# PaloAltoNetworks.XDR-Engineer.v2025-08-25.q18

| | |
|---|---|
| 試験コード: | XDR-Engineer |
| 試験名称: | Palo Alto Networks XDR Engineer |
| 認定資格: | Palo Alto Networks |
| 無料問題数: | 18 |
| バージョン: | v2025-08-25 |
| アクセス数: | 105 |
| ページビュー数: | 180 |
| https://www.jpnpdf.com/PaloAltoNetworks.XDR-Engineer.v2025-08-25.q18-mondaishu.html | |

最新問題: **1**
あるエンジニアが、様々なソースからのアラート数を視覚化するダッシュボードを構築しています。ダッシュボードのウィジェットの1つを下の画像に示します。


エンジニアは、このウィジェットにドリルダウンを設定して、ダッシュボードユーザーが任意のアラート名を選択し、関連する詳細情報とともにアラートを表示できるようにしたいと考えています。エンジニアは、この要件を満たすために、以下のXQLクエリを設定しました。
データセット = アラート
| フィールド: アラート名、説明、アラートソース、重大度、オリジナルタグ、アラートID、インシデントID
| フィルターアラート名
| 降順で並べ替え _時間
エンジニアは、選択したアラート名で動的なフィルタリングを可能にするために、クエリの 3 行目 (filter alert_name =) をどのように完成させるのでしょうか。
**A.** $y_axis.値

**B.** $x_axis.値
**C.** $x_axis.name
**D.** $y_axis.name
**Answer: B (メーッセージを残す)**
Cortex XDRでは、ダッシュボードとウィジェットがドリルダウン機能をサポートしており、ユーザーはウィジェット要素（例：棒グラフ内のアラート名）をクリックして、選択した値でフィルタリングされた詳細データを表示できます。これは、クリックした要素の値を参照する動的変数を含むXQL（XDRクエリ言語）クエリを使用して実現されます。提供されたXQLクエリでは、エンジニアはウィジェットで選択されたalert_nameに基づいてアラートをフィルタリングしたいと考えています。
ウィジェットは、アラート名をX軸に沿って表示します（例えば、各バーがアラート名とその件数を表す棒グラフなど）。ユーザーがアラート名をクリックすると、ドリルダウンクエリによってデータセットがフィルタリングされ、選択されたalert_nameに一致するアラートのみが表示されます。XQLでは、ドリルダウンの動的フィルタリングは、$x_axis.valueなどの変数を使用して、クリックされたX軸上の要素の値を取得します。
* 正解分析 (B): 変数$x_axis.valueは、ユーザーが選択したx軸要素（この場合はalert_name）の値を参照するために使用されます。フィルターalert_nameを使用してクエリを完成させます。
= $x_axis.value により、ドリルダウンによってアラート データセットがフィルターされ、クリックされた値とalert_nameが一致するレコードのみが表示されます。
* 他のオプションを選択しないのはなぜですか?
* A. $y_axis.value: この変数は、通常、categoricalalert_name ではなく、グラフ内の数値 (アラートの数など) を表す y 軸の値を参照します。
* C. $x_axis.name: これはドリルダウンに有効なXQL変数ではありません。XQLは選択された値を取得するために$x_axis.nameではなく$x_axis.valueを使用します。
* D. $y_axis.name: これも有効な XQL 変数ではなく、y 軸は byalert_name によるフィルタリングには関係ありません。
正確な抜粋または参照:
Cortex XDRドキュメントポータルのXQLリファレンスガイドでは、ドリルダウンの設定について次のように説明しています。「クリックされたウィジェット要素に基づいてデータをフィルタリングするには、$x_axis.valueを使用して、ユーザーが選択したx軸カテゴリの値を参照します」（ダッシュボードとウィジェットセクションからの引用）。EDU-262: Cortex XDR調査と対応コースでは、ダッシュボードの作成とXQLについて説明し、「ドリルダウンクエリは$x_axis.valueなどの変数を使用して、ユーザーの選択に基づいて動的にフィルタリングします」（コース資料からの引用）。Palo Alto Networks認定XDRエンジニアのデータシートには、インタラクティブウィジェットの設定を含む「ダッシュボードとレポート」が試験の主要トピックとして記載されています。
参考文献:
Palo Alto Networks Cortex XDR ドキュメント ポータル: XQL リファレンス ガイド (https://docs-cortex.
paloaltonetworks.com/)

EDU-262: Cortex XDR 調査と対応コースの目標
Palo Alto Networks 認定 XDR エンジニア データシー
ト:https://www.paloaltonetworks.com/services/education
/認定#xdr-エンジニア

最新問題**: 2**
XDRエンジニアが、特定のシステムにおけるログインアクティビティを監視するための相関ルールを作成しています。アクティビティが検出されるとアラートが生成されます。アラートは正常に生成されていますが、表示時にユーザー名が表示されません。アラートにユーザー名情報を含めるにはどうすればよいでしょうか？
**A.** MITRE ATT&CKマッピングで 「初期アクセス」を選択し、ユーザー名を含める
**B.** 相関ルールのクエリを更新してユーザー名フィールドを含めます
**C.** アラートフィールドマッピングにユーザー名フィールドのマッピングを追加します。
**D.** アラートにユーザー名フィールドを取得するドリルダウンクエリを追加します。
**Answer: C (**メーッセージを残す**)**
Cortex XDRでは、相関ルールを使用して、取り込んだデータを分析し、条件が満たされたときにアラートを生成することで、特定のパターンや行動（例：ログインアクティビティ）を検出します。アラートにユーザー名などの特定のフィールドを含めるには、相関ルールのアラートフィールドマッピング設定で、そのフィールドを明示的にマッピングする必要があります。このマッピングにより、生成されるアラートの詳細に、基になるデータセットのどのフィールドが含まれるかが決まります。
このシナリオでは、相関ルールはログインアクティビティに関するアラートを正しく生成していますが、ユーザー名フィールドがありません。これは、相関ルールのクエリは関連イベントを識別しているものの、ユーザー名フィールドがアラートの出力フィールドに含まれていないことを示しています。この問題を解決するには、エンジニアは相関ルールのアラートフィールドマッピングを更新し、ユーザー名フィールドを明示的に含め、アラートの詳細を表示したときにユーザー名フィールドが表示されるようにする必要があります。
* 正解分析 (C): アラートフィールドマッピングにユーザー名フィールドのマッピングを追加すると、そのフィールドがデータセットから抽出され、アラートのメタデータに含まれるようになります。これは相関ルール設定で実行され、管理者はアラート出力に含めるフィールドを指定できます。
* 他のオプションを選択しないのはなぜですか?
* A. MITRE ATT&CK マッピングで 「初期アクセス」を選択し、ユーザー名を含めます。
「初期アクセス」のようなMITRE ATT&CKテクニックへのマッピングは、攻撃の種類や行動を定義するものであり、ユーザー名などの特定のフィールドを定義するものではありません。これでは、フィールドの欠落の問題は解決されません。
* B. 相関ルールのクエリを更新し、ユーザー名フィールドを含める：相関ルールのクエリは、関連イベントを検出するためにユーザー名フィールドを参照する必要がありますが、クエリに含める

だけではアラート出力にユーザー名フィールドが表示されるとは限りません。アラートフィールドのマッピングは依然として必要です。
* D. アラートにユーザー名フィールドを取得するドリルダウンクエリを追加する :ドリルダウンクエリは、アラート生成後の追加調査に使用され、アラート自体にフィールドを含めるものではありません。この方法では、アラートの詳細にユーザー名が表示されない問題は解決されません。
正確な抜粋または参照:
Cortex XDRドキュメントポータルでは、相関ルールの設定について次のように説明しています。 生成されたアラートに特定のフィールドを含めるには、相関ルールのアラートフィールドマッピングを設定して、ユーザー名などのデータセットフィールドをアラート出力にマッピングします」（相関ルールセクションからの引用）。EDU-262: Cortex XDR調査と対応コースでは検出エンジニアリングについて取り上げており、「アラートフィールドマッピングによって、相関ルールによって生成されるアラートに含まれるデータフィールドが決定されます」（コース資料からの引用）。Palo Alto Networks認定XDRエンジニアのデータシートには、相関ルールの設定を含む「検出エンジニアリング」が試験の主要トピックとして記載されています。
参考文献:
Palo Alto Networks Cortex XDR ドキュメント ポータル:https://docs-cortex.paloaltonetworks.com/ EDU-262: Cortex XDR 調査および対応コースの目標 Palo Alto Networks 認定 XDR エンジニア データシート:https://www.paloaltonetworks.com/services/education/認定#xdr-エンジニア

