PaloAltoNetworks.PCDRA.v2024-06-03.q57

試験コード:	PCDRA
試験名称:	Palo Alto Networks Certified Detection and Remediation Analyst
認定資格:	Palo Alto Networks
無料問題数:	57
バージョン:	v2024-06-03
アクセス数:	563
ページビュー数:	570
https://www.jpnpdf.com/PaloAltoNetworks.PCDRA.v2024-06-03.q57-mondaishu.html	

最新問題: **1**
インシデントを直接表示する場合、Cortex に報告されたばかりの新しいインシデントの 割り当て先」フィールドの値は何ですか?
A. 未割り当て
B. 空白です
C. 新規
D. 保留中
Answer: C (メーッセージを残す**)**

最新問題: **2**
セキュリティ イベントに関連する追加の技術サポートについて TAC に問い合わせる場合。エージェントから収集する必要がある 2 つの重要な情報は何ですか? (2つ選択してください)
A. エージェントのテクニカル サポート ファイル。
B. アラートからの予防アーカイブ。
C. エージェントのディストリビューション ID。
D. エージェントに適用されている現在のすべての例外のリスト。
E. 一意のエージェント ID。
Answer: A,B (メーッセージを残す**)**
説明
セキュリティ イベントに関連する追加のテクニカル サポートを求めて TAC に連絡する場合、エージェントから収集する必要がある 2 つの重要な情報は次のとおりです。
* エージェントのテクニカル サポート ファイル。これは、構成、ステータス、ログ、システム情報など、エージェントに関する診断情報が含まれるファイルです。エージェントのテクニカル サポート ファイルは、TAC によるエージェントまたはエンドポイントの問題のトラブルシューティングと解決に役立ちます。エージェントのテクニカル サポート ファイルは、Cortex XDR コンソールまたはエージェント自体から生成およびダウンロードできます。

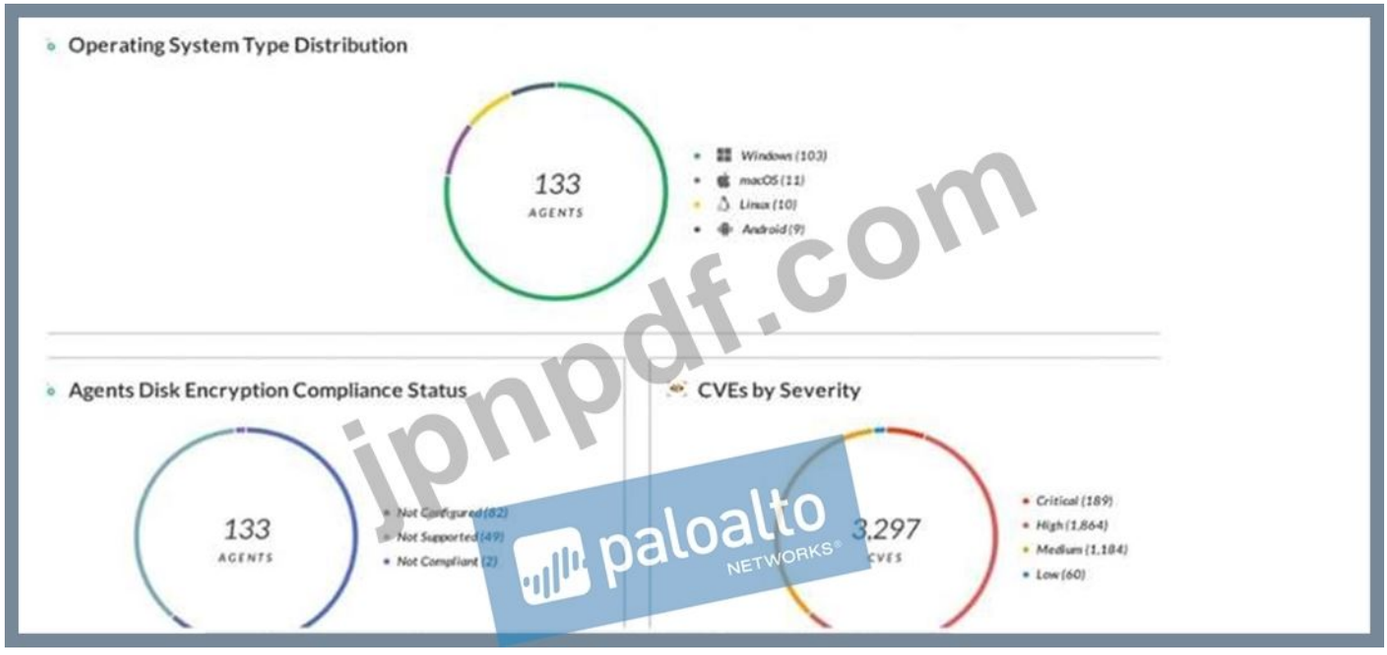
* アラートからの予防アーカイブ。これは、プロセス ツリー、ネットワーク アクティビティ、レジストリの変更、関連ファイルなど、アラートに関連するフォレンジック データが含まれるファイルです。予防アーカイブは、TAC がアラートと悪意のあるアクティビティを分析して理解するのに役立ちます。生成したり、
* Cortex XDR コンソールまたはエージェント自体から防止アーカイブをダウンロードします。
他のオプションは TAC にとって重要な情報ではないため、すべてのセキュリティ イベントに利用できない、または関連しない可能性があります。例えば :
* エージェントのディストリビューション ID は、エージェントがエンドポイントにインストールされるときにエージェントに割り当てられる一意の識別子です。ディストリビューション ID は、TAC がエージェントとそのプロファイルを特定するのに役立ちますが、テクニカル サポートやフォレンジック分析を提供するには十分ではありません。ディストリビューション ID は、Cortex XDR コンソールまたはエージェントのインストール フォルダーで確認できます。
* エージェントに適用される現在のすべての例外のリストは、エージェントのセキュリティ ポリシーから除外されるファイル、プロセス、または動作を定義する一連のルールです。例外は、TAC がエージェントの構成と動作を理解するのに役立ちますが、テクニカル サポートやフォレンジック分析を提供するためには必須ではありません。例外は、Cortex XDR コンソールまたはエージェント構成ファイルで確認できます。
* 一意のエージェント ID は、Cortex XDR に登録するときにエージェントに割り当てられる一意の識別子です。一意のエージェント ID は、TAC がエージェントとそのエンドポイントを識別するのに役立ちますが、テクニカル サポートやフォレンジック分析を提供するには十分ではありません。一意のエージェント ID は、Cortex XDR コンソールまたはエージェント ログ ファイルで確認できます。
参考文献:
* エージェント テクニカル サポート ファイルを生成してダウンロードする
* 予防アーカイブを生成してダウンロードする
* Cortex XDR エージェント管理者ガイド: エージェント配布 ID
* Cortex XDR エージェント管理者ガイド: 例外セキュリティ プロファイル
* [Cortex XDR エージェント管理者ガイド: 固有のエージェント ID]

最新問題**: 3**
アラートの除外を作成して実装すると、どのような結果になりますか?
A. Cortex XDR エージェントは、ブロックされたプロセスがエンドポイントで実行できるようにします。
B. Cortex XDR コンソールはこれらのアラートを削除し、今後のアラートの取り込みをブロックします。
C. Cortex XDR コンソールはこれらのアラートを非表示にします。
D. Cortex XDR エージェントは今後、このイベントのアラートを作成しません。
Answer: C (メーッセージを残す**)**

最新問題: **4**
Cortex XDR Windows エージェントのマルウェア保護フローで最初にチェックされる保護モジュールは次のうちどれですか?
A. ハッシュ判定の決定
B. 行動脅威からの保護
C. 制限ポリシー
D. 子プロセスの保護
Answer: (解答を表示する**)**
Cortex XDR エージェントは、エクスプロイト、マルウェア、ランサムウェア、ファイルレス攻撃に対する最先端の保護を備えた完全な防御スタックを提供します。これには、マルウェア感染につながるエクスプロイトをブロックするために利用できる最も広範なエクスプロイト保護モジュールのセットが含まれています。すべてのファイルは、新しい攻撃手法に対抗する方法を常に学習している、adaptiveAI 主導のローカル分析エンジンによって検査されます。BehavioralThreat Protection エンジンは、複数の関連プロセスの動作を検査して、攻撃が発生したときにそれを発見します。Palo Alto Networks WildFire® マルウェア防御サービスとの統合により、セキュリティの精度と適用範囲が向上します。

最新問題: **5**
ダッシュボードでカスタム XQL クエリを作成する場合、ユーザーはその XQL クエリをウィジェット ライブラリにどのように保存しますか?
A. ダッシュボードで [ウィジェット ライブラリに保存] をクリックすると、クエリの名前と説明を入力するように求められます。
B. これはサポートされていません。作成するには、まずダッシュボードを終了してウィジェット ライブラリに移動する必要があります。
C. ダッシュボードで [アクション センターに保存] をクリックすると、クエリの名前と説明を入力するように求められます。
D. ウィジェット上の 3 つの点をクリックし、[保存] を選択すると、クエリがウィジェット ライブラリにリンクされます。
Answer: A (メーッセージを残す**)**

最新問題: **6**
以下のレポート出力に基づいて正しい記述はどれですか?



