Splunk.SPLK-3001.v2022-12-04.q84

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:	84
バージョン:	v2022-12-04
アクセス数:	1570
ページビュー数:	840
https://www.jpnpdf.com/Splunk.SPLK-3001.v2022-12-04.q84-mondaishu.html	

最新問題: **1**
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場合。
B. Splunk_TA_ForIndexers.splisが最初にインストールされました。
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 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: B (メーッセージを残す**)**
説明/リファレンス：
https ://docs.splunk.com/Documentation/ES/6.1.0/Install/InstallTechnologyAdd-ons

最新問題: **2**
新しいイベントにインデックスが付けられると、相関検索が実行されることを示した設定はどれですか？
A. 常時オン
B. リアルタイム
C. 予定
D. 継続
Answer: C (メーッセージを残す**)**
参照：
https://docs.splunk.com/Documentation/ES/6.1.0/Admin/Configurecorrelationsearches

最新問題: **3**
ブルートフォースアクセス動作検出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。入力データが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すか？

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、しきい値を比較した後、一致する頻度を減らします。
C. 検索を編集し、whereまたはxswhereステートメントを探し、比較されるしきい値を変更して、より一般的な一致にします。
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**)**
参照：
https://docs.splunk.com/Documentation/ES/6.1.0/User/Howurgencyisassigned

最新問題**: 4**
アドオンをSplunkEnterpriseSecurity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. Splunk_TA_のプレフィックス
B. TECH_のプレフィックス
C. .splのサフィックス
D. CIM_のプレフィックス
Answer: A (メーッセージを残す**)**

最新問題**: 5**
「推奨アクション」と「適応応答アクション」はどちらも適応応答を使用します。それらはどのように異なりますか？
A. 推奨されるアクションはアナリストにテキストによる説明を示し、適応型応答アクションはそれらがエンコードされていることを示します。
B. 推奨アクションはアナリストへの適応応答のリストを表示します。適応応答アクションはそれらを自動的に実行します。
C. 推奨アクションはすでに実行されたアダプティブレスポンスのリストを表示します。アダプティブレスポンスアクションはそれらを自動的に実行します。
D. 推奨されるアクションはアナリストへの適応応答のリストを示します。適応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。
Answer: D (メーッセージを残す**)**
説明/参照：https ://docs.splunk.com/Documentation/ES/latest/Admin/Configureadaptiveresponse

最新問題**: 6**
ESをインストールする準備をするときの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. 使用するデータソースを特定します。
C. 必要なハードウェアを決定します。
D. インストールのサイズと範囲を決定します。

Answer: D (メーッセージを残す)
説明/参照：

最新問題**: 7**
管理者は、改ざんによってESインデックスデータが危険にさらされないようにする必要があります。この要件を満たす機能はどれですか？
A. インデックスの一貫性。
B. データ整合性制御。
C. インデクサーの確認。
D. インデックスアクセス許可。
Answer: (解答を表示する)
参照：
https://answers.splunk.com/answers/790783/anti-tampering-features-to-protect-splunk-logs-the.html

最新問題**: 8**
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
Answer: (解答を表示する)
説明/リファレンス：
https ://docs.splunk.com/Documentation/ES/6.4.1/Install/InstallTechnologyAdd-ons

最新問題**: 9**
ES用にデフォルトで構成されているアダプティブ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
Answer: D (メーッセージを残す)
説明/参照：

最新問題**: 10**
新しいESインストールで一連の相関検索が有効になり、結果が監視されます。相関検索の1つは、評価されたときに誤検知であると判断される多くの注目すべきイベントを生成することです。この問題の解決策は何ですか？
A. その相関検索からの注目すべきイベントを抑制します。

B. 相関検索のデフォルトのステータスと重大度を変更します。
C. サイトの相関スケジュールと感度を変更します。
D. 相関検索のアクセラレーションを無効にして、ストレージ要件を減らします。
Answer: A (メーッセージを残す**)**

最新問題**: 11**
セキュリティポスチャダッシュボードには何が表示されますか？
A. 活発な調査とその状況。
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**)**
説明
セキュリティポスチャダッシュボードは、展開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レベルの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 $OC）での表示に適しています。このダッシュボード