最新問題**: 3**
新しい相関ルールの条件が満たされた後、アラートが自動的に生成される最も早い時間枠はどれくらいですか?
**A.** 30分から45分の間
**B.** 直ちに
**C.** 5分以内
**D.** 10〜20分
**Answer: C (**メーッセージを残す**)**
Cortex XDRでは、相関ルールを使用して、取り込んだデータを分析し、条件が満たされたときにアラートを生成することで、特定のパターンや動作を検出します。アラート生成のタイミングは、データ取り込みパイプライン、Cortex XDRバックエンドの処理レイテンシ、およびルールの評価頻度によって異なります。
新しい相関ルールの場合、条件が満たされると（つまり、関連するイベントが取り込まれて処理されると）、Cortex XDR は、ほぼリアルタイムの処理機能により、通常は 5 分以内などの短い時間枠内でアラートを生成します。
* 正解分析 (C): Cortex XDRのアーキテクチャはイベントを迅速に処理・相関させるように設計されているため、アラートが生成される最短時間は5分以内です。これは、データの取り込み、相関ルールの評価、そしてシステム内でのアラート生成にかかる時間を考慮したものです。

* 他のオプションを選択しないのはなぜですか?
* A. 30〜45分 :Cortex XDRの準リアルタイム検出機能にはこの時間枠は長すぎます。処理のバックログが大きいシステムではこのような遅延が発生する可能性がありますが、適切に構成されたCortex XDR環境では発生しません。
* B. 即時 :Cortex XDRは高速ですが、「即時」とはレイテンシゼロを意味しますが、データの取り込み、処理、ルール評価のステップがあるため現実的ではありません。わずかな遅延（5分以内）が予想されます。
* D. 10〜20 分: システムは迅速な検出とアラート生成に最適化されているため、Cortex XDR で可能な限り早いアラート生成を行うには、これも長すぎます。
正確な抜粋または参照:
Cortex XDRドキュメントポータルでは、相関ルールの処理について次のように説明しています。「相関ルールの条件が満たされてから5分以内にアラートが生成されます。ただし、データはほぼリアルタイムで取り込まれ、処理されていると仮定します」（相関ルールセクションからの引用）。EDU-262 :Cortex XDR調査と対応コースでは検出エンジニアリングについて取り上げており、「Cortex XDRの相関エンジンは、通常、イベントの取り込みから数分以内にルールを処理し、アラートを生成します」（コース資料からの引用）。Palo Alto Networks認定XDRエンジニアのデータシートには、「検出エンジニアリング」が試験の主要トピックとして記載されており、相関ルールによるアラート生成も含まれています。
参考文献:
Palo Alto Networks Cortex XDR ドキュメント ポータル:https://docs-cortex.paloaltonetworks.com/ EDU-262: Cortex XDR 調査および対応コースの目標 Palo Alto Networks 認定 XDR エンジニア データシート:https://www.paloaltonetworks.com/services/education/認定#xdr-エンジニア

最新問題**: 4**
最小限の構成で、顧客が Windows DHCP サーバーから Cortex XDR に追加のイベントを取り込むにはどうすればよいですか?
**A.** Windows イベント コレクター (WEC) をアクティブ化する
**B.** XDRコレクターをインストールする
**C.** HTTPコレクター統合を有効にする
**D.** Cortex XDRエージェントをインストールする
**Answer: B (**メーッセージを残す**)**
Windows DHCPサーバーからCortex XDRに最小限の設定で追加イベントを取り込むには、Cortex XDR Collectorの使用をお勧めします。XDR Collectorは、Windowsサーバーを含む様々なソースからログとイベントを収集し、分析と相関分析のためにCortex XDRに転送するために設計された軽量コンポーネントです。Cortex XDRエージェントの完全な導入が不要なシナリオに最適化されており、データ収集プロセスの大部分を自動化することで設定のオーバーヘッドを最小限に抑えます。

Windows DHCPサーバーの場合、XDRコレクターをサーバーにインストールすることで、Windowsイベントログやその他の関連ソースからDHCPログ（リースの割り当て、更新、エラーなど）を収集できます。インストールが完了すると、コレクターは最小限の設定でこれらのイベントをCortex XDRテナントに転送します。必要なのは、ターゲットデータタイプの指定やCortex XDRクラウドへのネットワーク接続の確保といった基本的な設定のみです。このアプローチは、完全なエージェントをセットアップしたり、Windowsイベントコレクター（WEC）やHTTPコレクターなどの外部統合を設定したりするといった、追加のインフラストラクチャや手動設定を必要とする代替手段よりも簡単です。
* 他のオプションを選択しないのはなぜですか?
* A. Windows イベントコレクター (WEC) を有効化する：WEC は Windows サーバーからイベントを収集できますが、WEC サーバーのセットアップ、サブスクリプションの設定、別の取り込みメカニズムを介した Cortex XDR との統合など、多くの設定が必要です。これは最小限の設定ではありません。
* C. HTTP コレクター統合を有効にする: HTTP コレクター統合は、HTTP/HTTPS API 経由でデータを取り込むために使用されますが、DHCP ログは通常、HTTP 経由では公開されずに Windows イベント ログに保存されるため、Windows DHCP サーバー イベントには適用されません。
* D. Cortex XDRエージェントをインストールする：Cortex XDRエージェントは、防御、検知、対応機能を備えたフル機能のエンドポイント保護および検知ソリューションです。イベントデータの収集は可能ですが、DHCPサーバーイベントの取り込みという特定のタスクには過剰であり、XDRコレクターよりも多くの設定が必要です。
正確な抜粋または参照:
Cortex XDRドキュメントポータルでは、XDRコレクターは「最小限のセットアップでサーバーとエンドポイントからログとイベントを収集するツール」であると説明されています（データ取り込みセクションからの引用）。EDU-260：
Cortex XDRの予防と導入コースでは、「XDRコレクターは、Windows DHCPサーバーなどのサーバーログを、効率的な設定で取り込むのに最適です」（コース資料からの引用）と強調されています。Palo Alto Networks認定XDRエンジニアのデータシートでは、「データソースのオンボーディングと統合設定」が重要なスキルとして挙げられており、これにはログ取り込みのためのXDRコレクターの設定が含まれます。
参考文献:
Palo Alto Networks Cortex XDR ドキュメント ポータル:https://docs-cortex.paloaltonetworks.com/ EDU-260: Cortex XDR の防止と展開コースの目標 Palo Alto Networks 認定 XDR エンジニア データシート:https://www.paloaltonetworks.com/services/education/認定#xdr-エンジニア

最新問題: **5**
以下のクエリではどのようなアクションが実行されていますか?