A. ホスト インベントリ データ収集が有効になっています。
B. 合計 3,297 件のインシデントが検出されました。
C. フォレンジック インベントリ データ収集が有効になっています。
D. 133 エージェントがフルディスク暗号化を備えています。
Answer: (解答を表示する**)**
説明
レポート出力には、フォレンジック インベントリ データ収集が有効になっているエンドポイントの数が表示されます。これは、エンドポイントのハードウェア、ソフトウェア、およびネットワーク構成に関する詳細情報の収集を可能にする Cortex XDR の機能です。この機能は、エンドポイントの状態とアクティビティの包括的なビューを提供することで、アナリストがインシデントをより効果的に調査して対応できるようにします。フォレンジック インベントリ データの収集は、Cortex XDR のポリシーごとに有効または無効にできます。参考文献:
* フォレンジックインベントリデータ収集
* Cortex XDR 3: エンドポイント保護の入門

最新問題**: 7**
1 つの Broker VM ローカル エージェント アプレットがサポートできるエージェントの最大数はいくつですか?
A. 5,000
B. 10,000
C. 15,000
D. 20,000
Answer: (解答を表示する**)**
説明
Broker VM は、ネットワークに展開して、Cortex XDR エージェントにさまざまなサービスと機能を提供できる仮想マシンです。Broker VM が提供するサービスの 1 つは、ローカル エージェント設定アプレットです。これを使用すると、エージェント プロキシ、エージェント インストーラー、

およびエージェントのコンテンツ キャッシュ設定を構成できます。ローカル エージェント設定アプレットは、ブローカー VM あたり最大 10,000 のエージェントをサポートできます。
ネットワーク内に 10,000 を超えるエージェントがある場合は、追加の Broker VM をデプロイし、それらの間で負荷を分散する必要があります。参考文献:
* Broker VM の概要: このドキュメントでは、Broker VM とその機能、要件、展開オプションの概要を説明します。
* ブローカー VM の構成: このドキュメントでは、ESXi 環境でブローカー VM をインストール、セットアップ、および構成する方法について説明します。
* Cortex XDR 管理コンソールからの Broker VM の管理: このドキュメントでは、Cortex XDR 管理コンソールから Broker VM アプレットをアクティブ化および管理する方法について説明します。

最新問題: **8**
セキュリティ イベントを調査する場合、エンドポイントの変更を元に戻すのに役立つ Cortex XDR の機能はどれですか?
A. 修復の自動化
B. マシンの修復
C. 自動修復
D. 修復の提案
Answer: (解答を表示する**)**
説明
セキュリティ イベントを調査する場合、エンドポイントの変更を元に戻すのに役立つ Cortex XDR の機能は、修復の提案です。修復の提案は、エンドポイントに対する悪意のあるアクティビティの影響を元に戻すための推奨アクションを提供する Cortex XDR の機能です。Cortex XDR コンソールで各アラートまたはインシデントの修復提案を表示し、それらを適用するかどうかを決定できます。修復の提案は、エンドポイントを元の状態に復元したり、悪意のあるファイルやプロセスを削除したり、レジストリやシステム設定を修正したりするのに役立ちます。修復の提案は、Cortex XDR エージェントによって収集されたフォレンジック データと Cortex XDR によって実行された分析に基づいています。参考文献:
* 修復の提案
* 修復提案を適用する

最新問題: **9**
スケジュールされたレポートを作成する場合、オプションではありませんか?
A. 四半期ごとに特定の日時に実行します。
B. 毎週特定の日時に実行します。
C. 毎日特定の時刻 (時間と分を選択可能) に実行します。
D. 毎月特定の日時に実行します。
Answer: A (メーッセージを残す**)**

最新問題: **10**

Windows 用 Cortex XDR エージェントは、ランサムウェア攻撃によるファイル システムの侵害をどのように防ぎますか?
A. 最初にディスクを暗号化します。
B. おとりファイルを利用します。
C. 暗号化キーを取得します。
D. 脆弱なアプリケーションにパッチを適用することによって。
Answer: B (メーッセージを残す)
説明
Windows 用 Cortex XDR エージェントは、おとりファイルを利用してランサムウェア攻撃によるファイル システムの侵害を防ぎます。デコイ ファイルは、ユーザーのデスクトップ、ドキュメント、ピクチャ フォルダーなど、エンドポイント上の戦略的な場所に配置される、ランダムに生成されるファイルです。これらのファイルは、ランサムウェアが暗号化の対象とする貴重なデータのように見えるように設計されています。Cortex XDR エージェントは、プロセスがおとりファイルへのアクセスまたは変更を試みていることを検出すると、ただちにプロセスをブロックし、管理者に警告します。このようにして、Cortex XDR エージェントは、エンドポイント上の実際のファイルに損傷を与える前に、ランサムウェア攻撃を阻止できます。
参考文献:
* ランサムウェア対策保護
* PCDRA 学習ガイド

最新問題**: 11**
ファイルの実行が許可される前に、ファイルを評価するためにローカル分析が呼び出されるのはどのような条件ですか?
A. エンドポイントが切断されているか、WildFire からの判定は良性です。
B. エンドポイントが切断されているか、WildFire からの判定のタイプが不明です。
C. エンドポイントが切断されているか、WildFire からの判定はマルウェアのタイプです。
D. エンドポイントが切断されているか、WildFire からの判定はグレーウェアのタイプです。
Answer: (解答を表示する)
説明
ローカル分析は、分析のためにファイルを WildFire に送信せずに、エージェントがエンドポイント上でローカルにファイルを評価できるようにする Cortex XDR の機能です。ローカル分析は、次の条件が満たされた場合に呼び出されます。
* エンドポイントはインターネットまたは Cortex XDR 管理コンソールから切断されているため、WildFire と通信できません。
* WildFire からの判定は不明なタイプです。これは、WildFire がまだファイルを分析していないか、最終的な判定に達していないことを意味します。
ローカル分析では、機械学習モデルを使用してファイルの動作と特性を評価し、良性、マルウェア、グレーウェアのいずれかの判定を割り当てます。判定がマルウェアまたはグレーウェアの場合、エージェントはファイルの実行をブロックし、Cortex XDR 管理コンソールに報告します。判

定が良性の場合、エージェントはファイルの実行を許可し、Cortex XDR 管理コンソールに報告します。参考文献:
* ローカル分析
* WildFire ファイルの評決

最新問題: **12**
Cortex XDR Pro per Endpoint ライセンスと拡張エンドポイント データが有効になっている Linux エンドポイントから、削除したいファイルが作成された悪意のあるアクティビティが報告されました。ファイルを削除するにはどのような操作を実行できますか?
A. ファイルを自動的に削除するための修復提案を開始します。
B. Cortex XDR コンソールから NFS 接続を開き、ファイルを削除します。
C. Cortex XDR コンソールから X2go を開き、X2go 経由でファイルを削除します。
D. 問題のエンドポイントの問題を手動で修復します。
Answer: D (メーッセージを残す**)**

最新問題: **13**
Cortex XDR を使用しているマルウェア アナリストとして、サーバーの 1 つで Cobalt Strike をダウンロードしようとする試みが阻止されたことを示唆するアラートに気づきました。数日後、あなたは現在進行中の大規模なサプライチェーン攻撃について知ります。Cortex XDR を使用すると、サーバーが攻撃によって侵害されたこと、および Cortex XDR がそれを阻止したことを認識できます。すべてのサーバーに同じ保護を確実に適用するには、どのような手順を実行できますか?
A. すべてのサーバーで DLL 保護を有効にしますが、誤検知が発生する可能性があります。
B. 見つかった悪意のあるファイルの IOC を作成して、その実行を阻止します。
C. アクティビティを認識して防止するための行動脅威防止 (BTP) ルールを作成します。
D. cytool を使用して Behavioral Threat Protection (BTP) を有効にして、攻撃の拡大を防ぎます。
Answer: (解答を表示する**)**

最新問題: **14**
次のエージェント自動アップグレード ウィジェットに基づいて正しいのはどれですか?

A. 合計 689 人の最新エージェントがいます。
B. 保留中ステータスのエージェントが進行中ステータスよりも多くあります。

C. エージェントの自動アップグレードは有効になっていますが、すべてのエンドポイントで有効ではありません。
D. エージェントの自動アップグレードが有効になっていません。
Answer: C (メーッセージを残す**)**

最新問題**: 15**
Cortex XDR で現在利用できる BIOC ルールのタイプはどれですか?
A. スポイト
B. 脅威アクター
C. 発見
D. ネットワーク
Answer: A (メーッセージを残す**)**

最新問題**: 16**
どの Broker VM アプレットの展開で、強力な暗号 SHA256 ベースの SSL 証明書をインストールする必要がありますか?
A. Syslog コレクター
B. エージェント インストーラーとコンテンツ キャッシュ
C. CSV コレクター
D. エージェント プロキシ
Answer: B (メーッセージを残す**)**

最新問題**: 17**
Windows および macOS では、Cortex XDR エージェントがデジタル署名者に基づいたファイルの実行をブロックしないようにする必要があります。歌手に例外を追加する 1 つの方法は何ですか?
A. 制限プロファイルで、ファイル名とパスを実行可能ファイルの許可リストに追加します。
B. 新しいルール例外を作成し、歌手を特性として使用します。
C. 署名者をマルウェア プロファイルの許可リストに追加します。
D. アクション センター ページの許可リストに署名者を追加します。
Answer: C (メーッセージを残す**)**
説明

