスターおよび splunk applycluster-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。
C. デプロイメントサーバーにアプリを追加するとき。
D. サーチ 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。
Answer: D (メーッセージを残す)

最新問題: **93**
データを高速化するには、1 日当たりのデータ量の年間約何倍の追加ストレージ スペースが必要ですか?
A. 2.5
B. 1.0
C. 5.7
D. 3.4
Answer: D (メーッセージを残す)

最新問題: **94**
サイトには、CIM と非 CIM 準拠のアプリケーションの両方をホストする単一の既存の検索ヘッドがあります。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、優れた ES パフォーマンスも求めています。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すか?
A. ES を既存のサーチヘッドにインストールします。
B. 新しいサーチヘッドを追加し、そこに ES をインストールします。
C. サーチヘッドの CPU 数とメモリ量を増やしてから、ES をインストールします。
D. CIM 非準拠のアプリを検索ヘッドから削除してから、ES をインストールします。
Answer: B (メーッセージを残す)
説明/参照: https://www.splunk.com/pdfs/technical-briefs/splunk-validated-architectures.pdf

最新問題: **95**
アドオン ビルダーが新しいアドオンで構成できる機能は次のうちどれですか?
A. データを期限切れにします。
B. データを正規化します。
C. データを要約します。

D. データを変換します。
Answer: B (メーッセージを残す**)**
説明/参照: https://docs.splunk.com/Documentation/AddonBuilder/3.0.1/UserGuide/Overview

最新問題**: 96**
イベント内のアセットを識別するためにアセット ルックアップのどの列が使用されますか?
A. 送信元、DVC、宛先
B. cidr、ポート、netbios、saml
C. ip、mac、dns、nt_host
D. ホスト、ホスト名、URL、アドレス
Answer: C (メーッセージを残す**)**
説明/参照: https://docs.splunk.com/Documentation/ES/6.4.1/Admin/Formatassetoridentitylist

最新問題**: 97**
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は何ですか?
A. 設定 -> コンテンツ管理 -> タイプ: 相関検索
B. [設定] -> [インシデント管理] -> [重要なイベント ステータス]
C. 構成 -> 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
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]
Answer: D (メーッセージを残す**)**

最新問題**: 98**
分散構成管理の自動展開機能を使用して Indexes.conf を配布する場合のリスクは次のうちどれですか?
A. インデックスがクラッシュする可能性があります。
B. インデックスが処理中の可能性があります。
C. インデックスに到達できない可能性があります。
D. インデックスの設定が異なります。
Answer: D (メーッセージを残す**)**
説明
Distributed Configuration Management の自動導入機能は、indexes.conf などの設定ファイルを Splunk プラットフォーム インスタンスに自動的に配布できるツールです。ただし、この機能を使用してindexes.confを配布すると、インスタンス間で異なる設定のインデックスが存在するリスクが生じる可能性があります。これは、一部のインスタンスで Indexes.conf ファイルを手動で編集した場合、または異なるインスタンスに異なるバージョンの Splunk Enterprise Security がインストールされている場合に発生する可能性があります。インデックスの設定 (保存ポリシー、ストレージ パス、バケット サイズなど) が異なる場合、データの不整合、検索の非効率、またはデータ損失が発生する可能性があります。したがって、インスタンスにデプロイする前に、Distributed Configuration Management の手動デプロイ機能を

使用して、indexes.conf ファイルを確認および検証することをお勧めします12。参照 = 1: 分散構成管理 - Splunk ドキュメント - 自動導入。2: 分散構成管理 - Splunk ドキュメント - 手動導入。

最新問題: **99**
ES コンテンツがエクスポートされると、拡張子 .spl を持つ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場合のベスト プラクティスは何ですか?
A. コンテンツがエクスポートされるたびに、新しいアプリ名を使用します。
B. エクスポートに名前を付けるときに .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ます。
D. エクスポートごとに常に既存のコンテンツと新しいコンテンツを含めます。
Answer: C (メーッセージを残す**)**
毎回新しいアプリ名を使用するか (管理が難しい場合があります)、エクスポートするたびに常にすべてのコンテンツ (新旧) を含めるようにしてください。

最新問題: **100**
ES がダウンロードできる脅威インテリジェンスのタイプは次のうちどれですか? (該当するものをすべて選択してください)
A. テキスト
B. SplunkEnterpriseThreatGenerator
C. STIX/TAXII
D. VulnScanSPL
Answer: A,C (メーッセージを残す**)**

最新問題: **101**
新しいイベントのインデックス作成時に相関検索が実行されることを示す設定はどれですか?
A. スケジュール済み
B. 常時オン
C. 連続
D. リアルタイム
Answer: A (メーッセージを残す**)**

最新問題: **102**
アナリストは、ネットワーク トラフィック データを取得して分析する機能を要求しました。管理者はドキュメントを調査し、この調査に基づいて Splunk App for Stream を ES と統合することを決定しました。