データセット = xdr_data
| フィールド agent_hostname、_time、_product
| エージェントホスト名、_product による最新時刻の最新コンポーネント
| 結合タイプ = 内部 (データセット = エンドポイント
| フィールド endpoint_name、endpoint_status、endpoint_type) をルックアップ
lookup.endpoint_name = agent_hostname として
| フィルター エンドポイントステータス = ENUM.CONNECTED
| フィールド agent_hostname、endpoint_status、latest_time、_product
**A.** エンドポイントの最新のアクティビティを監視する
**B.** ネットワークから切断されたエンドポイントを識別する
**C.** 接続されたファイアウォールエンドポイントの最新のアクティビティを監視する
**D.** エージェントのバージョンが古いエンドポイントをチェックしています
**Answer: A (メーッセージを残す)**
Cortex XDRに付属するXQL（XDRクエリ言語）クエリは、データを取得・処理し、エンドポイントのアクティビティに関する洞察を提供します。その目的を理解するために、クエリを分解してみましょう。
* データセット = xdr_data | fields agent_hostname、_time、_product: xdr_dataデータセット (一般的なイベント データ) を選択し、エージェント ホスト名、タイムスタンプ、および製品 (エージェント タイプまたはコンポーネントなど) のフィールドを取得します。
* comp Latest as Latest_Time by Agent_hostname, _product: Agent_hostnameと_productの組み合わせごとに最新のタイムスタンプ（time）を計算し、結果にLatest_timeという名前を付けます。これにより、各エンドポイントと製品の最新のアクティビティが識別されます。
* join type=inner (dataset = endpoints | fields endpoint_name, endpoint_status, endpoint_type) as lookup lookup.endpoint_name = agent_hostname: エンドポイントデータセットとの内部結合を実行し、endpoint_name (エンドポイントデータセットから) と agent_hostname (xdr_data から) を一致させ、endpoint_status や endpoint_type などのフィールドを取得します。
* filter endpoint_status = ENUM.CONNECTED: 結果をフィルタリングして、ステータスが CONNECTED のエンドポイントのみを含めます。
* フィールド agent_hostname、endpoint_status、latest_time、_product: 最終フィールド (ホスト名、ステータス、最新のアクティビティ時間、製品) を出力します。
* 正解分析 (A): このクエリはエンドポイントの最新アクティビティを監視しています。イベントデータ (xdr_data) とエンドポイントメタデータ (endpoints) を結合し、接続されたエンドポイントをフィルタリングすることで、接続された各エンドポイント (agent_hostname) の最新アクティビティ (latest_time) を計算します。これにより、アクティブなエンドポイントの最新アクティビティが表示され、エンドポイントのステータスや最近のイベントの監視に役立ちます。
* 他のオプションを選択しないのはなぜですか?
* B. ネットワークから切断されたエンドポイントの識別: クエリは、endpoint_status = ENUM.CONNECTED をフィルターするため、接続されたエンドポイントのみが含まれ、切断されたエンドポイントは含まれません。

* C. 接続されたファイアウォールエンドポイントの最新アクティビティの監視 :このクエリは、ファイアウォールエンドポイントをフィルタリングしません（例endpoint_type または _product を使用してファイアウォールを指定する）。このクエリは、ファイアウォールだけでなく、接続されているすべてのエンドポイントに適用されます。
* D. 古いエージェント バージョンを持つエンドポイントの確認: クエリはエージェント バージョン情報 (agent_version フィールドなど) を取得または比較せず、最新のアクティビティ時間に焦点を当てます。
正確な抜粋または参照:
Cortex XDRドキュメントポータルでは、XQLクエリについて次のように説明しています。
「comp_latestとエンドポイントデータセットの結合を使用したクエリは、最新のイベントタイムスタンプを計算することで、接続されたエンドポイントの最新のアクティビティを監視できます」（XQLリファレンスガイドからの引用）。EDU-262 :Cortex XDR調査と対応コースでは、監視のためのXQLについて説明し、「xdr_dataとエンドポイントデータセットを最新の計算と組み合わせることで、最新のエンドポイントアクティビティを監視できます」（コース資料からの引用）。Palo Alto Networks認定XDRエンジニアのデータシートには、監視のためのXQLクエリを含む「ダッシュボードとレポート」が主要な試験トピックとして記載されています。
参考文献:
Palo Alto Networks Cortex XDR ドキュメント ポータル:https://docs-cortex.paloaltonetworks.com/ EDU-262: Cortex XDR 調査および対応コースの目標 Palo Alto Networks 認定 XDR エンジニア データシート:https://www.paloaltonetworks.com/services/education/認定#xdr-エンジニア

最新問題**: 6**
社内ノートPCに不正なリムーバブルドライブがマウントされているという証拠を提供するため、内部不正侵入調査の依頼を受けました。Cortex XDRエージェントは、デフォルトの防御エージェント設定プロファイルとデフォルトの拡張機能「デバイス構成」プロファイルを使用してインストールされています。エンジニアはどこで証拠を見つけることができますか？
**A.** ホストインベントリの確認 -> マウント
**B.** データセット = xdr_data | フィルター event_type = ENUM.MOUNT および event_sub_type = ENUM。
マウント_ドライブ_マウント
**C.** 要求されたデータを取得するには追加の構成が必要です
**D.** preset = device_control
**Answer: A (**メーッセージを残す**)**
Cortex XDR では、デバイス構成プロファイル (エージェント設定プロファイルの拡張) によって、Cortex XDR エージェントがリムーバブル ドライブのマウントなどのデバイス関連のアクティビティを監視および管理する方法が制御されます。

デバイス構成プロファイルには、USBドライブやその他のリムーバブルメディアがエンドポイントに接続された場合など、デバイスマウントイベントの監視がデフォルトで含まれています。これらのイベントはログに記録され、内部者による侵害シナリオにおける不正なドライブ使用の検出など、調査のためにアクセスできます。
* 正解分析 (A): Cortex XDRコンソールの「ホストインベントリ」→「マウント」セクションでは、各エンドポイントのマウントイベントの詳細なビューが提供され、システムにマウントされたリムーバブルドライブに関する情報も表示されます。これは、デフォルトのデバイス構成プロファイルによってキャプチャされたデバイスマウントイベントを集約しているため、会社のラップトップに許可されていないリムーバブルドライブがマウントされた証拠を見つける最も簡単な方法です。
* 他のオプションを選択しないのはなぜですか?
* B. データセット = xdr_data | フィルター event_type = ENUM.MOUNT および event_sub_type = ENUM。
MOUNT_DRIVE_MOUNT: このXQLクエリは、xdr_dataデータセットからマウントイベントを取得するには技術的には正しいですが、手動でクエリを実行し、特定のイベントタイプに関する知識が必要です。ホストインベントリ -> マウントセクションは、このデータにアクセスするためのよりユーザーフレンドリーで直接的な方法であるため、この問題を調査するエンジニアにとって推奨される選択肢です。
* C. 要求されたデータをキャプチャするには追加の構成が必要です: これは誤りです。デフォルトのデバイス構成プロファイルは既にリムーバブル ドライブのマウント イベントをキャプチャしているため、追加の構成は必要ありません。
* D. preset = device_control: XQLのdevice_controlpresetはデバイス制御関連のイベント（例USBブロックまたは許可アクション）を取得しますが、明示的に設定しない限り、マウントイベントは含まれない場合があります。この調査では、ホストインベントリ -> マウントセクションの方が対象となります。
正確な抜粋または参照:
Cortex XDRドキュメントポータルでは、デバイス監視について次のように説明しています。「デフォルトのデバイス構成プロファイルは、リムーバブルドライブのマウントイベントを記録します。これらのイベントは、コンソールの「ホストインベントリ」→「マウント」セクションで確認できます」（デバイス構成セクションからの引用）。EDU-262: Cortex XDR調査と対応コースでは、調査手法について説明しており、「デフォルトのデバイス監視が設定されているエンドポイントでは、リムーバブルドライブのマウントイベントはホストインベントリで確認できます」（コース資料からの引用）。Palo Alto Networks認定XDREngineerのデータシートには、エンドポイントイベントの調査を含む「メンテナンスとトラブルシューティング」が試験の主要トピックとして記載されています。
参考文献:
Palo Alto Networks Cortex XDR ドキュメント ポータル:https://docs-cortex.paloaltonetworks.com/ EDU-262: Cortex XDR 調査および対応コースの目標 Palo Alto

Networks 認定 XDR エンジニア データシー
ト:https://www.paloaltonetworks.com/services/education
/認定#xdr-エンジニア