Windows および macOS でのデジタル署名者に基づくファイルの実行が Cortex XDR エージェントによってブロックされないようにするには、署名者に例外を追加する 1 つの方法は、マルウェア プロファイルの許可リストに署名者を追加することです。マルウェア プロファイルは、エンドポイントでのマルウェアの防止と検出のための設定とアクションを定義するプロファイルです。マルウェア プロファイルを使用すると、マルウェアのスキャンとブロックから除外するファイル、フォルダー、または署名者のリストを指定できます。マルウェア プロファイルの許可リストに署名者を追加すると、その署名者によって署名されたファイルが Cortex XDR エージェントによってブロックされるのを防ぐことができます1。
包括的な説明を提供するために、他のオプションについて簡単に説明します。
A: 制限プロファイルで、ファイル名とパスを実行可能ファイルの許可リストに追加します。これは正しい答えではありません。制限プロファイルの実行可能ファイル許可リストにファイル名とパスを追加しても、Cortex XDR エージェントがデジタル署名者に基づいてファイルの実行をブロックすることは防止されません。制限プロファイルは、エンドポイントでのファイルまたはプロセスの実行を制限するための設定とアクションを定義するプロファイルです。制限プロファイルを使用すると、ファイル名とパスに基づいて許可またはブロックする実行可能ファイルのリストを指定できます。ただし、この方法ではファイルのデジタル署名者が考慮されていないため、ファイル名またはパスが変更された場合は効果がなくなる可能性があります2。
B: 新しいルール例外を作成し、署名者を特性として使用します。これは正しい答えではありません。新しいルール例外を作成し、署名者を特性として使用しても、Cortex XDR エージェントがデジタル署名者に基づいてファイルの実行をブロックすることは妨げられません。ルール例外は、特定の防止ルールまたは BIOC ルールの動作を変更するために作成できる例外です。ルール例外を使用すると、ファイル ハッシュ、プロセス名、IP アドレス、ドメイン名など、例外に適用する特性とアクションを指定できます。ただし、この方法は署名者を特性として使用することをサポートしておらず、すべての防止ルールや BIOC ルールに適用できるわけではありません 3。
D: アクション センター ページの許可リストに署名者を追加します。これは不正解です。アクション センター ページの許可リストに署名者を追加しても、Cortex XDR エージェントはデジタル署名者に基づいてファイルの実行をブロックできます。アクション センター ページは、エンドポイントで実行できるアクション (分離、スキャン、ファイルの収集、スクリプトの実行など) を作成および管理できるページです。アクション センター ページには、署名者を許可リストに追加するオプションがなく、マルウェアの防止または検出機能とは関係ありません4。
結論として、Cortex XDR エージェントが Windows および macOS のデジタル署名者に基づくファイルの実行をブロックしないようにするには、署名者に例外を追加する 1 つの方法は、署名者をマルウェア プロファイルの許可リストに追加することです。この方法を使用すると、信頼された署名者によって署名されたファイルをマルウェアのスキャンとブロックから除外できます。
参考文献:
* 新しいマルウェア セキュリティ プロファイルを追加する
* 新しい制限セキュリティ プロファイルを追加
* ルールの例外を作成する
* アクションセンター

最新問題: **18**
セキュリティ イベントを調査する場合、エンドポイントの変更を元に戻すのに役立つ Cortex XDR の機能はどれですか?
A. マシンの修復
B. 修復の自動化
C. 修復の提案
D. 自動修復
Answer: C (メーッセージを残す**)**

最新問題: **19**
攻撃者は、安全でない場所から macOS に動的ライブラリをロードしようとします。この攻撃を防ぐことができる Cortex XDR モジュールはどれですか?
A. DDL セキュリティ
B. ホットパッチ保護
C. カーネル整合性モニター (KIM)
D. Dylib ハイジャック
Answer: (解答を表示する**)**
説明
正解は D. Dylib Hijacking」です。Dylib ハイジャッキング (ダイナミック ライブラリ ハイジャッキングとも呼ばれます) は、攻撃者が安全でない場所から macOS に悪意のあるダイナミック ライブラリをロードするために使用される手法です。この手法は、アプリケーションの実行時にロードする動的ライブラリを macOS が検索する方法を利用しています。このような攻撃を防ぐために、パロアルトネットワークスは、Cortex XDR プラットフォームの一部として Dylib ハイジャッキング防止機能を提供しています。この機能は、許可されていない場所または安全でない場所から動的ライブラリをロードしようとする試みを検出してブロックするように設計されています1。
包括的な説明を提供するために、他のオプションについて簡単に説明します。
A: DDL セキュリティ: これは正しい答えではありません。DDL セキュリティは、macOS に対する動的ライブラリ読み込み攻撃を防ぐように特別に設計されたものではありません。DDL セキュリティは、Windows システム上の DLL (ダイナミック リンク ライブラリ) ハイジャックからの保護に重点を置いています2。
B: ホット パッチ保護: ホット パッチ保護は、動的ライブラリ読み込み攻撃の防止には直接関係しません。これは、実行時のパッチ適用やメモリ内のコードの変更を防ぐセキュリティ機能であり、高度な攻撃者がセキュリティ対策を回避するためによく使用します3。ホット パッチ保護は貴重なセキュリティ機能ですが、説明したシナリオには直接関係しません。
C: カーネル整合性モニター (KIM): カーネル整合性モニターも正解ではありません。KIM は、macOS カーネルの整合性の監視と保護に重点を置いた Cortex XDR のモジュールです。重要なカーネル コンポーネントへの不正な変更を検出し、防止します4。KIM は macOS のセキュリティ全体において重要な役割を果たしますが、動的ライブラリ読み込み攻撃の防止には特に対応していません。

結論として、Dylib Hijacking は、攻撃者が macOS 上の安全でない場所から動的ライブラリをロードすることの防止に特に対処する Cortex XDR モジュールです。このモジュールを活用することで、組織はセキュリティ体制を強化し、この特定の攻撃ベクトルから保護することができます。
参考文献:
* エンドポイント保護モジュール
* DDL セキュリティ
* ホットパッチ保護
* カーネル整合性モニター

最新問題: **20**
アプリケーションエクスプロイトとカーネルエクスプロイトについて正しいのはどれですか?
A. エクスプロイトの最終目標は、アプリケーションに到達することです。
B. カーネルのエクスプロイトは、アプリケーションのエクスプロイトよりも防ぐのが簡単です。
C. エクスプロイトの最終目標は、カーネルに到達することです。
D. アプリケーションのエクスプロイトはカーネルの脆弱性を利用します。
Answer: C (メーッセージを残す**)**
説明
エクスプロイトの最終目標は、最高レベルの特権とハードウェア リソースへのアクセスを持つオペレーティング システムのコア コンポーネントであるカーネルに到達することです。アプリケーションエクスプロイトは、Web ブラウザー、電子メールクライアント、オフィススイートなどの特定のアプリケーションの脆弱性を狙う攻撃です。カーネルエクスプロイトは、メモリ破損、権限昇格、コード実行など、カーネル自体の脆弱性を標的とする攻撃です。カーネル エクスプロイトは、セキュリティ メカニズムをバイパスし、その存在をユーザーやシステムから隠すことができるため、アプリケーション エクスプロイトよりも防止および検出することが困難です。
参考文献:
* Palo Alto Networks Certified Detection and Remediation Analyst (PCDRA) スタディ ガイド、8 ページ
* Palo Alto Networks Cortex XDR ドキュメント、エクスプロイト保護の概要

最新問題: **21**
スケジュールされたレポートを作成する場合、オプションではありませんか?
A. 毎週特定の日時に実行します。
B. 四半期ごとに特定の日時に実行します。
C. 毎月特定の日時に実行します。
D. 毎日特定の時刻 (時間と分を選択可能) に実行します。
Answer: B (メーッセージを残す**)**
説明
Cortex XDR でスケジュールされたレポートを作成する場合、四半期ごとに特定の日時に実行するオプションは使用できません。レポートのスケジュールは、毎日、毎週、または毎月実行するようにのみ設定できます。レポートの開始日と終了日、タイムゾーン、受信者を指定することもできま

す。スケジュールされたレポートは、ネットワーク内のセキュリティ イベント、インシデント、アラート、またはエンドポイントに関する定期レポートを生成するのに役立ちます。スケジュールされたレポートは、Cortex XDR コンソールの [レポート] ページから、またはクエリ センターからクエリをレポートとして保存して作成できます。
参考文献:
* レポートの実行またはスケジュール設定
* スケジュールされたレポートを作成する

最新問題: **22**
BIOC ルールを作成する場合、どの XQL クエリを使用できますか?
A. データセット = xdr_data
| フィルターevent_sub_type = PROCESS_STARTおよび
アクションプロセスイメージ名 ~= ".*?\.(?:pdf|docx)\.exe"
B. データセット = xdr_data
| フィルターevent_type = PROCESSおよび
events_sub_type = PROCESS_START および
アクションプロセスイメージ名 ~= ".*?\.(?:pdf|docx)\.exe"
C. データセット = xdr_data
| フィルターアクションプロセスイメージ名 ~= ".*?\.(?:pdf|docx)\.exe"
| フィールド action_process_image
D. データセット = xdr_data
| フィルターイベント動作 = true
events_sub_type = PROCESS_START および
アクションプロセスイメージ名 ~= ".*?\.(?:pdf|docx)\.exe"
Answer: (解答を表示する**)**
説明
BIOC ルールは、Cortex Query Language (XQL) を使用して潜在的な脅威を示す動作またはアクションを定義するカスタム検出ルールです。BIOC ルールでは、xdr_data および cloud_audit_log データセットと、これらのデータセットのプリセットを使用できます。BIOC ルールでは、XQL クエリで集計を行わずにフィルター ステージ、変更ステージ、および関数を使用することもできます。クエリは、action_process_image という名前の単一フィールドを返す必要があります。これは、疑わしいプロセスのプロセス イメージ名です。クエリには、ルールをトリガーするイベントのタイプとサブタイプを指定するために、フィルター ステージにevent_typeフィールドとevent_sub_typeフィールドも含める必要があります。
オプション B は、有効な BIOC ルール クエリの要件をすべて満たしているため、正解です。xdr_data データセット、フィルター ステージ、event_type フィールドとevent_sub_type フィールド、および action_process_image_name フィールドを正規表現とともに使用して、次で終わるプロセス イメージ名と一致します。
.pdf.exe または .docx.exe。悪意のあるファイルの一般的な指標です。

オプション A は、BIOC ルール クエリに必須であるフィルター ステージのevent_type フィールドが含まれていないため、不正解です。
オプション C は、フィルター ステージにevent_type フィールドとevent_sub_type フィールドが含まれておらず、BIOC ルール クエリではサポートされていないフィールド ステージを使用しているため、不正解です。また、action_process_image_name フィールドの代わりに action_process_image フィールドも返します。これは、BIOC ルール クエリの予期される出力です。
オプション D は、BIOC ルール クエリではサポートされていないevent_behavior フィールドを使用しているため、不正解です。また、フィルターステージにevent_typeフィールドが含まれておらず、event_sub_typeフィールドが誤って使用されています。
events_sub_type フィールドは、true ではなく、PROCESS_START と等しい必要があります。
参考文献:
* BIOC の操作
* Cortex クエリ言語 (XQL) リファレンス

