CrowdStrike.CCFA-200b.v2026-06-13.q88

試験コード:	CCFA-200b
試験名称:	CrowdStrike Certified Falcon Administrator - 2024 Version
認定資格:	CrowdStrike
無料問題数:	88
バージョン:	v2026-06-13
アクセス数:	108
ページビュー数:	880
https://www.jpnpdf.com/CrowdStrike.CCFA-200b.v2026-06-13.q88-mondaishu.html	

最新問題: **1**
MacOS に Falcon Sensor を手動でインストールするための一般的なプロセスを最もよく表すオプションはどれですか?
A. コマンドラインでインストールトークンを渡してFalconパッケージをインストールします。
B. Falcon パッケージをインストールし、falconctl を使用してセンサーのライセンスを取得し、システム拡張を承認し、センサーにフルディスクアクセスを許可します。
C. Falcon パッケージにフルディスクアクセスを許可し、Falcon パッケージをインストールし、falconctl を使用してセンサーのライセンスを取得します。
D. Falcon パッケージにフルディスクアクセスを許可し、Falcon パッケージをインストールし、コマンド 'falconctl stats' で Falcon Sensor をロードします。
Answer: (解答を表示する)

最新問題: **2**
Falcon 管理者として、防止ポリシーを調整し、使用された検出レベル (注意、中、積極的、または非常に積極的) に応じて過去 30 日間に発生した検出数を比較したいと考えています。適切な設定を評価するのに最も役立つ監査ログはどれですか?
A. 予防方針
B. ポリシーの有効性の監視
C. 機械学習による予防監視
D. 防止ポリシーのデバッグ
Answer: C (メーッセージを残す)

最新問題: **3**
Falcon クラウドに接続していないセンサーは、何日後にホスト リストから自動的に削除されますか?

A. 45日間
B. 60日間
C. 30日間
D. 90日間
Answer: D (メーッセージを残す)
Falconクラウドに接続していないセンサーは、90日後にホストリストから自動的に削除されます。7日以上Falconクラウドに接続していないセンサーは非アクティブとみなされ、ホスト管理ページからゴミ箱ページに移動されます。非アクティブなセンサーはゴミ箱ページに90日間保存された後、Falconプラットフォームから完全に削除されます。90日以内にFalconクラウドに再度接続した場合は、ゴミ箱ページから非アクティブなセンサーを復元できます。

最新問題: **4**
デフォルトのセンサー更新ポリシーに推奨される内容を説明している記述はどれですか。
A. デフォルトのセンサー更新ポリシーは、可能な限り自動 N-1 および自動 N-2 構成を活用しながら、組織の全体的なセンサー更新の実践と整合させる必要があります。
B. デフォルトのセンサーアップデートは、常に最新のセンサーバージョンに自動的にアップグレードするように設定する必要があります。
C. デフォルトのセンサー更新ポリシーは、推奨設定であらかじめ構成されているため、デフォルトのセンサー更新ポリシーを構成する必要はありません。
D. 設定は不要です。カスタムセンサー更新ポリシーを作成すると、デフォルトのセンサー更新ポリシーは無効になります。
Answer: (解答を表示する)
デフォルトセンサー更新ポリシーの推奨事項は、可能な限り自動N-1および自動N-2構成を活用しつつ、組織全体のセンサー更新方法と整合させることです。質問139で説明したように、デフォルトセンサー更新ポリシーは、特定のセンサー更新ポリシーに割り当てられていないすべてのホストに適用される 包括的な」ポリシーです。したがって、デフォルトセンサー更新ポリシーは、センサーの更新頻度や更新速度など、組織全体のセンサー更新方法と整合させることが推奨されます。また、手動による介入なしにセンサーを最新または2番目に新しいセンサーバージョンに自動的に更新できる自動N-1および自動N-2構成を活用することも推奨されます。

最新問題: **5**
Falcon管理者がリアルタイムレスポンスを使用して、センサーがインストールされているホストとのセッションを開始しようとしましたが、接続できません。最も考えられる原因は何でしょうか？
A. ホストにユーザーがログインしています
B. ドメインコントローラが接続を妨げています
C. RTRロールが割り当てられていない
D. 別のアナリストが接続されています

Answer: (解答を表示する)
センサーがインストールされているホストとリアルタイムレスポンスを使用してセッションを開始できない場合、最も可能性の高い原因は、ホストにRTRロールが割り当てられていないことです。RTR（リアルタイムレスポンス）ロールは、Falconのリアルタイムレスポンス機能を使用するためのアクセス権限を付与するロールです。これにより、リモートからホストにリアルタイムでアクセスして調査することができます。RTRロールには、リアルタイムレスポンス - 読み取り専用アナリスト、リアルタイムレスポンス - アクティブレスポンダー、リアルタイムレスポンス - 管理者の3種類があります。リアルタイムレスポンスを使用するには、これらのロールのうち少なくとも1つが割り当てられている必要があります。