最新問題: **7**
XDR Collector を使用して、Windows システムと Linux システムの両方に適用できる、利用可能な組み込みテンプレートを持つ構成プロファイル オプションはどれですか。
**A.** ファイルビート
**B.** HTTPコレクターテンプレート
**C.** XDRコレクターの設定
**D.** ウィンログビート
**Answer: A (メーッセージを残す)**
Cortex XDRのXDRコレクターは、WindowsおよびLinuxシステムを含むサーバーやエンドポイントからログとイベントを収集し、Cortex XDRクラウドに転送して分析するための軽量ツールです。設定を簡素化するために、Cortex XDRは様々なログ収集方法に対応した組み込みテンプレートを提供しています。この質問では、WindowsとLinuxの両方のシステムに適用できる組み込みテンプレートを含む構成プロファイルオプションについて尋ねています。
* 正解分析 (A):Filebeat は、Cortex XDR の XDR Collector でサポートされている多目的ログ シッパーであり、Windows と Linux の両方のシステムのファイルからログを収集するためのテンプレートが組み込まれています。
Filebeatは、様々なソース（アプリケーションログ、システムログなど）からログを収集するように設定でき、プラットフォームに依存しないため、異機種混在環境にも適しています。Cortex XDRは、一般的なログタイプの設定を効率化するための事前設定済みFilebeatテンプレートを提供し、オペレーティングシステム間の互換性を確保します。
* 他のオプションを選択しないのはなぜですか?
* B. HTTPコレクターテンプレート: HTTPコレクターテンプレートは、HTTP経由でデータを取り込むために使用されます。
/HTTPS APIはWindowsやLinuxシステムに固有のものではなく、プラットフォームベースのログ収集方法でもありません。また、Filebeatと比較すると、システムレベルのログ収集ではあまり使用されません。
* C. XDRコレクター設定：「XDRコレクター設定」はXDRコレクターの一般的な設定を指し、特定のテンプレートを指すものではありません。XDRコレクターは実際のログ収集にFilebeatやWinlogbeatなどのテンプレートを使用するため、このオプションは曖昧すぎます。
* D. Winlogbeat: Winlogbeatは、Windowsイベントログの収集に特化したログシッパーです。Linuxシステムではサポートされていないため、どちらのプラットフォームにも適していません。
正確な抜粋または参照:
Cortex XDRドキュメントポータルでは、XDRコレクターテンプレートについて次のように説明しています。 「Filebeatテンプレートは、WindowsとLinuxの両方のシステム上のファイルからログを収集するために提供されており、プラットフォーム間で柔軟なログ収集を可能にします」 データ

取り込みセクションからの引用）。EDU-260 :Cortex XDRの予防と展開コースでは、XDRコレクターの設定について説明し、 Filebeatは、WindowsとLinux用の組み込みテンプレートでサポートされている、ログ収集のためのクロスプラットフォームソリューションです」 ロース資料からの引用）と述べています。Palo Alto Networks認定XDRエンジニアのデータシートには、XDRコレクターテンプレートを含む データの取り込みと統合」が主要な試験トピックとして記載されています。
参考文献:
Palo Alto Networks Cortex XDR ドキュメント ポータル:https://docs-cortex.paloaltonetworks.com/ EDU-260: Cortex XDR の防止と展開コースの目標 Palo Alto Networks 認定 XDR エンジニア データシート:https://www.paloaltonetworks.com/services/education/認定#xdr-エンジニア

最新問題**: 8**
Palo Alto Networks NGFW を Cortex XDR にオンボードする場合、デバイスを選択して検証した後、ログが正常に取り込まれていることを確認するには、何を行う必要がありますか?
**A.** NGFWログデータに対してXQLクエリを実行する
**B.** NGFWに関連するインシデントが表示されるまで待ちます
**C.** 選択したデバイスに有効な証明書があることを確認します
**D.** NGFWダッシュボードからデバイス証明書を取得する
**Answer: A (**メーッセージを残す**)**
Palo Alto Networksの次世代ファイアウォール NGFW）をCortex XDRにオンボーディングする際は、デバイスの選択と検証を行い、Cortex XDRにログを送信できることを確認するプロセスが必要です。このステップの後、ログの取り込みが成功したことを確認することが、統合の検証において不可欠です。取り込みを確認する最も直接的かつ確実な方法は、XQL XDRクエリ言語）を使用して取り込んだログをクエリすることです。これにより、エンジニアはCortex XDR内でNGFWのログデータを検索できます。
* 正解分析 (A): NGFW ログ データに対して XQL クエリを実行するのが正しいアクションです。オンボーディング後、エンジニアはdataset = panw_ngfw_logs | limit 10などのXQLクエリを実行して、Cortex XDRにNGFWログが存在するかどうかを確認できます。これにより、ログが正常に取り込まれ、適切なデータセットに保存されていることが確認でき、統合が期待どおりに機能していることが保証されます。
* 他のオプションを選択しないのはなぜですか?
* B. NGFWに関連するインシデントが発生するまで待つ :インシデントが発生するまで待つことは、ログの取り込みを確認するための信頼性が高く、またプロアクティブな方法とは言えません。インシデントは検出ルールに依存しており、ログが取り込まれていてもすぐには発生しない可能性があります。

* C. 選択したデバイスに有効な証明書があることを確認します。オンボーディング プロセス中は有効な証明書が必要ですが (安全な通信のためなど)、この手順は検証プロセスの一部であり、検証後にログの取り込みを確認する方法ではありません。
* D. NGFWダッシュボードからデバイス証明書を取得する :NGFWダッシュボードからデバイス証明書を取得することは、Cortex XDRへのログ取り込みの確認とは無関係です。証明書はセットアップ時に管理され、オンボーディング後の検証には使用されません。
正確な抜粋または参照:
Cortex XDRドキュメントポータルでは、NGFWログの取り込み検証について次のように説明しています。 Palo Alto Networks NGFWログの取り込みが成功したことを確認するには、XQLクエリ（例dataset = panw_ngfw_logs）を実行して、Cortex XDRにログデータが存在することを確認します」データ取り込みセクションからの引用）。EDU-260 :Cortex XDRの予防と展開コースでは、NGFW統合について取り上げており、 オンボーディング後にNGFWログが取り込まれていることを検証するためにXQLクエリが使用されます」ロース資料からの引用）。Palo Alto Networks認定XDRエンジニアのデータシートには、ログ取り込み検証を含む データの取り込みと統合」が試験の主要トピックとして記載されています。
参考文献:
Palo Alto Networks Cortex XDR ドキュメント ポータル:https://docs-cortex.paloaltonetworks.com/ EDU-260: Cortex XDR の防止と展開コースの目標 Palo Alto Networks 認定 XDR エンジニア データシート:https://www.paloaltonetworks.com/services/education/認定#xdr-エンジニア

最新問題**: 9**
以前導入したWindows XDR Collectorエージェントのログイベントが、OSのアップグレード後にコンソールに表示されなくなりました。この現象の原因として考えられるのは、ログイベントのどの部分でしょうか？
**A.** 5MBより大きい
**B.** Filebeat形式です
**C.** Winlogbeat形式です
**D.** 1MB未満です
**Answer: A (**メーッセージを残す**)**

最新問題**: 10**
ダッシュボードのドリルダウンによってトリガーされる可能性のある 2 つのアクションは何ですか? (2 つ選択してください。)
**A.** 別のダッシュボードに移動する
**B.** 自動応答アクションを開始する
**C.** XQLクエリへのリンク
**D.** コンソールユーザーにアラートを送信する