最新問題**: 23**
ネットワークベースの攻撃を阻止するには、攻撃パターンの一部に干渉するだけで攻撃の成功を阻止できます。Cortex XDR Analytics モジュールに関して正しい記述はどれですか?
A. エンドポイント上のパターンのどの部分にも干渉しません。
B. ファイアウォールによって監視されるとすぐにパターンに干渉します。
C. 攻撃を防ぐためにパターンのどの部分にも干渉する必要はありません。
D. エンドポイントで観察されるとすぐにパターンに干渉します。
Answer: D (メーッセージを残す**)**
説明
Cortex XDR Analytics モジュールに関する正しい記述は D です。これは、エンドポイントで観察されるとすぐにパターンに干渉します。Cortex XDR Analytics モジュールは、機械学習と動作分析を使用してエンドポイントに対するネットワークベースの攻撃を検出および防止する Cortex XDR の機能です。Cortex XDR Analytics モジュールは、エンドポイント上のネットワーク トラフィックとアクティビティを分析し、パロアルトネットワークスの脅威調査チームによって定義された攻撃パターンと比較します。Cortex XDR Analytics モジュールは、エンドポイントで攻撃パターンが検出されるとすぐに、悪意のあるネットワーク接続、プロセス、またはファイルをブロックすることで攻撃パターンを阻止します。このようにして、Cortex XDR Analytics モジュールは、損害や侵害が発生する前に攻撃を阻止できます。
他の記述は、次の理由により正しくありません。
* A は不正解です。Cortex XDR Analytics モジュールは、悪意のあるネットワーク接続、プロセス、またはファイルをブロックすることで、エンドポイントの攻撃パターンに干渉します。Cortex XDR Analytics モジュールは、攻撃を阻止するためにファイアウォールやその他のネットワーク デバイスに依存せず、エンドポイントにインストールされた Cortex XDR エージェントを使用して干渉を実行します。

* B は不正解です。Cortex XDR Analytics モジュールは、ファイアウォールによって監視されるとすぐには攻撃パターンに干渉しません。Cortex XDR Analytics モジュールは、ファイアウォールやその他のネットワーク デバイスに依存せず、攻撃の検出や防御を行いますが、エンドポイントにインストールされている Cortex XDR エージェントを使用して分析と干渉を実行します。攻撃者によって攻撃パターンが暗号化、難読化、またはバイパスされている場合、ファイアウォールは攻撃パターンを監視またはブロックできない可能性があります。
* C は不正解です。攻撃を防ぐには、Cortex XDR Analytics モジュールが攻撃パターンに干渉する必要があるからです。Cortex XDR Analytics モジュールは、攻撃パターンを検出するだけでなく、悪意のあるネットワーク接続、プロセス、またはファイルをブロックすることで攻撃の成功を阻止します。Cortex XDR Analytics モジュールは、攻撃を阻止するために他の応答メカニズムや人間の介入に依存せず、エンドポイントにインストールされた Cortex XDR エージェントを使用して干渉を実行します。
参考文献:
* Cortex XDR 分析モジュール
* Cortex XDR 分析モジュールの検出と防止

最新問題**: 24**
インシデントを直接表示する場合、Cortex に報告されたばかりの新しいインシデントの 「割り当て先」フィールドの値は何ですか?
A. 保留中
B. 空白です
C. 未割り当て
D. 新規
Answer: C (メーッセージを残す**)**
説明
Cortex に報告されたばかりの新しいインシデントの 「割り当て先」フィールドの値は 「未割り当て」です。これは、インシデントがまだどのアナリストにもグループにも割り当てられておらず、誰かがインシデントの所有権を取得するのを待っていることを意味します。 「担当者」フィールドは、インシデント レイアウトに表示されるデフォルト フィールドの 1 つで、インシデント リスト内のインシデントをフィルタリングおよび並べ替えるのに使用できます。 「割り当て先」フィールドは、アナリストが手動で変更することも、プレイブックやルールによって自動的に変更することもできます12。
包括的な説明を提供するために、他のオプションについて簡単に説明します。
A: 保留中: これは正しい答えではありません。保留中は、 「担当者」フィールドの有効な値ではありません。保留中は、インシデントの現在の状態を示す 「ステータス」フィールドの可能な値です。ステータス フィールドには、 「新規」、 「アクティブ」、 「完了」、 「クローズ」、または 「保留中」などの値を設定できます3。
B: 空白です: これは正しい答えではありません。どのインシデントでも 「担当者」フィールドが空白になることはありません。プレイブックまたはルールによって特定のアナリストまたはグルー

プに割り当てられていない限り、新しいインシデントのデフォルト値は常に 未割り当て」になります12。
D: 新しい: これは正しい答えではありません。New は、 担当者」フィールドの有効な値ではありません。New は、インシデントの現在の状態を示す ステータス」フィールドの値です。ステータス フィールドには、 新規」、 アクティブ」、 完了」、 クローズ」、または 保留中」などの値を設定できます3。
結論として、Cortex に報告されたばかりの新しいインシデントの 割り当て先」フィールドの値は 未割り当て」です。
このフィールドは、インシデントの所有権と責任を管理するために使用でき、手動または自動で変更できます。
参考文献:
* Cortex XDR Pro 管理者ガイド: インシデントの管理
* Cortex XDR Pro 管理者ガイド: インシデントの割り当て
* Cortex XDR Pro 管理者ガイド: インシデント ステータスの更新

最新問題**: 25**
wss (WebSocket Secure) プロトコルはいつ使用されますか?
A. Cortex XDR エージェントが新しいセキュリティ コンテンツをダウンロードするとき
B. Cortex XDR エージェントがアラート データをアップロードするとき
C. Cortex XDR エージェントが WildFire に接続して分析用のファイルをアップロードするとき
D. Cortex XDR エージェントが双方向通信チャネルを確立するとき
Answer: D (メーッセージを残す**)**
説明
WSS (WebSocket Secure) プロトコルは、インターネット上で安全な通信チャネルを提供する WebSocket プロトコルの拡張機能です。これは、クライアント (この場合は Cortex XDR エージェント) とサーバー (Cortex XDR 管理コンソールやその他のコンポーネントなど) の間に永続的な全二重通信チャネルを確立するために使用されます。Cortex XDR エージェントは、WSS プロトコルを使用して、Cortex XDR 管理コンソールまたはパロアルトネットワーク セキュリティ エコシステム内の他のコンポーネントとの安全でリアルタイムの双方向通信チャネルを確立します。この通信チャネルを使用すると、エージェントはセキュリティ イベント、アラート、その他の関連情報などのデータを管理コンソールに送信し、コマンド、ポリシーの更新、および応答を受信できます。WSS プロトコルを使用することにより、Cortex XDR エージェントは管理コンソールとの永続的な接続を維持できるため、セキュリティ関連情報のタイムリーな通信が可能になり、効率的なインシデント対応と修復アクションが可能になります。質問で言及されている他のオプションにも CortexXDR エージェントとさまざまなコンポーネント間の通信が含まれることに注意することが重要ですが、WSS プロトコルの使用については特に言及されていません。例えば :
* A: 新しいセキュリティ コンテンツをダウンロードする Cortex XDR エージェントは通常、HTTP や HTTPS などのプロトコルを利用します。

* B: Cortex XDR エージェントがアラート データをアップロードするとき、データを安全に送信するために HTTP や HTTPS などのプロトコルを使用する場合があります。
* C: Cortex XDR エージェントが WildFire に接続して分析用のファイルをアップロードする場合、通常は HTTP や HTTPS などのプロトコルを使用します。したがって、Cortex XDR エージェントが双方向通信チャネルを確立する場合、正解は D です。参考文献:
* デバイス通信プロトコル - AWS IoT Core
* WebSocket - ウィキペディア
* パロアルトネットワークス認定検出および修復アナリスト (PCDRA) - パロアルトネットワークス
※【WebSocketとは何ですか？| Webセキュリティアカデミー】
* [Palo Alto Networks Certified Detection and Remediation Analyst PCDRA 認定試験の練習問題と解答 (Q&A) ダンプは、詳細な説明と参考資料が無料で提供されており、Palo Alto Networks Certified Detection and Remediation Analyst PCDRA 試験に合格し、Palo Alto Networks Certified Detection を取得するのに役立ちます。および修復アナリスト PCDRA 認定。]

最新問題**: 26**
Cortex XDR Pro per Endpoint ライセンスと拡張エンドポイント データが有効になっている Linux エンドポイントから、削除したいファイルが作成された悪意のあるアクティビティが報告されました。ファイルを削除するにはどのような操作を実行できますか?
A. 問題のエンドポイントの問題を手動で修復します。
B. Cortex XDR コンソールから X2go を開き、X2go 経由でファイルを削除します。
C. ファイルを自動的に削除するための修復提案を開始します。
D. Cortex XDR コンソールから NFS 接続を開き、ファイルを削除します。
Answer: (解答を表示する**)**
説明
Linux エンドポイント上のファイルを削除するための最善のアクションは、Cortex XDR コンソールから修復提案を開始することです。修復の提案は、エンドポイントに対する悪意のあるアクティビティの影響を元に戻すための推奨アクションを提供する Cortex XDR の機能です。Cortex XDR コンソールで各アラートまたはインシデントの修復提案を表示し、それらを適用するかどうかを決定できます。修復の提案は、エンドポイントを元の状態に復元したり、悪意のあるファイルやプロセスを削除したり、レジストリやシステム設定を修正したりするのに役立ちます。修復の提案は、Cortex XDR エージェントによって収集されたフォレンジック データと Cortex XDR によって実行された分析に基づいています。
他のオプションは次の理由により正しくありません。
* A は不正解です。エンドポイントの問題を手動で修復することは、ファイルを削除する便利な方法でも効率的な方法でもないからです。問題を手動で修復するには、エンドポイントに直接アクセスし、root としてログインし、ファイルを見つけて削除する必要があります。また、エンドポイントにアクセスするために必要な権限と資格情報を持っていること、ファイルの正確なパスと名前を知っていることも必要になります。