最新問題**: 12**
注目すべきネットワーク異常を調査する際にセキュリティアナリストが使用するES機能は次のうちどれですか？
A. 相関エディター。
B. キーインジケーター検索。
C. 脅威の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。
Answer: D (メーッセージを残す**)**
説明/参照 :https ://www.splunk.com/en_us/products/premium-solutions/splunk-enterprise-security/features.html

最新問題**: 13**
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. インデクサーを追加します。
C. KVストアを削除します。
D. フォワーダーを追加します。
Answer: B (メーッセージを残す**)**

最新問題**: 14**
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. デプロイメントサーバーにアプリを追加する場合。

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splunkapplycluster-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**)**
参照：
https://docs.splunk.com/Documentation/ES/6.1.0/Install/InstallTechnologyAdd-ons

最新問題**: 15**
非クラウド オンプレミス）ESデプロイメントの場合、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ボリュームはどれくらいですか？
A. 50 GB
B. 100 GB
C. 300 GB
D. 500 MB
Answer: (解答を表示する**)**

最新問題**: 16**
ネットワークのアクティビティ全体で使用されているネットワークサービスを観察するには、エンタープライズセキュリティ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
Answer: (解答を表示する**)**
説明

最新問題**: 17**
非標準のフィールド名をCIMフィールド名にマップするには何を使用する必要がありますか？
A. フィールドエイリアス。

B. 検索時間の抽出。
C. タグ。
D. イベントタイプ。
Answer: A (メーッセージを残す**)**
説明

最新問題**: 18**
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、およびRAMの参照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: C (メーッセージを残す**)**
参照：
https://docs.splunk.com/Documentation/Splunk/8.0.2/Capacity/Referencehardware

最新問題**: 19**
ESアプリケーションをアップロードする必要があるのは次のうちどれですか？
A. インデクサー。
B. KVストア。
C. サーチヘッド。
D. 専用フォワーダー。
Answer: C (メーッセージを残す**)**
参照：
https://docs.splunk.com/Documentation/ES/6.1.0/Install/InstallEnterpriseSecuritySHC

最新問題**: 20**
新しいイベントにインデックスが付けられると、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. 予定
D. 継続
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/Configurecorrelationsearches

最新問題**: 21**

ESがダウンロードできる脅威インテリジェンスの種類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. SplunkEnterpriseThreatGenerator
B. VulnScanSPL
C. STIX / TAXII
D. テキスト
Answer: C,D (メーッセージを残す**)**

最新問題**: 22**
ネットワークのアクティビティ全体で使用されているネットワークサービスを観察するには、エンタープライズセキュリティ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. 脅威インテリジェンス
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**: 23**
次のうち、新しいESインストールの相関検索の調整の一部はどれですか？
A. 相関適応応答の構成。
B. 相関結果ストレージの構成。
C. 相関注目イベントインデックスを構成します。
D. 相関権限を構成します。
Answer: (解答を表示する**)**

最新問題**: 24**
管理者は、「Nslookup」適応応答アクションを構成するように求められます。これにより、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->推奨されるアクション
-> Nslookup
B. 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
C. 構成->タイプ：相関検索->注目->推奨されるアクション->Nslookup
D. 構成->コンテンツ管理->タイプ：相関検索->注目->Nslookup
Answer: A (メーッセージを残す**)**

最新問題**: 25**

管理者は、改ざんによってESインデックスデータが危険にさらされないようにする必要があります。
この要件を満たす機能はどれですか？
A. インデックスの一貫性。
B. データ整合性制御。
C. インデクサーの確認。
D. インデックスアクセス許可。
Answer: B (メーッセージを残す**)**
説明/参照 :https ://answers.splunk.com/answers/790783/anti-tampering-features-to-protect-splunk-logs- the.html

最新問題**: 26**
サイトには、CIMと非CIM準拠の両方のアプリケーションを組み合わせて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。お客様は、コストを慎重に管理したいと考えていますが、優れたESパフォーマンスを望んでいます。
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. 既存のサーチヘッドにESをインストールします。
B. 新しいサーチヘッドを追加し、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をインストールしてください。
D. CIMに準拠していない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**: 27**
サイトには、CIMと非CIM準拠の両方のアプリケーションを組み合わせて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。お客様は、コストを慎重に管理したいと考えていますが、優れたESパフォーマンスを望んでいます。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. 新しいサーチヘッドを追加し、ESを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をインストールしてください。
C. 既存のサーチヘッドにESをインストールします。
D. CIMに準拠していない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: A (メーッセージを残す**)**