**Answer: (解答を表示する)**
Cortex XDRでは、ダッシュボードのドリルダウン機能により、ユーザーはウィジェット（グラフや表など）の要素をクリックして詳細情報にアクセスしたり、アクションを実行したりすることができます。ドリルダウンは、関連データやビューへのリンクを提供することで、ダッシュボードの調査機能を強化します。
* 正解分析（A、C）：
* A. 別のダッシュボードへの移動：ドリルダウンを設定することで、別のダッシュボードに移動し、より詳細なビューや関連指標を表示できます。例えば、ウィジェット内のアラート数をクリックすると、アラートの詳細にフォーカスしたダッシュボードが開きます。
* C. XQLクエリへのリンク：ドリルダウンは、クリックした要素（アラート名やソースなど）に基づいてデータをフィルタリングするXQLクエリにリンクしていることがよくあります。これにより、ユーザーはクエリビルダーや調査ビューで生のイベントや詳細なレコードを表示できます。
* 他のオプションを選択しないのはなぜですか?
* B. 自動対応アクションの開始：ドリルダウンは主にナビゲーションとデータ探索を目的としており、自動対応アクションのトリガーには使用されません。対応アクション（エンドポイントの隔離など）は通常、ダッシュボードではなく、インシデントビューまたはアラートビューから開始されます。
* D. コンソールユーザーへのアラート送信：ドリルダウンではユーザーにアラートは送信されません。アラートは相関ルールまたはBIOCによって生成され、ダッシュボードはアラート配信ではなく可視化に使用されます。
正確な抜粋または参照:
Cortex XDRドキュメントポータルでは、ドリルダウン機能について次のように説明しています。「ダッシュボードのドリルダウンでは、別のダッシュボードに移動したり、XQLクエリにリンクして、選択したウィジェット要素に基づいて詳細なデータを表示したりできます」（ダッシュボードとウィジェットセクションからの引用）。EDU-262: Cortex XDR調査と対応コースではダッシュボードについて説明しており、「ドリルダウンにより、他のダッシュボードやXQLクエリに移動してより詳細な分析を行うことができます」（コース資料からの引用）。Palo Alto Networks認定XDRエンジニアのデータシートには、ドリルダウンの設定を含む「ダッシュボードとレポート」が試験の主要トピックとして記載されています。
参考文献:
Palo Alto Networks Cortex XDR ドキュメント ポータル:https://docs-cortex.paloaltonetworks.com/ EDU-262: Cortex XDR 調査および対応コースの目標 Palo Alto Networks 認定 XDR エンジニア データシート:https://www.paloaltonetworks.com/services/education/認定#xdr-エンジニア

最新問題**: 11**
機密性が高く、規制の厳しい環境向けに Cortex XDR エージェントを構成する際に考慮すべき 2 つの手順はどれですか (2 つ選択してください)。

**A.** 重要な環境バージョンを有効にする
**B.** エージェントのアップグレード範囲がメンテナンスリリースのみであるエージェント設定プロファイルを作成します。
**C.** エージェント設定プロファイルを作成し、コンテンツの自動更新を有効にし、4日間の遅延を設定します。
**D.** マイナーコンテンツバージョンの更新を有効にする
**Answer: (**解答を表示する**)**
機密性が高く、規制の厳しい環境（医療、金融など）では、Cortex XDRエージェントの構成において、セキュリティ、安定性、コンプライアンスのバランスを取る必要があります。これには、エージェントのアップグレードとコンテンツの更新を制御し、中断を最小限に抑えながら、タイムリーな保護アップデートを確実に実行することが含まれることがよくあります。このバランスを実現するために、以下の手順が推奨されます。
* 正解分析（B、C）：
* B. エージェントのアップグレード範囲をメンテナンスリリースのみに限定したエージェント設定プロファイルを作成する：規制の厳しい環境では、エージェントの頻繁なアップグレードは不安定性や互換性の問題を引き起こすリスクがあります。アップグレードをメンテナンスリリースのみ（例：バグ修正やマイナーアップデート、メジャーバージョンアップは除く）に限定することで、安定性を確保しながら重大な問題に対処できます。これは、エージェント設定プロファイルで設定することで、アップグレード範囲を制御できます。
* C. エージェント設定プロファイルを作成し、コンテンツの自動更新を有効にして、4 日間の遅延を含めます。コンテンツの更新 (例: 行動脅威保護ルール、ローカル分析ロジック) は保護を維持するために重要ですが、規制された環境ではテストのために遅延できます。
4 日遅延のコンテンツ自動更新を有効にすると、更新が自動的に適用されることが保証されますが、変更を検証する時間も提供されるため、予期しない動作のリスクが軽減されます。
* 他のオプションを選択しないのはなぜですか?
* A. 重要な環境バージョンを有効にする：Cortex XDRには「重要な環境バージョン」という具体的な設定はありません。このオプションは誤った名称であるように思われ、規制環境における標準的なエージェント設定方法と一致していません。
* D. マイナー コンテンツ バージョン更新を有効にする: マイナー コンテンツ更新を有効にすると便利な場合がありますが、規制された環境で必要な制御 (テストの遅延など) は提供されません。
オプション C (遅延を伴う自動更新) は、より包括的で適切なステップです。
正確な抜粋または参照:
Cortex XDRドキュメントポータルでは、規制環境におけるエージェント設定について次のように説明しています。「機密性の高い環境では、エージェント設定プロファイルを設定して、アップグレードをメンテナンスリリースに制限し、コンテンツの自動更新を遅延（例4日間）させて、安定性とコンプライアンスを確保します」（エージェント設定セクションからの引用）。EDU-260：Cortex XDRの予防と展開コースでは、エージェント管理について説明しており、「規制環境では、セキュリティと安定性のバランスをとるために、メンテナンスのみのアップグレードと遅延コン

テンツ更新が推奨されます」ロース資料からの引用）。Palo Alto Networks認定XDRエンジニアのデータシートには、「Cortex XDRエージェント設定」が試験の主要トピックとして記載されており、規制環境向けの設定も網羅されています。
参考文献:
Palo Alto Networks Cortex XDR ドキュメント ポータル:https://docs-cortex.paloaltonetworks.com/ EDU-260: Cortex XDR の防止と展開コースの目標 Palo Alto Networks 認定 XDR エンジニア データシート:https://www.paloaltonetworks.com/services/education/認定#xdr-エンジニア

最新問題**: 12**
Cortex XDR では動的エンドポイント グループはどのように作成および管理されますか?
**A.** エンドポイント グループでは、ネットワークに新しいデバイスが追加されたときに、新しいエンドポイントでグループを更新するための介入が必要です。
**B.** 各エンドポイントは複数のグループに同時に所属することができ、同じデバイスに同時に異なるセキュリティポリシーを適用できます。
**C.** エンドポイントグループを作成した後、グループを削除して再作成しない限り、割り当てられたセキュリティポリシーを変更することはできません。
**D.** エンドポイントグループは、OSの種類、OSのバージョン、ネットワークセグメントなどのフィールドに基づいて定義されます。
**Answer: D (**メーッセージを残す**)**
Cortex XDRでは、動的エンドポイントグループを使用してエンドポイントを整理し、セキュリティポリシーの適用、構成の管理、運用の効率化を図ります。これらのグループは、OSの種類、OSのバージョン、ネットワークセグメント、ホスト名、その他のエンドポイント属性といった動的な基準に基づいて定義されます。新しいエンドポイントがネットワークに追加されると、これらの基準に基づいて適切なグループに自動的に割り当てられます。手動による介入は必要ありません。この動的な割り当てにより、グループの条件に一致するエンドポイントにセキュリティポリシーが一貫して適用されます。
* 正解分析 (D): 選択肢Dは、動的なエンドポイントグループの作成と管理方法を正確に説明しています。管理者は、オペレーティングシステム（Windows、macOS、Linuxなど）、OSバージョン（Windows 10 21H2など）、ネットワークセグメント（サブネットやドメインなど）などのエンドポイント属性に基づくフィルターを使用してグループを定義します。これらのフィルターは動的に評価されるため、エンドポイントの属性が変更されたり、新しいデバイスがオンボードされたりすると、エンドポイントは自動的にグループに追加または削除されます。
* 他のオプションを選択しないのはなぜですか?
* A. エンドポイント グループでは、ネットワークに新しいデバイスが追加されたときに、グループを新しいエンドポイントで更新するための介入が必要です。これは誤りです。動的エンドポイント グループは、手動介入なしに、グループの基準に一致する新しいエンドポイントを自動的に含めるように設計されているためです。