問題を手動で修復しても、監査証跡や削除の確認は得られません。
* B は不正解です。Cortex XDR コンソールから X2go を開くことは、サポートされていない、または安全なファイル削除方法ではありません。X2go は、グラフィカル ユーザー インターフェイスから Linux エンドポイントにアクセスできるようにするサードパーティのリモート デスクトップ ソフトウェアです。ただし、X2go は Cortex XDR と統合されていないため、X2go を使用するには、Cortex XDR コンソールとエンドポイントの両方に X2go をインストールして構成する必要があります。また、X2go を使用すると、エンドポイントがネットワーク攻撃や不正アクセスにさらされる可能性があり、監査証跡や削除の確認は提供されません。
* D は不正解です。Cortex XDR コンソールから NFS 接続を開くことは、ファイルを削除するための実行可能または信頼できる方法ではないためです。NFS は、リモート サーバー上のファイルにローカルであるかのようにアクセスできるようにするネットワーク ファイル システム プロトコルです。ただし、NFS は Cortex XDR と統合されていないため、NFS を使用するには、Cortex XDR コンソールとエンドポイントの両方で NFS サーバーとクライアントをセットアップして維持する必要があります。NFS の使用はネットワークの可用性とパフォーマンスにも依存し、監査証跡や削除の確認は提供されません。
参考文献:
* 修復の提案
* 修復提案を適用する

最新問題: **27**
Broker VM のインストールに推奨される標準インストール ディスク容量はどれくらいですか?
A. 1GB のディスク容量
B. 256GB のディスク容量
C. 2GB のディスク容量
D. 512GB のディスク容量
Answer: D (メーッセージを残す**)**

最新問題: **28**
サードパーティのファイアウォール ログを Cortex Data Lake に取り込むには、Broker VM のどの機能を使用しますか?
A. Netflow コレクター
B. Syslog コレクター
C. DB コレクター
D. パスファインダー
Answer: B (メーッセージを残す**)**
説明
Broker VM は、サードパーティ データ ソースと Cortex Data Lake の間のデータ ブローカーとして機能する仮想マシンです。syslog、netflow、データベース、パスファインダーなど、さまざまな種類のデータを取り込むことができます。Broker VM の Syslog Collector 機能を使用すると、ファイアウォール、ルーター、スイッチ、サーバーなどのサードパーティ デバイスから syslog メッセー

ジを受信し、Cortex Data Lake に転送できます。Syslog コレクターは、Cortex Data Lake に送信する前に syslog メッセージをフィルター、解析、強化するように構成できます。Syslog Collector を使用して、Cisco、Fortinet、Check Point などのサードパーティ ファイアウォール ベンダーから Cortex Data Lake にログを取り込むこともできます。これにより、Cortex XDR はファイアウォール ログを分析し、ネットワーク境界全体の可視性と脅威検出を提供できるようになります。参考文献:
* Cortex XDR データ ブローカー VM
* Syslog コレクター
* サポートされているサードパーティ ファイアウォール ベンダー

最新問題: **29**
Windows および macOS では、Cortex XDR エージェントがデジタル署名者に基づいたファイルの実行をブロックしないようにする必要があります。歌手に例外を追加する 1 つの方法は何ですか?
A. 署名者をマルウェア プロファイルの許可リストに追加します。
B. アクション センター ページの許可リストに署名者を追加します。
C. 新しいルール例外を作成し、歌手を特性として使用します。
D. 制限プロファイルで、ファイル名とパスを実行可能ファイルの許可リストに追加します。
Answer: A (メーッセージを残す**)**

最新問題: **30**
Cortex XDR の次のエンジンのうち、各アラートで最も関連性の高いアーティファクトを特定し、イベントに関連するすべてのアラートを 1 つのインシデントに集約するのはどれですか?
A. センサー エンジン
B. 因果関係分析エンジン
C. ログステッチングエンジン
D. 因果関係チェーン エンジン
Answer: B (メーッセージを残す**)**
説明
各アラートで最も関連性の高いアーティファクトを特定し、イベントに関連するすべてのアラートをインシデントに集約するエンジンは、因果関係分析エンジンです。因果関係分析エンジンは、エンドポイント、ネットワーク、クラウドなどのさまざまなソースから収集されたデータに対して高度な分析を実行する Cortex XDR のコア コンポーネントの 1 つです。因果関係分析エンジンは、機械学習と動作分析を使用して、根本原因、攻撃チェーン、各アラートの影響を特定します。また、アラート間の時間的および論理的な関係に基づいて、関連するアラートをインシデントにグループ化します。因果関係分析エンジンは、アラートやインシデントのノイズと複雑さを軽減し、攻撃ストーリーの明確かつ簡潔なビューを提供します12。
包括的な説明を提供するために、他のオプションについて簡単に説明します。
A: センサー エンジン: これは正しい答えではありません。センサー エンジンは、各アラートで最も関連性の高いアーティファクトを特定したり、イベントに関連するすべてのアラートをインシ

デントに集約したりする責任を負いません。センサー エンジンは、エンドポイントにインストールされた Cortex XDR エージェント上で実行されるコンポーネントです。センサー エンジンは、プロセス、ファイル、レジストリ キー、ネットワーク接続、ユーザー アクティビティなどのエンドポイント データを収集および分析します。また、センサー エンジンはエンドポイント セキュリティ ポリシーを適用し、予防および対応アクションを実行します3。
C: ログステッチングエンジン: これは正しい答えではありません。ログ結合エンジンは、各アラートで最も関連性の高いアーティファクトを特定したり、イベントに関連するすべてのアラートをインシデントに集約したりする責任を負いません。ログ ステッチング エンジンは、Cortex XDR のクラウドベースのデータ ストレージおよび処理プラットフォームである Cortex Data Lake 上で実行されるコンポーネントです。ログ ステッチング エンジンは、ファイアウォール、プロキシ、エンドポイント、クラウドなどのさまざまなソースからのデータを正規化し、結合します。ログ ステッチング エンジンにより、Cortex XDR は複数のソースからのデータを関連付けて分析し、ネットワーク アクティビティと脅威の状況を統合したビューを提供できるようになります4。
D: 因果関係連鎖エンジン: これは正しい答えではありません。Causality Chain Engine は、Cortex XDR エンジンのいずれに対しても有効な名前ではありません。Cortex XDR には、各アラートで最も関連性の高いアーティファクトを特定し、イベントに関連するすべてのアラートをインシデントに集約する機能を実行するエンジンはありません。
結論として、因果関係分析エンジンは、各アラートで最も関連性の高いアーティファクトを特定し、イベントに関連するすべてのアラートを 1 つのインシデントに集約するエンジンです。Cortex XDR は、因果関係分析エンジンを使用することで、包括的かつ正確な検出および対応機能をセキュリティ アナリストに提供できます。
参考文献:
* Cortex XDR Pro 管理者ガイド: 因果関係分析エンジン
* Cortex XDR Pro 管理者ガイド: インシデントの詳細の表示
* Cortex XDR Pro 管理者ガイド: センサー エンジン
* Cortex XDR Pro 管理者ガイド: ログ ステッチング エンジン

最新問題**: 31**
脆弱性を表示するのに最適な可視性を提供するモジュールはどれですか?
A. フォレンジックモジュール
B. デバイス制御違反モジュール
C. ホスト インサイト モジュール
D. ライブターミナルモジュール
Answer: C (メーッセージを残す**)**

最新問題: 32
Cortex XDR Windows マルウェア プロファイルの 悪意のある因果関係チェーンへの対応」の 2 つの目的は何ですか? (2つお選びください。)
A. 悪意のあるトラフィックに関係する接続を自動的に閉じます。
B. 悪意のあるアクティビティに関与するプロセスを自動的に強制終了します。
C. 悪意のあるアクティビティに関与するスレッドを自動的に終了します。
D. 悪意のあるトラフィックに関与する IP アドレスを自動的にブロックします。
Answer: A,D (メーッセージを残す)
参照：
%20脅威%20保護%2C%20、出現%20正当%20if%20検査%20個別

最新問題: 33
Live Terminal は、エンドポイント上のエージェントとの通信にどのタイプのプロトコルを使用しますか?
A. NetBIOS over TCP
B. WebSocket
C. UDP とランダム ポート
D. TCP、ポート 80 経由
Answer: B (メーッセージを残す)
説明
Live Terminal は、WebSocket プロトコルを使用してエンドポイント上のエージェントと通信します。WebSocket は、単一の TCP 接続を介してクライアントとサーバー間の双方向データ交換を可能にする全二重通信プロトコルです。WebSocket は Web ブラウザおよび Web サーバーに実装されるように設計されていますが、任意のクライアントまたはサーバー アプリケーションで使用できます。WebSocket は、Cortex XDR コンソールとエンドポイントの間に永続的な接続を提供し、コマンドを実行してリアルタイムで応答を受信できるようにします。
Live Terminal は、WebSocket 通信にポート 443 を使用します。これは、HTTPS トラフィックに使用されるポートと同じです。
参考文献:
* ライブターミナルセッションを開始する
* ウェブソケット

最新問題: 34
Cortex XDR が企業内に展開されており、進行中のサプライ チェーン侵害によるコバルト ストライク攻撃が 1 台のサーバーで阻止されたことがわかります。すべてのサーバーに同じ保護を確実に適用するには、どのような手順を実行できますか?
A. 徹底的なエンドポイント マルウェア スキャンを実行します。