最新問題**: 28**
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. RESTAPI呼び出し。
B. 調査の最終結果のステータス。

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: (解答を表示する**)**
参照：
https://docs.splunk.com/Documentation/ES/6.1.0/User/EndpointProtectionDomaindashboards

最新問題**: 29**
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のはどこですか？
A. コンテンツエクスポーター
B. 構成->コンテンツ管理
C. コンテンツダッシュボードのエクスポート
D. 設定メニュー->ES->エクスポート
Answer: (解答を表示する**)**
説明
説明/参照 :https ://docs.splunk.com/Documentation/ES/6.1.0/Admin/Export

最新問題**: 30**
管理者は、改ざんによってESインデックスデータが危険にさらされないようにする必要があります。この要件を満たす機能はどれですか？
A. インデクサーの確認。
B. インデックスの一貫性。
C. データ整合性制御。
D. インデックスアクセス許可。
Answer: C (メーッセージを残す**)**

最新問題**: 31**
新しいイベントにインデックスが付けられると、相関検索が実行されることを示した設定はどれですか？
A. 常時オン
B. 予定
C. リアルタイム
D. 継続
Answer: (解答を表示する**)**

最新問題: 32
この写真の赤いボックスにはどのような値がありますか？

Additional Fields	Value
HTTP Method	GET
Source	10.98.27.195 500
Source Expected	false
Source PCI Domain	untrust
Source Requires Antivirus	false
Source Should Time Synchronize	false
Source Should Update	false
Tag	modaction_result

A. IPアドレスの評価。
B. ソースランキング。
C. イベントの優先度。
D. リスクスコア。
Answer: (解答を表示する**)**

最新問題: 33
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ためにどの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. $ fieldname $
D. %fieldname%
Answer: C (メーッセージを残す**)**

最新問題: 34
ネットワークのアクティビティ全体で使用されているネットワークサービスを観察するには、エンタープライズセキュリティ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
Answer: (解答を表示する**)**
説明/参照：
https ://docs.splunk.com/Documentation/ES/6.1.0/User/NetworkProtectionDomaindashboards

最新問題: **35**
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. DA-
B. SA-
C. TA-
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: **36**
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: **37**
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. 構成->コンテンツ管理->タイプ：相関検索
B. 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
C. 構成->インシデント管理->注目すべきイベントステータス
D. 構成->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: **38**
「推奨アクション」と「適応応答アクション」はどちらも適応応答を使用します。それらはどのように異なりますか？
A. 推奨されるアクションはアナリストにテキストによる説明を示し、適応型応答アクションはそれらがエンコードされていることを示します。
B. 推奨アクションはアナリストへの適応応答のリストを表示します。適応応答アクションはそれらを自動的に実行します。
C. 推奨アクションはすでに実行されたアダプティブレスポンスのリストを表示します。アダプティブレスポンスアクションはそれらを自動的に実行します。

D. 推奨されるアクションはアナリストへの適応応答のリストを示します。適応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。
Answer: (解答を表示する**)**
参照：
https://docs.splunk.com/Documentation/ES/latest/Admin/Configureadaptiveresponse

最新問題**: 39**
調査を削除できるのは誰ですか？
A. ess_adminユーザーのみ。
B. 調査の所有者のみ。
C. 調査の所有者およびess-admin。
D. 調査の所有者と協力者。
Answer: (解答を表示する**)**
参照：
https://docs.splunk.com/Documentation/ES/6.1.0/Admin/Manageinvestigations

最新問題**: 40**
エンタープライズセキュリティの次のルックアップタイプのうち、既知の敵対的な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. セキュリティドメイン。
B. 脅威インテリジェンス。
C. アセット。
D. ドメイン。
Answer: B (メーッセージを残す**)**
説明/参照 :https ://docs.splunk.com/Documentation/ES/6.4.1/Admin/Manageinternallookups

最新問題**: 41**
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は、最新の1時間のデータが表示されていません。検索のスキップなどの潜在的なエラーについて、どのデータモデルをチェックする必要がありますか？
A. リスク
B. パフォーマンス
C. 認証
D. Web
Answer: (解答を表示する**)**