最新問題: **6**
顧客 ID (CID) は次のどのシナリオで重要ですか?
A. Falconコンソールのユーザーアプリケーションにユーザーを追加する場合
B. センサーのインストールプロセスを実行するとき
C. APIキーを設定する場合
D. ホスト検索を実行するとき
Answer: B (メーッセージを残す)
カスタマーID（CID）は、センサーのインストールプロセスを実行するときとAPIキーを設定するときに重要になります。CIDは組織固有の識別子であり、センサーのインストールとFalconクラウドとの通信を認証するために必要です。Falconセンサーをホストにインストールする際には、コマンドラインパラメータまたはfalconctlツールを使用してCIDを指定する必要があります。CIDは、Falcon APIを介してプログラム的にFalconプラットフォームにアクセスするために使用するAPIキーの設定にも必要です。Falconコンソールの「APIクライアントとキー」ページでAPIクライアントとキーを作成する際にも、CIDを指定する必要があります。

最新問題: **7**
Falconでホストがネットワークコンテンンテートされており、ゼロデイパッチを適用してオペレーティングシステムを更新するよう指示されました。このタスクにパッチ更新システムを使用しようとしましたが、ジョブが失敗しました。
Falcon UI のどの構成手順でこれらのアクティビティが可能になりますか?
A. パッチ管理ツールの特定のIPアドレスを許可する封じ込めポリシーを作成します。
B. パッチ管理ツールの完全修飾名のリストを許可する包含ポリシーを作成します。
C. パッチ管理ツールを許可するファイアウォールポリシーを作成します
D. ホストの包含を解除し、すべてのパッチでホストを更新します
Answer: A (メーッセージを残す)

最新問題: **8**
ユーザーのパスワードをリセットするには管理者は何をする必要がありますか?

A. ユーザー管理から、影響を受けるユーザーのアカウント詳細を開き、 新しいパスワードの生成」を選択します。
B. ユーザー管理から、影響を受けるユーザーアカウントの3つのドットメニューから 「パスワードのリセット」を選択します。
C. ユーザー管理から 「アカウントの更新」を選択し、影響を受けるユーザーアカウントの新しいパスワードを手動で作成します。
D. ユーザー管理から、ユーザー固有の秘密/公開鍵生成用の証明書が有効ではなくなったため、管理者はアカウントを再構築する必要があります。
Answer: B (メーッセージを残す**)**
管理者は、ユーザー管理ページで該当のユーザーアカウントの3点メニューから 「パスワードのリセット」を選択することで、ユーザーのパスワードをリセットできます。これにより新しいパスワードが生成され、ユーザーのメールアドレスに送信されます。その他のオプションは正しくないか、利用できません。

最新問題**: 9**
検出のみのポリシーを作成したいのですが、ポリシー設定でどのように設定すればよいですか？
A. 検出スライダーを有効にし、防止スライダーを無効にします。次に、Next Gen Antivirus が有効になっていることを確認し、Windows Defender を無効にします。
B. 検出のみ」テンプレートを選択します。ハッシュブロックと除外を無効にします。
C. 検出のみで防止しないポリシーを作成することはできません。検出にはカスタムIOA ルールを使用してください。
D. 次世代アンチウイルスの検出設定を希望の検出レベルに設定し、すべての防御スライダーを無効にします。その他のブロックやマルウェア防御オプションは有効にしないでください。
Answer: (解答を表示する**)**
管理者は、次世代アンチウイルスの検出設定を必要な検出レベルに設定し、ポリシー設定ですべての防御スライダーを無効にすることで、検出のみのポリシーを作成できます。これにより、Falconはこのポリシーを使用しているホスト上の脅威を検出しますが、防御は行いません。その他のブロックまたはマルウェア防御オプションは、防御アクションを有効にするため、有効にしないでください。その他のオプションは、正しくないか、検出のみのポリシーの作成とは無関係です。

最新問題**: 10**
センサーが自動センサー更新を受信する速度を制御するのは次のどれですか?
A. メンテナンストークン
B. センサー更新ポリシー
C. センサー更新スロットル
D. チャネルファイルの更新スロットル

Answer: (解答を表示する**)**
センサーが自動センサーアップデートを受信する速度を制御するオプションは、"センサーアップデートスロットリング"です。センサーアップデートスロットリングを使用すると、1時間あたりに新しいセンサーバージョンをダウンロードできるセンサーの数を制限できます。これにより、同時センサーアップデートによるネットワークの輻輳や帯域幅の問題を回避できます。センサーアップデートスロットリングの設定は、各プラットフォームのセンサーアップデートポリシーで行うことができます。