B. すべてのサーバーで DLL 保護を有効にしますが、誤検知が発生する可能性があります。
C. cytool を使用して Behavioral Threat Protection (BTP) を有効にして、攻撃の拡大を防ぎます。
D. 発見した悪意のあるファイルの IOC を作成して、その実行を阻止します。
Answer: D (メーッセージを残す)
説明
すべてのサーバーに同じ保護を確実に適用するための最良の手順は、見つかった悪意のあるファイルの侵害インジケータ (IOC) を作成して、その実行を阻止することです。IOC は、ファイル ハッシュ、IP アドレス、ドメイン名、レジストリ キーなど、エンドポイント上の潜在的な脅威や侵害を示す情報です。Cortex XDR で IOC を作成し、IOC に一致するファイルまたはネットワーク アクティビティをブロックまたは警告できます。コバルト ストライク攻撃に関与する悪意のあるファイルの IOC を作成することで、それらのファイルがサーバー上で実行または拡散するのを防ぐことができます。
他のオプションは、次の理由から最適な手順ではありません。
* 悪意のあるファイルが難読化、暗号化、または隠蔽されている場合、徹底的なエンドポイント マルウェア スキャンを実行してもコバルト ストライク攻撃を検出または防止できない可能性があるため、A は最善の手順ではありません。エンドポイント マルウェア スキャンは、エンドポイントで既知のマルウェアをスキャンし、見つかった悪意のあるファイルを隔離できる Cortex XDR の機能です。ただし、エンドポイント マルウェア スキャンは、検出を回避する回避技術を使用する未知の脅威や高度な脅威に対しては効果的ではない可能性があります。
* すべてのサーバーで DLL 保護を有効にすると、誤検知が発生し、正規のアプリケーションが中断される可能性があるため、B は最善の手順ではありません。DLL 保護は、Cortex XDR の機能で、署名されていない DLL、ネットワーク上の場所からロードされた DLL、特定のプロセスによってロードされた DLL など、特定の条件に一致する DLL ロード アクティビティをブロックまたはアラートできるようにします。ただし、DLL 保護は、通常のシステムまたはアプリケーション操作の一部である無害な DLL 読み込みアクティビティをブロックまたは警告することもあり、その結果、誤検知やパフォーマンスの問題が発生することがあります。
* 悪意のあるファイルがすでにエンドポイント上にある場合、または攻撃が検出を回避するために他の方法を使用している場合、cytool で Behavioral Threat Protection (BTP) を有効にしても攻撃の拡散を防ぐことができない可能性があるため、C は最良のステップではありません。Behavioral Threat Protection は、ランサムウェア、認証情報の盗難、横方向の移動など、特定のパターンに一致するエンドポイントの動作をブロックまたは警告できるようにする Cortex XDR の機能です。Cytool は、エンドポイント上で Cortex XDR エージェントを構成および管理できるコマンドライン ツールです。ただし、悪意のあるファイルがすでにエンドポイント上に存在する場合、または攻撃が暗号化、難読化、プロキシ サーバーなどの他の方法を使用して検出を回避している場合、行動脅威防御は攻撃の拡散を防ぐことができない可能性があります。
参考文献:
* IOC を作成する
* エンドポイントでマルウェアをスキャンする
* DLL 保護

* 行動脅威からの保護
* Windows 用 Cytool

最新問題**: 35**
42部隊の目的は何ですか？
A. Unit 42 は、脅威調査、マルウェア分析、脅威ハンティングを担当します。
B. ユニット 42 は製品の自動化とオーケストレーションを担当します
C. ユニット 42 は、Cortex XDR エージェントの迅速な展開を担当します。
D. ユニット 42 は、Cortex XDR サーバーの構成の最適化を担当します。
Answer: A (メーッセージを残す**)**

最新問題**: 36**
ライブターミナルセッションではどのような種類のアクションを実行できますか?
A. ネットワーク構成の管理、ファイルの隔離、PowerShell スクリプトの実行
B. プロセスの管理、ファイルの管理、オペレーティング システム コマンドの実行、Ruby コマンドとスクリプトの実行
C. パッチの適用、システムの再起動、エンド ユーザーへの通知の送信、Python コマンドとスクリプトの実行
D. プロセスの管理、ファイルの管理、オペレーティング システム コマンドの実行、Python コマンドとスクリプトの実行
Answer: (解答を表示する**)**
説明
ライブ ターミナル セッションは、Cortex XDR コンソールからエンドポイントにリモートでアクセスして制御できるようにする Cortex XDR の機能です。ライブ ターミナル セッションを使用すると、エンドポイントで次のようなさまざまなアクションを実行できます。
* プロセスの管理: エンドポイント上のプロセスを表示、開始、または強制終了し、CPU とメモリの使用状況を監視できます。
* ファイルの管理: エンドポイント上のファイルとフォルダーを表示、作成、削除、または移動したり、エンドポイントとの間でファイルをアップロードまたはダウンロードしたりできます。
* オペレーティング システム コマンドの実行: Windows の cmd.exe、Linux の bash、macOS の zsh など、オペレーティング システムのネイティブ コマンド ライン インターフェイスを使用して、エンドポイントでコマンドを実行できます。
* Python コマンドとスクリプトの実行: Cortex XDR エージェントに埋め込まれた Python インタープリターを使用して、エンドポイントで Python コマンドとスクリプトを実行できます。Python コマンドとスクリプトを使用して、エンドポイントで高度なタスクや自動化を実行できます。
参考文献:
* ライブターミナルセッションを開始する
* プロセスの管理
* ファイルの管理

* オペレーティング システム コマンドを実行する
* Python コマンドとスクリプトを実行する

最新問題: **37**
Cortex XDR Prevent ライセンスでは、どのオブジェクトがセンサーとみなされますか?
A. Syslog サーバー
B. サードパーティのセキュリティ デバイス
C. Cortex XDR エージェント
D. パロアルトネットワークスの次世代ファイアウォール
Answer: C (メーッセージを残す**)**
説明
Cortex XDR Prevent ライセンスを持つセンサーとみなされるオブジェクトは、Cortex XDR エージェントとパロアルトネットワークスの次世代ファイアウォールです。これらは、Cortex XDR が脅威の検出と対応のために収集および分析できる 2 つのデータ ソースです。Cortex XDR エージェントは、Windows、Linux、Mac デバイスなどのエンドポイントで実行されるソフトウェア コンポーネントであり、マルウェア、エクスプロイト、ファイルレス攻撃に対する保護を提供します。Cortex XDR エージェントは、プロセス アクティビティ、ネットワーク トラフィック、レジストリの変更、ユーザー アクションなどのエンドポイント データを収集し、分析と関連付けのために Cortex Data Lake に送信します。パロアルトネットワークスの次世代ファイアウォールは、ネットワーク トラフィックの可視性と制御を提供し、アプリケーション、ユーザー、コンテンツに基づいてセキュリティ ポリシーを適用するネットワーク セキュリティ デバイスです。次世代ファイアウォールは、分析と関連付けのために、ファイアウォール ログ、DNS ログ、HTTP ヘッダー、WildFire 判定などのネットワーク データを収集し、Cortex Data Lake に送信します。Cortex XDR エージェントと次世代ファイアウォールの両方からのデータを統合することで、Cortex XDR は攻撃対象領域の包括的なビューを提供し、ネットワーク層とエンドポイント層全体の脅威を検出できます。参考文献:
* Cortex XDR Prevent ライセンス
* Cortex XDR エージェントの機能
* 次世代ファイアウォール機能

最新問題: **38**
一度に複数のインシデントを選択する場合、ユーザーがインシデントを右クリックするとメニューからどのようなオプションが利用可能ですか? (2つお選びください。)
A. インシデントをアナリストに一括で割り当てます。
B. 複数のインシデントのステータスを変更します。
C. 複数のインシデントを一度に調査します。
D. 選択したインシデントを削除します。
Answer: (解答を表示する**)**
説明

一度に複数のインシデントを選択する場合、ユーザーがインシデントを右クリックしたときにメニューから使用できるオプションは、「アナリストにインシデントを一括で割り当てる」と「複数のインシデントのステータスを変更する」です。これらのオプションを使用すると、ユーザーは、選択したインシデントに対して、特定のアナリストに割り当てたり、ステータスをオープン、進行中、解決済み、または終了に変更したりするなど、一括アクションを実行できます。これらのオプションは、ユーザーがインシデントをより効率的かつ効果的に管理し、優先順位を付けるのに役立ちます。これらのオプションを使用するには、ユーザーはインシデント テーブルからインシデントを選択し、それらを右クリックして、メニューから目的のオプションを選択する必要があります。ユーザーは、Ctrl+A ですべてのインシデントを選択し、Ctrl+Shift+A でインシデントをアナリストに割り当て、Ctrl+Shift+S でインシデントのステータスを変更するなど、キーボード ショートカットを使用してこれらのアクションを実行することもできます12。
* インシデントをアナリストに一括で割り当て
* 複数のインシデントのステータスを変更する

最新問題: **39**
Cortex XDR Analytics は、次の MITRE ATT&CKTM 技術に一致するアクティビティを検出したときにアラートを送信できます。
A. 流出、指揮統制、影響
B. 窃盗、指揮統制、特権昇格
C. 窃盗、指揮統制、横方向の移動
D. 窃盗、指揮統制、収集
Answer: C (メーッセージを残す**)**

最新問題: **40**
Android システムで利用できる Live Terminal オプションは次のうちどれですか?
A. ライブターミナルはサポートされていません。
B. アプリを停止します。
C. APK スクリプトを実行します。
D. Android コマンドを実行します。
Answer: D (メーッセージを残す**)**
説明
Cortex XDR は Android システム用のライブ ターミナルをサポートしており、コマンドライン インターフェイスを使用して Android エンドポイントにリモートでアクセスして管理できるようになります。Live Terminal を使用して、adb Shell、adb logcat、adb install、adb uninstall などの Android コマンドを実行できます。Live Terminal を使用して、Android エンドポイント上のファイル、ディレクトリ、権限を表示および変更することもできます。Android システムの Live Terminal は、アプリの停止や APK スクリプトの実行をサポートしていません。参考文献:
* Cortex XDR ドキュメント ポータル
* ライブターミナルセッションを開始する