最新問題**: 42**
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のはどこですか？
A. コンテンツダッシュボードのエクスポート
B. 設定メニュー->ES->エクスポート

C. コンテンツエクスポーター
D. 構成->コンテンツ管理
Answer: D (メーッセージを残す**)**

最新問題**: 43**
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. web.conf、props.conf、transforms.conf
B. inputs.conf、props.conf、transforms.conf
C. indexes.conf、props.conf、transforms.conf
D. eventtypes.conf、indexes.conf、tags.conf
Answer: C (メーッセージを残す**)**

最新問題**: 44**
非クラウド（オンプレミス）ESデプロイメントの場合、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ボリュームはどれくらいですか？
A. 50 GB
B. 100 GB
C. 300 GB
D. 500 MB
Answer: (解答を表示する**)**
参照：
https://docs.splunk.com/Documentation/ITSI/4.4.2/Install/Plan

最新問題**: 45**
注目すべきイベントの作成を抑制するために使用される相関検索機能はどれですか？
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: C (メーッセージを残す**)**
説明/参照：
https ://docs.splunk.com/Documentation/ES/6.1.0/Admin/Configurecorrelationsearches

最新問題**: 46**
ESで使用されるデータモデル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. Web
B. 異常
C. 認証

D. ネットワークトラフィック
Answer: B (メーッセージを残す**)**
説明/参照：
https ://dev.splunk.com/enterprise/docs/developapps/enterprisesecurity/datamodelsusedbyes/

最新問題: **47**
新しいイベントにインデックスが付けられると、相関検索が実行されることを示した設定はどれですか？
A. 常時オン
B. リアルタイム
C. 予定
D. 継続
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: **48**
ESをサーチヘッドにインストールする必要があります。次のオプションのどれを使用しますか？
A. インストールされている他のアプリ。
B. 他のアプリはありません。
C. デフォルトの組み込みアプリとCIM準拠アプリのみ。
D. TA- *を除くすべてのアプリが削除されました。
Answer: C (メーッセージを残す**)**

最新問題: **49**
セキュリティポスチャダッシュボードには何が表示されますか？
A. 活発な調査とその状況。
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**)**
セキュリティポスチャダッシュボードは、展開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レベルの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 $OC）での表示に適しています。このダッシュボード

最新問題**: 50**
ガラステーブルの主な特徴は次のうちどれですか？
A. 後で取得するための強力なデータ。
B. インタラクティブな調査。
C. 剛性。
D. カスタマイズ。
Answer: D (メーッセージを残す**)**

最新問題**: 51**
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**)**
説明/リファレンス：
https ://docs.splunk.com/Documentation/AddonBuilder/3.0.1/UserGuide/Overview

最新問題**: 52**
ESコンテンツがエクスポートされると、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、常に既存のコンテンツと新しいコンテンツの両方を含めます。
D. エクスポートごとに既存のコンテンツと新しいコンテンツを常に含めます。
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**: 53**
Enterprise Securityのダッシュボードは、主にどのタイプのナレッジオブジェクトからデータを取得しますか？
A. Tstats
B. KVストア
C. データモデル

D. 動的ルックアップ
Answer: C (メーッセージを残す**)**
参照：
https://docs.splunk.com/Splexicon:Knowledgeobject

最新問題**: 54**
注目すべきイベントの緊急度はどのように計算されますか？
A. 資産の優先度と脅威の重み。
B. 相関検索によって検出されたアラートの重大度。
C. 相関検索によって検出された資産またはID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と、関連付けられたアセットまたはIDに割り当てられた優先度。
Answer: D (メーッセージを残す**)**
参照：
https://docs.splunk.com/Documentation/ES/6.1.0/User/Howurgencyisassigned

最新問題**: 55**
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（8000）、Splunk Management（8089）、KVストア（8191）
B. SplunkWeb（8088）、Splunk Management（8089）、KVストア（8000）
C. SplunkWeb（8043）、Splunk Management（8088）、KVストア（8191）
D. SplunkWeb（8386）、Splunk Management（8926）、KVストア（8106）
Answer: A (メーッセージを残す**)**
説明/参照：
https ://docs.splunk.com/Documentation/Splunk/8.1.2/Security/SecureSplunkonyournetwork