アナリストがネットワーク ストリーム データを表示および分析できるようにするために、どのダッシュボードがサポートされるようになりますか?
A. エンドポイント ダッシュボード。
B. ユーザー インテリジェンス ダッシュボード。
C. プロトコル インテリジェンス ダッシュボード。
D. Web Intelligence ダッシュボード。
Answer: C (メーッセージを残す**)**
説明
Splunk Enterprise Security のドキュメントによると、プロトコル インテリジェンス ダッシュボードは、ネットワーク ストリーム データの表示および分析機能をサポートするダッシュボードです。プロトコル インテリジェンス ダッシュボードには、TCP、UDP、ICMP などのプロトコルごとのネットワーク トラフィックの概要が表示されます。また、各プロトコルの上位の送信元、宛先、ポート、およびアプリケーションも表示されます。ダッシュボードを使用すると、時間範囲、プロトコル、送信元、宛先、ポート、アプリケーションごとにデータをフィルタリングできます。ダッシュボードには、さらに分析するための、ネットワーク解決ダッシュボードやトラフィック サイズ分析ダッシュボードなどの他のダッシュボードへのドリルダウン リンクも提供されます。Protocol Intelligence ダッシュボードでは、ネットワーク トラフィック データをキャプチャして解析するために、Splunk App for Stream と Splunk Add-on for Stream が必要です。したがって、正解はCです。
プロトコル インテリジェンス ダッシュボード。参考 = プロトコル インテリジェンス ダッシュボード。
Splunk 用 Anomali ThreatStream アプリ | Splunkbase


最新問題: **103**
ES のインストール後、管理者は Leers に ss_uso r ロールを設定し、注目すべきイベントを閉じる機能を設定しました。管理者は、これらのユーザーが 解決済み」の重要な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. [ステータス設定] ウィンドウから、クローズ済み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_use r を削除します。
C. Enterprise Security で、ess_user ロールに独自の重要なイベント権限を与えます。
D. Splunk Access Controls から、ess_user ロールを選択し、edit_notabie_events 機能を削除します。
Answer: (解答を表示する**)**
説明
Splunk Enterprise Security のドキュメントによると、[ステータス設定] ウィンドウでは、重要なイベントのステータス値と遷移をカスタマイズできます。どのロールが重要なイベントのステータスをある値から別の値に変更できるか、またどのロールが特定のステータスの重要なイベントを表示できるかを定義できます。ess_user ロールを持つユーザーが 解決済みの重要なイベント」のステータスを クローズ済み」に変更できないように制限するには、次の手順を実行する必要があります。
Enterprise Security メニュー バーで、[構成] > [インシデント管理] > [ステータス構成] を選択します。
 ステータス構成」ウィンドウで、値のリストから 解決済み」ステータスを選択します。
 ステータス遷移」セクションで、クローズ済みステータスの行を見つけて、 編集」アイコンをクリックします。
 ステータス遷移の編集」ダイアログ ボックスで、 ロール」フィールドからess_userロールを削除し、 保存」をクリックします。
 変更を保存」をクリックして、変更を ステータス構成」ウィンドウに適用します。
これにより、ess_user ロールを持つユーザーが重要なイベントのステータスを 解決済み」から クローズ済み」に変更できなくなります。許可があれば、他の注目すべきイベントのステータスを終了に変更することもできます。したがって、正解は A です。[ステータス設定] ウィンドウで [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。参照 = 注目すべきイベントのステータス値と遷移をカスタマイズします。

最新問題: **104**
Security Posture ダッシュボードには何が表示されますか?
A. 進行中の調査とそのステータス。
B. 注目すべきイベントの概要。

C. SOC によって追跡されている現在の脅威。
D. セキュリティ ツールのステータスの表示。
Answer: B (メーッセージを残す**)**
Security Posture ダッシュボードは、導入環境のすべてのドメインにわたる注目すべきイベントに関する高度な洞察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

最新問題**: 105**
注目すべきイベントの作成を抑制するためにどの相関検索機能が使用されますか?
A. スケジュールの優先度。
B. ウィンドウ間隔。
C. ウィンドウ期間。
D. スケジュールウィンドウ。
Answer: (解答を表示する**)**
説明/参照:
https://docs.splunk.com/Documentation/ES/6.1.0/Admin/Configurecorrelationsearches

最新問題**: 106**
カスタム相関検索を作成する場合、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. $フィールド名$
B. "フィールド名"
C. %フィールド名%
D. _フィールド名_
Answer: A (メーッセージを残す**)**
説明
カスタム相関検索を作成する場合、フィールド名形式を使用して、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ことができます。これにより、検索結果からの動的な情報を使用して注目すべきイベントをカスタマイズできます。たとえば、src を使用してイベントの送信元 IP アドレスを含めたり、user を使用して event1 のユーザー名を含めたりできます。参照 = 1: 相関検索の作成 - Splunk ドキュメント - 注目すべきイベントを定義します。

最新問題: **107**
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. eventtypes.conf、indexes.conf、tags.conf
C. web.conf、props.conf、transforms.conf
D. indexes.conf、props.conf、transforms.conf
Answer: D (メーッセージを残す**)**

最新問題: **108**
注目すべきイベントの短縮 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. 寄与するイベント。
D. 説明。
Answer: (解答を表示する**)**
説明
https://docs.splunk.com/Documentation/ES/6.4.1/User/Takeactiononanotableevent