* B. 各エンドポイントは同時に複数のグループに属することができるため、同じデバイスに異なるセキュリティ ポリシーを同時に適用できます。これは誤りです。Cortex XDR では、競合を避けるために、エンドポイントはポリシー適用のために単一のエンドポイント グループに割り当てられます。
エンドポイントは複数のグループ基準に一致する可能性がありますが、システムは優先順位または階層を使用して、ポリシー適用のためにエンドポイントを 1 つのグループに割り当てます。
* C. エンドポイント グループを作成した後、グループを削除して再作成しない限り、割り当てられたセキュリティ ポリシーを変更することはできません。これは誤りです。Cortex XDR では、管理者はグループを削除して再作成しなくても、エンドポイント グループに割り当てられたセキュリティ ポリシーを変更できます。
正確な抜粋または参照:
Cortex XDR ドキュメント ポータルでは、エンドポイント グループ管理について次のように説明しています。 動的エンドポイント グループは、OS の種類、バージョン、ネットワーク セグメントなどのエンドポイント属性に基づいてフィルターを定義することによって作成されます。
エンドポイントは、これらの基準に基づいて自動的にグループに割り当てられます 「エンドポイント管理セクションからの引用」。EDU-260 :Cortex XDRの予防と展開コースでは、エンドポイントグループの構成について説明し、 「エンドポイントがネットワークに参加または離脱すると、定義された属性に基づいてグループが動的に更新されます」 「コース資料からの引用」と述べています。Palo Alto Networks認定XDRエンジニアのデータシートには、動的なエンドポイントグループを含む 「エンドポイント管理とポリシー構成」が主要な試験トピックとして記載されています。
参考文献:
Palo Alto Networks Cortex XDR ドキュメント ポータル:https://docs-cortex.paloaltonetworks.com/ EDU-260: Cortex XDR の防止と展開コースの目標 Palo Alto Networks 認定 XDR エンジニア データシート:https://www.paloaltonetworks.com/services/education/認定#xdr-エンジニア

最新問題**: 13**
以下の SBAC シナリオ画像に基づくと、テナントが許可モードに切り替えられた場合、どのエンドポイントのデータにアクセスできるようになりますか?


**A.** E1のみ
**B.** E2のみ
**C.** E1、E2、およびE3

**D.** E1、E2、E3、E4
**Answer: C (メーッセージを残す)**
Cortex XDRでは、スコープベースのアクセス制御（SBAC）は、エンドポイント、ユーザー、またはその他のリソースに割り当て可能な定義済みのスコープに基づいて、ユーザーのデータアクセスを制限します。許可モードでは、SBACは割り当てられたスコープ内のデータへのアクセスをユーザーに許可しますが、スコープ外のデータへのアクセスを制限する場合があります。この質問は、4つのエンドポイント（E1、E2、E3、E4）を持つSBACシナリオを想定しています。ユーザーは、E1、E2、E3を含む特定のスコープ（例：スコープA）にアクセスできる可能性がありますが、E4は別のスコープ（例：スコープB）にあります。
* 正解分析 (C): テナントが許可モードに切り替えられると、これらのエンドポイントはユーザーに割り当てられたスコープ (スコープ A など) 内にあるため、ユーザーは E1、E2、および E3 にアクセスできるようになります。
E4 は別のスコープ（例：スコープ B）にあるため、ユーザーがそのスコープへの明示的なアクセス権を持っていない限りアクセスできません。Permissive モードではスコープ制限が適用され、ユーザーのスコープ内のデータのみが表示されます。
* 他のオプションを選択しないのはなぜですか?
* A. E1 のみ: これは制限が厳しすぎます。ユーザーの範囲には E1 だけでなく、E1、E2、E3 が含まれます。
* B. E2 のみ: 同様に、これは制限が厳しすぎます。ユーザーの範囲には、E2 だけでなく、E1、E2、E3 が含まれます。
* D. E1、E2、E3、E4: これは、ユーザーがスコープAとスコープBの両方にアクセスできる場合、または許容モードでスコープ制限が完全に無視される場合にのみ有効です（許容モードではそのようなことはありません）。許容モードでは、SBACルールが引き続き適用され、ユーザーに割り当てられたスコープへのアクセスが制限されます。
正確な抜粋または参照:
Cortex XDRドキュメントポータルでは、SBACについて次のように説明しています。「許可モードでは、スコープベースアクセス制御によって、割り当てられたスコープ内のエンドポイントへのユーザーアクセスが制限され、スコープ権限に応じたデータ可視性が確保されます」（スコープベースアクセス制御セクションからの引用）。EDU-260：Cortex XDRの予防と導入コースでは、SBACの設定について、「許可モードでは、E1、E2、E3など、ユーザーのスコープ内のエンドポイントへのアクセスが許可され、他のスコープ内のエンドポイントへのアクセスは制限されます」（コース資料からの引用）。Palo Alto Networks認定XDREngineerのデータシートには、SBAC設定を含む「導入後の管理と設定」が試験の主要トピックとして記載されています。
参考文献:
Palo Alto Networks Cortex XDR ドキュメント ポータル:https://docs-cortex.paloaltonetworks.com/ EDU-260: Cortex XDR の防止と展開コースの目標 Palo Alto Networks 認定 XDR エンジニア データシート:https://www.paloaltonetworks.com/services/education/認定#xdr-エンジニア

最新問題: **14**
カスタム防止ルールで特定の動作をブロックできるようにするにはどうすればよいでしょうか?
**A.** エージェントブロッキングプロファイルに追加された相関ルール
**B.** エクスプロイトプロファイルに追加されたカスタムの行動指標（BIOC）
**C.** 制限プロファイルに追加されたカスタムの行動指標（BIOC）
**D.** マルウェアプロファイルに追加された相関ルール
**Answer: C (**メーッセージを残す**)**
Cortex XDRでは、カスタム防御ルールを使用して、行動侵害指標（BIOC）を活用し、エンドポイント上の特定の動作やアクティビティをブロックします。BIOCは、特定のプロセス実行、ファイル変更、ネットワークアクティビティなどの動作パターンを定義し、検出された場合には、プロセスのブロックやエンドポイントの隔離などの予防措置をトリガーします。これらのBIOCは通常、制限プロファイルに関連付けられており、一致した動作に対してブロックアクションが適用されます。
* 正解分析 (C): 制限プロファイルにカスタムの行動指標（BIOC）を追加することで、特定の行動をブロックするカスタム防止ルールが有効になります。BIOCは検出する行動（例：機密ファイルにアクセスするプロセス）を定義し、制限プロファイルは予防措置（例プロセスのブロック）を指定します。この設定により、プロファイルが適用されたエンドポイントで、特定された行動が確実にブロックされます。
* 他のオプションを選択しないのはなぜですか?
* A. エージェントブロッキングプロファイルに追加された相関ルール:相関ルールは、データセット全体のイベントを相関させてアラートを生成するために使用されるものであり、動作を直接ブロックするものではありません。
Cortex XDR の 「エージェント ブロッキング プロファイル」。これは誤った名称です。
* B. エクスプロイト プロファイルに追加されたカスタムの行動侵害指標 (BIOC):
エクスプロイトプロファイルは、BIOC によって定義される一般的な動作パターンではなく、エクスプロイトベースの攻撃（例メモリ破損）を検出して防止するために使用されます。BIOC は、動作をブロックするための制限プロファイルに関連付けられています。
* D. マルウェアプロファイルに追加された相関ルール：相関ルールは動作を直接ブロックするのではなく、アラートを生成します。マルウェアプロファイルは、BIOCによる動作ブロックではなく、ファイルベースの脅威（例WildFireで分析された実行ファイル）に重点を置いています。
正確な抜粋または参照:
Cortex XDRドキュメントポータルでは、BIOCと制限プロファイルについて次のように説明しています。 制限プロファイルにカスタムBIOCを追加することで、エンドポイント上の特定の動作をブロックし、カスタマイズされた防止ルールを実現できます」（BIOCと制限プロファイルのセクションからの引用）。EDU-260 :Cortex XDRの防止と展開コースでは、防止ルールについて説明しており、 制限プロファイル内のBIOCにより、エンドポイント上の特定の動作をブロックできます」（コース資料からの引用）。Palo Alto Networks認定XDRエンジニアのデータシートには、BIOC