* ライブターミナルコマンド

最新問題: **41**
OS の機能に基づいた攻撃を防ぐために使用できる Exploit ProtectionModule (EPM) はどれですか?
A. UASLR
B. JIT の軽減
C. メモリ制限ヒープ スプレー チェック
D. DLL セキュリティ
Answer: B (メーッセージを残す**)**
説明
JIT 軽減策は、OS の機能に基づいて攻撃を防止するために使用できるエクスプロイト保護モジュール (EPM) です。JIT 軽減策は、OS のジャストインタイム (JIT) コンパイラーを使用して悪意のあるコードを実行するエクスプロイトから保護します。JIT 軽減策は、JIT コンパイラによって割り当てられたメモリ ページを監視し、それらのページからコードを実行しようとする試みをブロックします。これにより、攻撃者がデータ実行防止 (DEP) やアドレス空間レイアウトのランダム化 (ASLR) などの他のセキュリティ メカニズムをバイパスする方法として JIT コンパイラーを使用することができなくなります。参考文献:
* パロアルトネットワークス。(2023年)。PCDRA 学習ガイド。PDF ファイル。から取得 https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/datasheets/education/pcdra-study-g
* パロアルトネットワークス。(2021年)。エクスプロイト保護モジュール。ウェブページ。から取得 https://docs.paloaltonetworks.com/traps/6-0/traps-endpoint-security-manager-admin/traps-endpoint-securit

最新問題: **42**
経営幹部が平均解決時間 (MTTR) 指標を探している場合、どの組み込みダッシュボードが最適なオプションでしょうか?
A. インシデント管理ダッシュボード
B. セキュリティ管理者ダッシュボード
C. セキュリティ マネージャー ダッシュボード
D. データ取り込みダッシュボード
Answer: C (メーッセージを残す**)**

最新問題: **43**
アラートの除外を作成して実装すると、どのような結果になりますか?
A. Cortex XDR エージェントは、ブロックされたプロセスがエンドポイントで実行できるようにします。
B. Cortex XDR コンソールはこれらのアラートを非表示にします。

C. Cortex XDR エージェントは今後、このイベントのアラートを作成しません。
D. Cortex XDR コンソールはこれらのアラートを削除し、今後のアラートの取り込みをブロックします。
Answer: B (メーッセージを残す**)**
説明
アラートの除外を作成して実装すると、Cortex XDR コンソールは除外基準に一致するアラートを非表示にします。アラートの除外は、関連性のないアラート、誤検知、または優先度の低いアラートをフィルターで除外し、注意が必要なアラートに焦点を当てることができるポリシーです。アラートの除外を作成するときは、アラート名、重大度、ソース、エンドポイントなど、除外するアラートを定義する基準を指定できます。アラートの除外を作成すると、Cortex XDR は基準に一致する今後のアラートを非表示にし、インシデントおよび検索クエリの結果から除外します。ただし、アラートの除外は、Cortex XDR エージェントの動作やエンドポイントのセキュリティ ポリシーには影響しません。Cortex XDR エージェントは引き続きイベントのアラートを作成し、セキュリティ ポリシーに従ってブロックや隔離などの適切なアクションを適用します。アラートの除外は、Cortex XDR コンソール上のアラートの表示にのみ影響し、エンドポイントの実際の保護には影響しません。したがって、正解は B です。Cortex XDR コンソールはこれらのアラートを非表示にします12。
* アラートの除外
* アラート除外ポリシーを作成する

最新問題**: 44**
Cortex XDR エージェントによって使用される Windows レジストリを最も適切に定義するものは次のうちどれですか?
A. 所有権を証明するために正式にライセンスされたバージョンのソフトウェアを登録するための、インターネット経由で利用できる中央システム
B. 使用可能なハードウェア リソースを超えるメモリをコミットするためにオペレーティング システムが使用するファイル システム。 ?ワップ」とも呼ばれます
C. 合計ディスク使用量とオペレーティング システムが使用できる残りのディスク容量に関する正確な最新情報を維持するための台帳
D. オペレーティング システムとアプリケーションの設定を保存する階層データベース
Answer: D (メーッセージを残す**)**

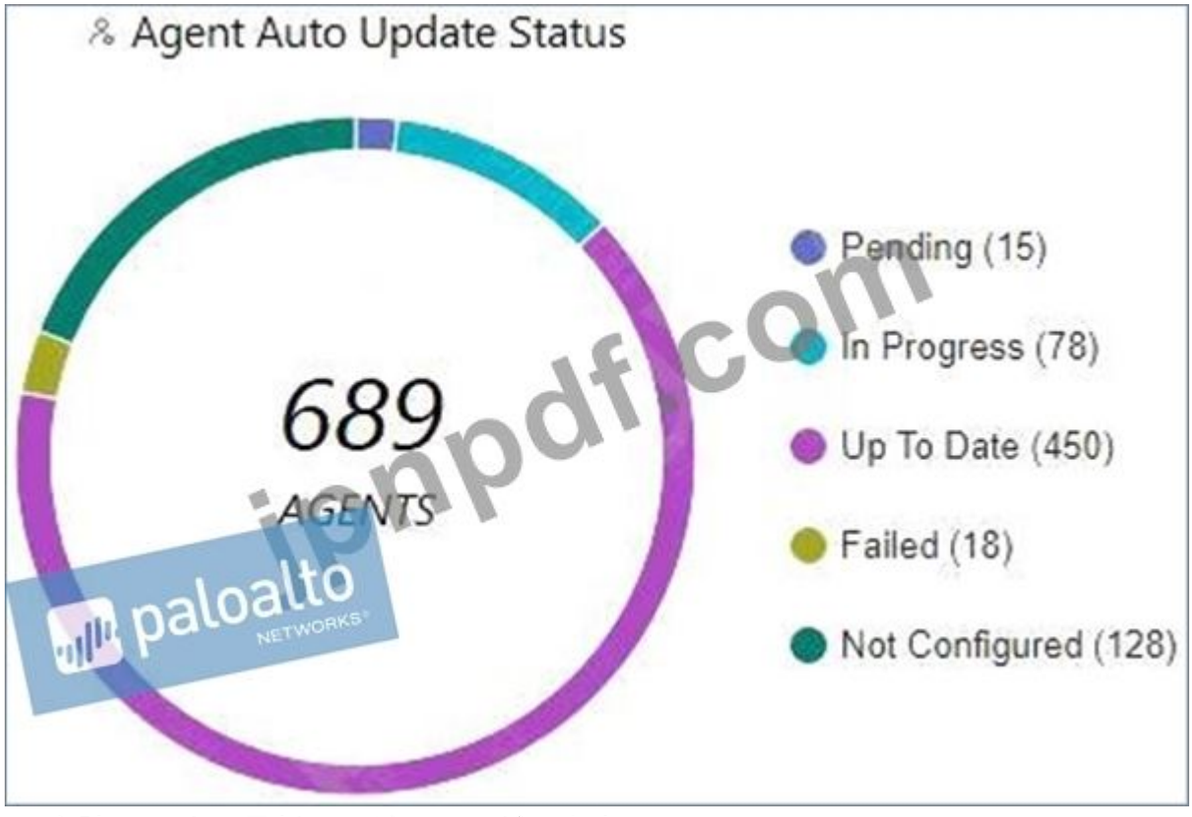
最新問題**: 45**
さまざまなベンダーから外部ログを取り込むにはどのようなライセンスが必要ですか?
A. ホストごとの Cortex XDR クラウド
B. TB あたりの Cortex XDR Pro
C. エンドポイントごとの Cortex XDR Pro
D. Cortex XDR ベンダー非依存プロ
Answer: (解答を表示する**)**

最新問題: **46**
Cortex XDR で作成できる例外プロファイルの 2 つのタイプはどれですか? (2つお選びください。)
A. 特定のエンドポイントに適用されるロールベースのプロファイル
B. 特定のエンドポイントに適用されるエージェント例外プロファイル
C. すべてのエンドポイントに適用されるグローバル例外プロファイル
D. 特定のエンドポイントに適用される例外プロファイル
Answer: (解答を表示する**)**

最新問題: **47**
Cortex XDR Analytics は、次の MITRE ATT&CKTM 技術に一致するアクティビティを検出したときにアラートを送信できます。
A. 窃盗、指揮統制、収集
B. 窃盗、指揮統制、特権昇格
C. 窃盗、指揮統制、影響
D. 窃盗、指揮統制、横方向の移動
Answer: (解答を表示する**)**
説明
Cortex XDR Analytics は、機械学習と行動分析を活用して、ネットワーク層とエンドポイント層全体にわたる悪意のあるアクティビティを検出して警告する Cortex XDR の機能です。Cortex XDR Analytics は、次の MITRE ATT&CKTM テクニックに一致するアクティビティを検出したときにアラートを送信できます: 抽出、コマンド アンド コントロール、横方向移動、実行、永続化、特権エスカレーション、防御回避、資格情報アクセス、検出、および収集。ただし、問題に示された選択肢のうち、正解は D、Exfiltration、Command and Control、Lateral Movement です。これらは、環境内の高度かつ持続的な脅威 (APT) を示す最も重要な手法の 3 つです。漏洩とは、侵害されたシステムまたはネットワークから敵が制御する外部の場所にデータまたは情報を転送する手法を指します。コマンド アンド コントロールとは、侵害されたシステムまたはネットワークと通信して、指示を提供したり、データを受信したり、マルウェアを更新したりする技術を指します。水平移動とは、通常、より多くのリソースまたはデータにアクセスするために、同じ環境内で 1 つのシステムまたはネットワークから別のシステムまたはネットワークに移動する手法を指します。Cortex XDR Analytics は、ネットワーク トラフィック、ファイアウォール ログ、エンドポイント イベント、脅威インテリジェンスなどのさまざまなデータ ソースを分析し、動作モデル、異常検出、相関

ルールを適用することで、これらの手法に関するアラートを発行できます。Cortex XDR Analytics は、アラートを対応する MITRE ATT&CKTM 技術にマッピングし、追加のコンテキストと攻撃チェーンの可視性を提供することもできます1234
* Cortex XDR 分析
* MITRE ATT&CKTM
* Cortex XDR 分析 MITRE ATT&CKTM テクニック
* Cortex XDR 分析アラート カテゴリ

最新問題: **48**
次のエージェント自動アップグレード ウィジェットに基づいて正しいのはどれですか?