最新問題: **11**
Windows/Mac/*nix ごとに個別のセンサー更新ポリシーを設定することが重要なのはなぜですか?
A. センサーの展開のテストと追跡を支援するため
B. 監査の要件です
C. 各OSごとに特別な考慮事項がある場合があります
D. ネットワークプロトコルはホストOSごとに異なります
Answer: C (メーッセージを残す**)**

最新問題: **12**
ネットワーク封じ込めポリシーの目的は何ですか?
A. 割り当てられた予防ポリシーの積極性を高める
B. 侵害されたホストがネットワークに与える影響を制限する
C. ネットワークアクティビティの可視性を高める
D. プライバシーのためにネットワークを分割する
Answer: B (メーッセージを残す**)**
ネットワーク封じ込めポリシーの目的は、侵害を受けたホストがネットワークに与える影響を最小限に抑えることです。このポリシーにより、ユーザーはホストをネットワークから隔離しつつ、Falcon Cloudやその他の重要なサービスとの通信を許可することができます。これにより、侵害を受けたホストによるさらなる被害やデータ流出を防ぐことができます。その他のオプションは正しくないか、ポリシーに関連しません。

最新問題: **13**
Falcon ではユーザー権限はどのように設定されますか?
A. 権限はユーザーグループに割り当てられ、その後ユーザーはそのグループに割り当てられ、それによってそれらの権限が継承されます。
B. 事前定義された権限は、ロールと呼ばれるセットに割り当てられます。ユーザーは職務に基づいて複数のロールを割り当てることができ、それらの割り当てに基づいて累積的な権限セットを付与されます。
C. 管理者は、ユーザー作成時にFalcon権限リストから個別の詳細な権限を選択します。
D. 権限はトークンベースです。ユーザーは定義された権限セットへのアクセスを要求し、管理者はそのトークンを権限セットに追加します。

Answer: (解答を表示する**)**
Falcon では、ロールと呼ばれるセットに事前定義された権限を割り当てることによってユーザー権限が設定されます。
ユーザーには職務内容に基づいて複数のロールを割り当てることができ、それらの割り当てに基づいて累積的な権限セットが付与されます。ロールとは、Falcon でユーザーが表示および実行できる内容を定義する権限の集合です。権限とは、ユーザーが Falcon の特定の機能にアクセスできるようにする詳細なアクションです。例えば、Falcon 管理者ロールと Falcon 調査員ロールの両方が割り当てられたユーザーは、両方のロールのすべての権限を持ちます。

最新問題**: 14**
エージェント ID の重複を防ぐために、永続クローンとして使用される VM ではどのようなインストール パラメータを使用する必要がありますか?
A. NO_START=1
B. VM=真
C. ProvNoWait=1
D. /静かに
Answer: (解答を表示する**)**

最新問題**: 15**
CrowdStrike Falcon の Windows センサー インストーラーはどこで入手できますか?
A. センサーはホスト > センサーダウンロードからダウンロードされます
B. センサーインストーラーは顧客ごとに固有であり、サポートから入手する必要があります。
C. センサーインストーラーは、CrowdStrike Webサイトのサポートセクションからダウンロードされます。
D. センサーはFalcon内から展開されるため、センサーインストーラーは使用されません。
Answer: A (メーッセージを残す**)**
CrowdStrike FalconのWindowsセンサーインストーラーは、Falconコンソールの「ホスト」> 「センサーダウンロード」ページからダウンロードできます。このページでは、様々なOSおよびプラットフォーム向けのセンサーバージョンとインストーラーをダウンロードできるほか、インストール手順とリリースノートも確認できます。その他のオプションは正しくないか、利用できません。

最新問題**: 16**
Falcon SensorがインストールパラメータNO_START=1を使用して仮想マシンテンプレートにインストールされたと仮定します。その後、仮想マシンテンプレートを再起動します。再起動後、Falcon Sensorにはどのような影響がありますか？
A. ファルコンセンサーは起動時にBIOSチェックを無効にします
B. Falcon Sensorは起動しますが、Falconコンソールにハートビートを送信するだけです。

C. Falcon Sensorは再起動時に自動的に起動しません。手動で起動する必要があります。
D. 再起動時に Falcon Sensor が起動し、エージェント ID が生成されます。
Answer: (解答を表示する**)**

最新問題: **17**
どのデフォルトのユーザー ロールで、アナリスト セッションの詳細をすべて表示できますか?
A. リアルタイムレスポンス - 管理者
B. ファルコン管理者
C. リアルタイムレスポンス - 読み取り専用アナリスト
D. リアルタイムレスポンス - アクティブレスポンダー
Answer: B (メーッセージを残す**)**