と防止ルールの設定を含む「検出エンジニアリング」が試験の主要トピックとして記載されています。
参考文献:
Palo Alto Networks Cortex XDR ドキュメント ポータル:https://docs-cortex.paloaltonetworks.com/ EDU-260: Cortex XDR の防止と展開コースの目標 Palo Alto Networks 認定 XDR エンジニア データシート:https://www.paloaltonetworks.com/services/education/認定#xdr-エンジニア

最新問題: **15**
Cortex XDRエージェントを多数のエンドポイントに導入した後、一部のエンドポイントの保護状態が「部分的に保護されている」状態になりました。この状態の原因に関する知見は、どの2つの場所で確認できますか？（2つ選択してください。）
**A.** 管理監査ログ
**B.** エンドポイントデータセットのXQLクエリ
**C.** すべてのエンドポイントページ
**D.** 資産インベントリ
**Answer: B,C** (メーッセージを残す)
Cortex XDRでは、エンドポイントの部分的保護ステータスは、一部のエージェントコンポーネントまたは保護モジュール（マルウェア対策、エクスプロイト防止など）が完全に動作していないことを示します。これは、互換性の問題、前提条件の不足、または構成エラーが原因である可能性があります。このステータスをトラブルシューティングするには、エンジニアはエンドポイントに影響を与えている特定のコンポーネントまたは問題を特定する必要があります。これは、詳細なエンドポイントデータとステータス情報を調べることで実現できます。
* 正解分析（B、C）：
* B. エンドポイントデータセットのXQLクエリ:エンドポイントデータセットに対するXQL (XDRクエリ言語)クエリ(例: データセット = エンドポイント | フィルター エンドポイントステータス = PARTIALLY_PROTECTED」| フィールド endpoint_name、protection_status_details) は、部分的に保護されている状態になった理由に関する詳細な情報を提供します。エンドポイントデータセットには、どのモジュールが機能していないか、またその理由を特定するprotection_status_details などのフィールドが含まれています。
* C. すべてのエンドポイントページ :Cortex XDRコンソールの「すべてのエンドポイント」ページには、部分的に保護されているエンドポイントも含め、すべてのエンドポイントとそのステータスのリストが表示されます。エンドポイントの詳細をクリックすると、無効化されているモジュールや問題が発生しているモジュールなど、保護ステータスに関する具体的な情報が表示され、ステータスの原因を特定するのに役立ちます。
* 他のオプションを選択しないのはなぜですか?

* A. 管理監査ログ: 管理監査ログは管理アクション (ポリシーの変更、エージェントのインストールなど) を追跡しますが、エンドポイントの保護状態や部分的な保護の理由に関する詳細な情報は提供しません。
* D. 資産インベントリ: 資産インベントリでは、資産 (ハードウェア、ソフトウェアなど) の概要が提供されますが、Cortex XDR エージェントの保護状態や部分的な保護の理由については具体的には説明されません。
正確な抜粋または参照:
Cortex XDRドキュメントポータルでは、部分的に保護されたエンドポイントのトラブルシューティングについて次のように説明しています。「[すべてのエンドポイント]ページを使用して詳細な保護ステータスを確認し、エンドポイントデータセットに対してXQLクエリを実行して、部分的に保護されたステータスの原因となっている具体的な問題を特定します」（エンドポイント管理セクションからの引用）。EDU-260：Cortex XDRの予防と展開コースでは、エンドポイントのトラブルシューティングについて取り上げており、「[すべてのエンドポイント]ページとエンドポイントデータセットのXQLクエリは、部分的に保護された問題に関する洞察を提供します」（コース資料からの引用）。Palo Alto Networks認定XDRエンジニアのデータシートには、エンドポイントステータスの調査を含む「メンテナンスとトラブルシューティング」が主要な試験トピックとして記載されています。
参考文献:
Palo Alto Networks Cortex XDR ドキュメント ポータル:https://docs-cortex.paloaltonetworks.com/ EDU-260: Cortex XDR の防止と展開コースの目標 Palo Alto Networks 認定 XDR エンジニア データシート:https://www.paloaltonetworks.com/services/education/認定#xdr-エンジニア

最新問題**: 16**
管理者は、カスタム解析ルール内で再利用可能なルールを適用し、複数のデータソースにわたって一貫したログフィールド抽出を適用したいと考えています。Cortex XDRでこれらの再利用可能なルールを定義するには、解析ルールのどのセクションを使用すればよいですか？
**A.** ルール
**B.** 摂取
**C.** フィルター
**D.** 定数
**Answer: D (**メーッセージを残す**)**
Cortex XDRでは、解析ルールを用いて、様々なソースから取り込んだログデータからフィールドを抽出・正規化し、一貫した分析と相関関係を実現します。複数のデータソース間で一貫性のあるログフィールド抽出を実現する再利用可能なルールを作成するには、管理者は解析ルール設定内のCONSTセクションを使用します。CONSTセクションでは、異なる解析ルールに適用できる再利用可能な定数またはルールを定義できるため、フィールドの抽出と処理方法の一貫性が確保されます。

CONSTセクションは、解析ルールの他の部分（RULEセクションやINGESTセクションなど）で参照できる定数値や再利用可能な式を保持するために特別に設計されています。これは、複数のデータソースで同様のフィールド抽出ロジックが必要な場合に特に便利です。冗長性が削減され、一貫性が確保されるためです。例えば、IPアドレスを抽出するための定数正規表現パターンをCONSTセクションで定義し、複数の解析ルールで再利用することができます。
* 他のオプションを選択しないのはなぜですか?
* RULE: RULE セクションでは、ログ エントリからフィールドを解析および抽出するための特定のロジックを定義しますが、CONST で定義された定数を介して参照されない限り、複数のルール間で本質的に再利用できません。
* INGEST: INGEST セクションでは、再利用可能なルールが定義される場所ではなく、生のログ データが取り込まれ、前処理される方法を指定します。
* FILTER: FILTER セクションは、再利用可能な抽出ルールを定義するためではなく、条件に基づいてログ エントリを含めるか除外するために使用されます。
正確な抜粋または参照:
CONSTセクションの目的の正確な文言は、一般向けドキュメントには直接引用されていません（EDU-260やCortex XDR管理者ガイドなどの独自のトレーニング資料に詳細が記載されているため）。Cortex XDRドキュメントポータル（docs-cortex.paloaltonetworks.com）では、データの取り込みと解析のワークフローについて説明されており、再利用可能な設定のための定数の使用が強調されています。 EDU-260 :Cortex XDRの予防と展開」コースでは、データのオンボーディングと解析について取り上げ、「CONSTセクションで定義された定数は、ソース間で一貫したフィールド抽出のための再利用可能な解析ロジックを可能にします」（コースの目標からの引用）と述べています。さらに、Palo Alto Networks認定XDRエンジニアのデータシートでは、「データソースのオンボーディングと統合設定」が重要なスキルとして挙げられており、これには解析ルールとそのコンポーネント（CONSTなど）の習得が含まれます。
参考文献:
Palo Alto Networks Cortex XDR ドキュメント ポータル:https://docs-cortex.paloaltonetworks.com/ EDU-260: Cortex XDR の防止と展開コースの目標 Palo Alto Networks 認定 XDR エンジニア データシート:https://www.paloaltonetworks.com/services/education/認定#xdr-エンジニア