最新問題**: 56**
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は、最新の1時間のデータが表示されていません。検索のスキップなどの潜在的なエラーについて、どのデータモデルをチェックする必要がありますか？
A. Web
B. リスク
C. パフォーマンス
D. 認証
Answer: (解答を表示する**)**
参照：
https://answers.splunk.com/answers/565482/how-to-resolve-skipped-scheduled-searches.html

最新問題**: 57**

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

最新問題**: 58**
ESがダウンロードできる脅威インテリジェンスの種類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. SplunkEnterpriseThreatGenerator
Answer: B (メーッセージを残す**)**
参照：
https://docs.splunk.com/Documentation/ES/6.1.0/Admin/Downloadthreatfeed

最新問題**: 59**
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のはどこですか？
A. コンテンツエクスポーター
B. 構成->コンテンツ管理
C. コンテンツダッシュボードのエクスポート
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**)**
参照：
https://docs.splunk.com/Documentation/ES/6.1.0/Admin/Export

最新問題**: 60**
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: B (メーッセージを残す**)**
説明/リファレンス：
https ://docs.splunk.com/Documentation/AddonBuilder/3.0.1/UserGuide/Installation

最新問題**: 61**
アドオンビルダーはどこから入手できますか？

A. SplunkBase
B. GitHub
C. ESインストールパッケージ
D. www.splunk.com
Answer: A (メーッセージを残す**)**

最新問題**: 62**
アセットルックアップのどの列を使用して、イベント内のアセットを識別しますか？
A. src、dvc、dest
B. cidr、port、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**: 63**
ESの実装中に役立つシナリオが含まれている機能はどれですか？
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**: 64**
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. DA-
B. SA-
C. TA-
D. アプリ-
Answer: C (メーッセージを残す**)**
参照：

https://dev.splunk.com/enterprise/docs/developapps/enterprisesecurity/abouttheessolution/

最新問題: **65**
アナリストは、ネットワークトラフィックデータをキャプチャして分析する機能を要求しています。管理者はドキュメントを調査し、この調査に基づいて、Splunk AppforStream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、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. プロトコルインテリジェンスダッシュボード。
C. Webインテリジェンスダッシュボード。
D. ユーザーインテリジェンスダッシュボード。
Answer: B (メーッセージを残す**)**

最新問題: **66**
注目すべきイベントの作成を抑制するために使用される相関検索機能はどれですか？
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: C (メーッセージを残す**)**
参照：
https://docs.splunk.com/Documentation/ES/6.1.0/Admin/Configurecorrelationsearches

最新問題: **67**
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. [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。
B. 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。
C. 相関検索、管理されたルックアップ、およびガラステーブルのみ。
D. 相関検索のみ。
Answer: (解答を表示する**)**
参照：
%20content%20from%20Splunk%20Enterprise%20Security%20as、from%20the%20Content%20Management
%20page。&text = You%20can%20export%20any%20type、%2C%20data%20models%2C%20and%20views。

最新問題: **68**
脅威生成検索は何を生成しますか？
A. KVストアコレクションでIntelを脅かします。

B. 脅威相関検索。
C. 注目すべきインデックスの注目すべき脅威。
D. threat_activityインデックスのイベント。
Answer: D (メーッセージを残す**)**
説明
https://docs.splunk.com/Documentation/ES/6.4.1/Admin/Createthreatmatchspecs

最新問題**: 69**
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. ワークステーション、ノートブック、およびPOSシステム。
B. RESTAPI呼び出し。
C. 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。
D. 調査の最終結果のステータス。
Answer: C (メーッセージを残す**)**

最新問題**: 70**
セキュリティポスチャダッシュボードには何が表示されますか？
A. 活発な調査とその状況。
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: (解答を表示する**)**
セキュリティポスチャダッシュボードは、展開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レベルの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が提供されます。
参照：https://docs.splunk.com/Documentation/ES/6.1.0/User/SecurityPosturedashboard

最新問題**: 71**
CIMデータモデルに対してデフォルトで検索されるインデックスはどれですか？
A. 注目すべきデフォルト
B. 要約と注目すべき
C. _内部および要約
D. すべてのインデックス
Answer: D (メーッセージを残す**)**
説明/参照：https://answers.splunk.com/answers/600354/indexes-searched-by-cim-data-models.html