A. 合計 689 人の最新エージェントがいます。
B. エージェントの自動アップグレードは有効になっていますが、すべてのエンドポイントで有効ではありません。
C. エージェントの自動アップグレードが有効になっていません。
D. 保留中ステータスのエージェントの数が進行中ステータスよりも多くあります。
Answer: B (メーッセージを残す**)**
説明
エージェント自動アップグレード ウィジェットには、エンドポイントのエージェント自動アップグレード機能のステータスが表示されます。ウィジェットには、最新、進行中、保留中、失敗したエージェント、および未構成のエージェントの数が表示されます。この場合、ウィジェットには、最新のエージェントが 450 個、進行中のエージェントが 78 個、保留中のエージェントが 15 個、失敗したエージェントが 18 個、未構成のエージェントが 128 個あることが表示されます。これ

は、エージェントの自動アップグレード機能が有効になっているものの、すべてのエンドポイントで有効ではないことを意味します。
参考文献:
* Cortex XDR エージェントの自動アップグレード
* PCDRA 学習ガイド

最新問題: **49**
「ファイルの検索と破棄」機能を使用する場合、次の検索ハッシュ タイプのうちどれがサポートされますか?
A. ファイルの MD5 ハッシュ
B. ファイルの SHA1 ハッシュ
C. ファイルの AES256 ハッシュ
D. ファイルの SHA256 ハッシュ
Answer: (解答を表示する**)**

最新問題: **50**
XQL クエリの論理スキーマは何に含まれますか?
A. ビン
B. 配列の展開
C. フィールド
D. データセット
Answer: (解答を表示する**)**
説明
XQL クエリの論理スキーマはフィールドであり、データセットの名前付き属性です。フィールドには、文字列、整数、ブール値、配列などのデータ型を指定できます。フィールドには、クエリ出力のフィールド値を変換する bin や Expand などの修飾子を含めることもできます。フィールドは、XQL クエリの select、where、group by、order by、having 句で使用できます。参考文献:
* XQL 構文
* XQL データ型
* XQLフィールド修飾子

最新問題: **51**
Cortex XDR 用の WildFire の機能は何ですか?
A. WildFire はクラウドで実行され、XDR エージェントからのアラート データを分析して、行動上の脅威をチェックします。
B. WildFire はサンプルを受け入れて分析し、判定を出します。
C. WildFire は、ローカル エージェント上で実行され、エンドポイントで行動上の脅威が発生しているかどうかを判断するエンジンです。
D. WildFire はエージェント上で完全に実行され、サンプルを迅速に分析して判定を行います。
Answer: B (メーッセージを残す**)**

最新問題: **52**
Cortex XDR エージェントを DaemonSet として Kubernetes クラスターにデプロイする場合、どのライセンスが必要ですか?
A. TB あたりの Cortex XDR Pro
B. ホストの分析情報
C. エンドポイントごとの Cortex XDR Pro
D. ホストごとの Cortex XDR クラウド
Answer: (解答を表示する**)**
説明
Cortex XDR エージェントを DaemonSet として Kubernetes クラスターにデプロイする場合、必要なライセンスはホストごとの Cortex XDR Cloud です。このライセンスを使用すると、Cortex XDR を使用して、Kubernetes クラスター、コンテナー、サーバーレス機能などのクラウド ワークロードを保護および監視できます。Cortex XDR Cloud per Host ライセンスを使用すると、Cortex XDR エージェントを DaemonSet として Kubernetes クラスターにデプロイでき、クラスター内のすべてのノードでエージェントのコピーが実行されるようになります。Cortex XDR エージェントは、分析と関連付けのために、ポッド イベント、コンテナー ログ、ネットワーク トラフィックなどのデータを Kubernetes クラスターから収集し、Cortex Data Lake に送信します。Cortex XDR は、クラウド環境全体の脅威を検出して対応し、クラウド ワークロードに可視性とコンテキストを提供します。Cortex XDR Cloud per Host ライセンスは、各ホスト上のコンテナーや機能の数に関係なく、Cortex XDR エージェントを実行するホストの数に基づいています。ホストは、Cortex XDR エージェントを実行する仮想マシン、物理サーバー、または Kubernetes ノードとして定義されます。Cortex XDR Cloud per Host ライセンスと、Cortex XDR エージェントを Kubernetes クラスターにデプロイする方法の詳細については、こちら 1 およびこちら 2 を参照してください。参考文献:
* ホストごとの Cortex XDR クラウド ライセンス
* Cortex XDR エージェントを DaemonSet として Kubernetes クラスターにデプロイする

最新問題: **53**
Cortex Data Lake の目的は何ですか?
A. ログとアラート データを集約できるローカル ストレージ施設
B. ファイアウォール ログが保存されるクラウドベースのストレージ施設
C. ファイアウォールと Cortex XDR エージェント間のインターフェイス
D. 潜在的なマルウェア ファイルを爆発させるための Cortex XDR エージェントのワークスペース
Answer: (解答を表示する**)**

最新問題: **54**
フィッシングは次の MITRE ATT&CK 戦術のどれに属しますか?
A. 初期アクセス、永続性

B. 永続性、コマンド アンド コントロール
C. 偵察、持続
D. 偵察、初期アクセス
Answer: (解答を表示する**)**
説明
フィッシングは、偵察と初期アクセスという 2 つの MITRE ATT&CK 戦術に属する手法です。
偵察は、攻撃を開始する前にターゲットに関する情報を収集するプロセスです。情報のフィッシングは偵察のサブテクニックであり、フィッシング メッセージを送信して、ターゲティング時に使用できる機密情報を引き出します。初期アクセスは、ネットワークまたはシステムに足場を築くプロセスです。フィッシングは、フィッシング メッセージを送信して被害者のシステム上で悪意のあるコードを実行する、初期アクセスのサブテクニックです。フィッシングは、フィッシング メッセージの目的と内容に応じて、偵察と初期アクセスの両方に使用できます。参考文献:
* フィッシング、テクニック T1566 - エンタープライズ | マイターアタック&CK 1
* 情報目的のフィッシング、テクニック T1598 - エンタープライズ | マイターアタック&CK 2
* 情報目的のフィッシング、パート 2: 戦術とテクニック 3
* フィッシングと MITREATT&CK フレームワーク - EnterpriseTalk 4
* 初期アクセス、戦術 TA0001 - エンタープライズ | マイターアタック&CK 5

最新問題**: 55**
フィッシングは次の MITRE ATT&CK 戦術のどれに属しますか?
A. 偵察、初期アクセス
B. 永続性、コマンド アンド コントロール
C. 初期アクセス、永続性
D. 偵察、持続
Answer: A (メーッセージを残す**)**

最新問題**: 56**
経営幹部が平均解決時間 (MTTR) 指標を探している場合、どの組み込みダッシュボードが最適なオプションでしょうか?
A. セキュリティ マネージャー ダッシュボード
B. データ取り込みダッシュボード
C. セキュリティ管理者ダッシュボード
D. インシデント管理ダッシュボード
Answer: (解答を表示する**)**
説明
インシデント管理ダッシュボードは、平均解決時間 (MTTR) メトリクスを含む、インシデント対応プロセスの概要を提供します。このメトリクスは、インシデントが作成された瞬間からクローズされる瞬間まで、インシデントを解決するのにかかる平均時間を測定します。ダッシュボードには、ステータス、重大度、担当アナリストごとのインシデント数のほか、カテゴリ、ソース、宛先ごとの上位アラートも表示されます。インシデント管理ダッシュボードは、セキュリティ チームのパ

フォーマンスと効率を監視したい経営者やマネージャー向けに設計されています。参考文献: [PCDRA 研究ガイド]、18 ページ。

最新問題: **57**
「ファイルの検索と破棄」機能を使用する場合、次の検索ハッシュ タイプのうちどれがサポートされますか?
A. ファイルの SHA256 ハッシュ
B. ファイルの AES256 ハッシュ
C. ファイルの MD5 ハッシュ
D. ファイルの SHA1 ハッシュ
Answer: (解答を表示する**)**
説明
ファイルの検索と破棄機能は、エンドポイント全体で悪意のあるファイルや不要なファイルを検索して削除できるようにする Cortex XDR の機能です。この機能を使用すると、インシデントに迅速に対応し、脅威を修復し、コンプライアンス ポリシーを適用できます。ファイルの検索と削除機能を使用するには、検索して削除するファイルのファイル名とファイル ハッシュを指定する必要があります。ファイル ハッシュは、暗号化ハッシュ関数によって生成されるファイルの一意の識別子です。ファイル ハッシュにより、類似した名前や異なるバージョンのファイルではなく、必要なファイルを正確にターゲットにすることができます。ファイルの検索と破棄機能は、256 ビット (32 バイト) のハッシュ値を生成する安全なハッシュ アルゴリズムである SHA256 ハッシュ タイプをサポートします。SHA256 ハッシュ タイプは、ファイルの整合性検証とデジタル署名に広く使用されています。ファイルの検索と破棄機能は、暗号化アルゴリズムまたは安全性の低いハッシュ アルゴリズムである AES256、MD5、SHA1 などの他のハッシュ タイプをサポートしません。したがって、正解は A、file1234 の SHA256 ハッシュです。
* ファイルの検索と破壊
* ファイルハッシュとは何ですか?
* SHA-2 - フリー百科事典ウィキペディア
※ 「ファイルの検索と破棄」機能を使用する場合、次の検索ハッシュの種類のうちどれがサポートされますか?