最新問題: 17
高可用性（HA）環境にブローカーVMを展開する際、ブローカーVMのFQDNを設定した後、XDRエンジニアは、フェイルオーバー間でパフォーマンスの一貫性を維持するために、エージェントインストーラの可用性と効率的なコンテンツキャッシュを確保する必要があります。エンジニアはどのような追加構成手順を実行する必要がありますか？
**A.** すべてのブローカーVMに共有SSL証明書とキーを使用し、フェイルオーバー用に単一のIPアドレスを構成する
**B.** 署名されたSSLサーバ証明書とキーをアップロードし、ロードバランサを展開します。
**C.** ロードバランサを展開し、ロードバランサでSSL終了を構成する
**D.** ブローカーVM間で同期されたセッションの永続性を有効にし、自己署名証明書とキーを使用します。
**Answer: B** (メーッセージを残す)
高可用性（HA）環境では、Cortex XDRのBroker VMがローカルプロキシとして機能し、エージェント通信、コンテンツキャッシュ、インストーラ配信を容易にすることで、クラウドへの直接接続への依存を軽減します。フェイルオーバー時におけるエージェントインストーラの可用性と効率的なコンテンツキャッシュを確保するには、1つのVMに障害が発生した場合でも、Broker VMがエージェント要求を一貫して処理できるように構成する必要があります。そのためには、適切なSSL証明書管理と、複数のBroker VM間でトラフィックを分散するための負荷分散が必要です。
* 正解分析 (B): エンジニアは、通信をセキュリティで保護し、エージェントとブローカー VM 間の信頼を確保するために、署名された SSL サーバー証明書とキーを各ブローカー VM にアップロードする必要があります。
さらに、ブローカーVMのフロントエンドにロードバランサーを配置することで、トラフィックを複数のVMに分散し、フェイルオーバー時の可用性とパフォーマンスの一貫性を確保できます。ロードバランサーは、設定されたブローカーVMのFQDNを使用してエージェント要求をルーティングし、署名付きSSL証明書によって安全で中断のない通信を保証します。この設定により、エージェントへの安定した接続ポイントが維持され、コンテンツのキャッシュとインストーラーの配布がサポートされます。
* 他のオプションを選択しないのはなぜですか?
* A. すべてのBroker VMで共有SSL証明書とキーを使用し、フェイルオーバー用に単一のIPアドレスを設定します。共有SSL証明書を使用することもできますが、フェイルオーバー用に単一のIPアドレスを設定する（VRRPやフローティングIPなど）と、ロードバランサよりも柔軟性が低く、複数のVM間でのコンテンツのキャッシュやインストーラの配布を効率的に処理できない可能性があります。Cortex XDRのHA設定にはロードバランサが推奨されます。
* C. ロードバランサを導入し、ロードバランサでSSLターミネーションを設定する :ロードバランサでSSLターミネーションを設定すると、ロードバランサはトラフィックをブローカーVMに転送する前に復号化するため、ロードバランサとVM間の通信は暗号化されません。ブローカーVMは

セキュリティのためにエンドツーエンドのSSL暗号化を必要とし、SSLターミネーションは証明書管理を複雑にするため、Cortex XDRでは推奨されません。
* D. ブローカー VM 間で同期されたセッションの永続性を有効にし、自己署名証明書とキーを使用します。自己署名証明書は、エージェントとの信頼の問題が発生し、手動での構成が必要になる可能性があるため、運用 HA 環境には推奨されません。
同期されたセッションの永続性は、Broker VM の標準機能ではないため、コンテンツのキャッシュやインストーラーの可用性には必要ありません。
正確な抜粋または参照:
Cortex XDRドキュメントポータルでは、ブローカーVMのHA構成について次のように説明しています。 高可用性を実現するには、ロードバランサーの背後に複数のブローカーVMを展開し、署名済みのSSLサーバー証明書とキーを各VMにアップロードして、エージェントの通信を保護します」（ブローカーVMの展開セクションからの引用）。EDU-260: Cortex XDRの予防と導入コースでは、ブローカーVMのセットアップについて説明し、 署名付きSSL証明書を備えたロードバランサは、HA環境におけるエージェントインストーラの可用性とコンテンツのキャッシュを確保する」と述べています（コース資料より抜粋）。Palo Alto Networks認定XDRエンジニアのデータシートには、
試験の主要トピックとして「計画とインストール」を取り上げ、HA のためのブローカー VM の展開を網羅します。
参考文献:
Palo Alto Networks Cortex XDR ドキュメント ポータル:https://docs-cortex.paloaltonetworks.com/ EDU-260: Cortex XDR の防止と展開コースの目標 Palo Alto Networks 認定 XDR エンジニア データシート:https://www.paloaltonetworks.com/services/education/認定#xdr-エンジニア

最新問題**: 18**
Pathfinder の認証方法として Kerberos を使用する場合、DNS サーバーで検証する必要がある 2 つの設定はどれですか (2 つ選択してください)。
**A.** DNSフォワーダー
**B.** 逆DNSゾーン
**C.** 逆DNSレコード
**D.** AD DS 統合ゾーン
**Answer: B,C (**メーッセージを残す**)**
Cortex XDRのPathfinderは、ネットワーク内の管理対象外エンドポイントを検出するためのツールです。多くの場合、Kerberosなどの認証方式を使用してシステムに安全にアクセスします。Kerberos認証は、ホスト名の解決と、クライアント、サーバー、Kerberos鍵配布センター（KDC）間の適切な通信の確保のために、DNSに大きく依存しています。PathfinderでKerberos認証が正しく機能するには、特定のDNS設定を検証する必要があります。
* 正解分析（B、C）：

* B. 逆DNSゾーン：逆DNSゾーンは、IPアドレスをホスト名（PTRレコード）にマッピングするために必要です。Kerberosは、このPTRレコードを使用してサーバーとクライアントのIDを検証します。逆DNSゾーンが適切に設定されていない場合、ホスト名解決の問題によりKerberos認証が失敗する可能性があります。
* C. 逆引きDNSレコード：逆引きDNSゾーン内の逆引きDNSレコード（PTRレコード）は、関連するすべてのホストに対して正しく設定されている必要があります。これらのレコードは、IPアドレスが正しいホスト名に解決されることを保証します。これは、KerberosがPathfinderのエンドポイントへのアクセスを認証するために不可欠です。
* 他のオプションを選択しないのはなぜですか?
* A. DNSフォワーダー：DNSフォワーダーは、ローカルDNSサーバーがDNSクエリを解決できない場合に、外部サーバーにDNSクエリをルーティングするために使用されます。一般的なDNS解決には役立ちますが、Kerberos認証やPathfinderには特に必要ありません。
* D. AD DS統合ゾーン：Active Directoryドメインサービス（AD DS）統合ゾーンは、AD環境におけるDNS管理を強化しますが、Kerberos認証に必須ではありません。Kerberosは、AD固有のDNS構成ではなく、適切な正引きおよび逆引きDNS解決に依存します。
正確な抜粋または参照:
Cortex XDRドキュメントポータルでは、Pathfinderの設定について次のように説明しています。「Kerberos認証では、DNSサーバーにホスト名解決をサポートする逆引きDNSゾーンと逆引きDNSレコードが適切に設定されていることを確認してください」（Pathfinderの設定セクションからの引用）。EDU-260：Cortex XDRの予防と導入コースでは、Pathfinderの設定について説明しており、「Kerberos認証には有効な逆引きDNSゾーンとPTRレコードが必要です」（コース資料からの引用）。Palo Alto Networks認定XDREngineerのデータシートには、Pathfinderの認証設定を含む「計画とインストール」が試験の主要トピックとして記載されています。
参考文献:
Palo Alto Networks Cortex XDR ドキュメント ポータル:https://docs-cortex.paloaltonetworks.com/ EDU-260: Cortex XDR の防止と展開コースの目標 Palo Alto Networks 認定 XDR エンジニア データシート:https://www.paloaltonetworks.com/services/education/認定#xdr-エンジニア