最新問題**: 72**

プロパティの正規化された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 datamodelsearchで、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 loadjobsearchで、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 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。
Answer: B (メーッセージを残す)
説明/参照：
https ://docs.splunk.com/Documentation/CIM/4.15.0/User/UsetheCIMtonormalizedataatsearchtime

最新問題**: 73**
リスク分析ダッシュボードのパネルに表示されるデータモデルはどれですか？
A. リスク
B. 監査
C. ドメイン分析
D. 脅威インテリジェンス
Answer: (解答を表示する)
説明/参照：
参照 :https ://docs.splunk.com/Documentation/ES/6.1.0/User/RiskAnalysis#Dashboard_panels

最新問題**: 74**
$ SPLUNK_HOME / etc / appsのESアプリとアドオンは、ステージングインスタンスからクラスターデプロイヤー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 / searchpeers /
C. $ SPLUNK_HOME / etc / shcluster / apps
D. $ SPLUNK_HOME / etc / master-apps /
Answer: C (メーッセージを残す)
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、デプロイヤーに移行され、サーチヘッドクラスター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をにコピーします
デプロイヤー上の$SPLUNK_HOME/ etc / shcluster/apps。1.デプロイヤーで、ステージング時のアップグレード中に削除された$ 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。ステージング時に生成されたESアップグレードレポートを確認するか、に移動したアプリを調べて確認します
$ SPLUNK_HOME / etc/disabled-ステージング時のアプリ

最新問題**: 75**

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、またはその他のタイプ）に何を追加しますか？
A. 緊急性。
B. リスクプロファイル。
C. 集計。
D. 数値スコア。
Answer: C (メーッセージを残す**)**
参照：
https://docs.splunk.com/Documentation/ES/6.1.0/User/RiskScoring

最新問題**: 76**
ダッシュボード要件マトリックスドキュメント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. 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。
C. 各ダッシュボードに依存するデータモデルを識別します。
D. ローカルデータモデル用に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。
Answer: (解答を表示する**)**

最新問題**: 77**
加速ストレージの代替の場所を指定するためにindexes.confで使用される設定はどれですか？
A. thawedPath
B. tstatsHomePath
C. summaryHomePath
D. warmToColdScript
Answer: (解答を表示する**)**
説明/参照：
https ://docs.splunk.com/Documentation/Splunk/8.0.2/Knowledge/Acceleratedatamodels

最新問題**: 78**
データが取り込まれた後、生データをデータモデルによって高速化し、ESで使用できるようにするために、どのデータ管理ステップが不可欠ですか？

A. フィールドの抽出。
B. 顧客標準への正規化。
C. Splunk CommonInformationModelへの正規化。
D. タグを適用します。
Answer: C (メーッセージを残す**)**

最新問題**: 79**
ES資産の例は何ですか？
A. サーバー
B. MACアドレス
C. ユーザー名
D. 人
Answer: B (メーッセージを残す**)**

最新問題**: 80**
ブルートフォースアクセス動作検出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。入力データが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すか？
A. 検索を編集し、whereまたはxswhereステートメントを探し、しきい値を比較した後、一致する頻度を減らします。
B. 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。
C. 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。
D. 検索を編集し、whereまたはxswhereステートメントを探し、比較されるしきい値を変更して、より一般的な一致にします。
Answer: A (メーッセージを残す**)**

最新問題**: 81**
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. 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。
B. インデックス付きリアルタイム検索を無効にします。
C. 誤検知の数が多い相関検索に注目すべきイベント抑制を追加します。
D. すべての相関検索の優先度を上げます。
Answer: B (メーッセージを残す**)**

最新問題**: 82**
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、およびRAMの参照最小要件は何ですか？

A. OS :64ビット、RAM :32 MB、CPU :12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 :12 MB、CPU :16コア
Answer: D (メーッセージを残す)

最新問題**: 83**
ESで使用されるデータモデル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. 異常
B. ネットワークトラフィック
C. 認証
D. Web
Answer: (解答を表示する)

最新問題**: 84**
ネットワークのアクティビティ全体で使用されているネットワークサービスを観察するには、エンタープライズセキュリティ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 (メーッセージを残す)
参照：
https://docs.splunk.com/Documentation/ES/6.1.0/User/NetworkProtectionDomaindashboards