最新問題: **18**
貴社の環境に最適な予防ポリシーの機械学習スライダー設定を評価しています。テストフェーズでは、検出スライダーを 「アグレッシブ」に設定しました。この設定でセンサーを1週間テストした後、組織に最適な機械学習スライダー設定を決定するために、どの監査レポートを確認すべきでしょうか？
A. 予防ポリシー監査証跡
B. 防止ポリシーのデバッグ
C. 防止ハッシュは無視されます
D. 機械学習による予防監視
Answer: (解答を表示する**)**
監査ログ --> 機械学習防止監視 定義された期間の検出レベルに基づいて ML が予測した検出の数と、各検出レベルで検出されるファイルのリストが表示されます。

最新問題: **19**
非アクティブなホストは、ホスト管理ページまたはゴミ箱ページに何日間表示されますか?
A. 45日間
B. 15日間
C. 90日間

D. 120日
Answer: (解答を表示する**)**
非アクティブなホストは、ホスト管理ページまたはゴミ箱ページに90日間表示されます。非アクティブなホストとは、Falconプラットフォームと7日間以上通信していないホストのことです。非アクティブなホストは、7日間非アクティブな状態が続くと、ホスト管理ページからゴミ箱ページに移動されます。非アクティブなホストは、ゴミ箱ページに90日間表示された後、Falconプラットフォームから完全に削除されます。90日以内に非アクティブなホストが再びアクティブになった場合は、ゴミ箱ページから復元できます。

最新問題: **20**
Falcon プラットフォームで発生する特定のイベントに基づいてカスタム通知を作成できるワークフローを作成するために使用されるモデルは何ですか?
A. For - While 文
B. トリガー、条件、アクション
C. イベントトリガー
D. 定義済みのワークフローテンプレート
Answer: B (メーッセージを残す**)**
Falcon プラットフォームで発生する特定のイベントに基づいてカスタム通知を作成できるワークフローを作成するために使用されるモデルは、トリガー、条件、アクションです。このモデルでは、ワークフローをトリガーするイベント、ワークフローを実行するために満たす必要がある条件、そしてワークフローによって実行されるアクションを指定できます。
その他のオプションは間違っているか、ワークフローの作成に関連していません。

最新問題: **21**
カスタム IOA ルールはどの構文を使用して定義されますか?
A. グロブ
B. PowerShell
C. 子供
D. 正規表現
Answer: D (メーッセージを残す**)**

最新問題: **22**
封じ込め期間中に特定のトラフィックを許可するように設定を変更できるのはどこですか?
A. 予防方針
B. ホスト設定
C. 封じ込めポリシー
D. ファイアウォール設定
Answer: C (メーッセージを残す**)**

管理者は、封じ込めポリシーを作成または編集することで、封じ込め期間中に特定のトラフィックを許可するように設定を変更できます。このポリシーでは、ネットワーク封じ込め中に許可またはブロックするポート、プロトコル、IPアドレスを指定できます。その他のオプションは正しくないか、ネットワーク封じ込めとは関係ありません。

最新問題: **23**
ユーザーがリアルタイム レスポンスを使用してホストに接続できるのはどのロールですか?
A. エンドポイントマネージャー
B. ファルコン管理者
C. リアルタイム レスポンダー ?アクティブ レスポンダー
D. 予防ハッシュマネージャー
Answer: C (メーッセージを残す**)**
リアルタイムレスポンスを使用してホストに接続できるロールは、リアルタイムレスポンダ - アクティブレスポンダです。このロールでは、 ホストへの接続」機能を使用してホストから追加情報を収集したり、ホスト上でコマンドやスクリプトを実行したりできます。他のロールにはこの機能はありません。

最新問題: **24**
特定のドメインに対してカスタム IOA を作成する場合、すべてのサブドメインでも検出または防止するにはどの構文が最適ですか?
A. *\.baddomain\.xyz|baddomain\.xyz
B. *baddomain\. xyz|baddomain\. xyz. *
C. ドメインに対してカスタムIOAルールを作成できません
D. **baddomain\. xyz|baddomain\. xyz**
Answer: A (メーッセージを残す**)**
すべてのサブドメインで検出または防止するのに最適な構文は次のとおりです。
*.baddomain.xyz|baddomain.xyz。この構文は、.baddomain.xyzで終わるドメイン、またはbaddomain.xyzと完全に一致するドメインに一致します。ワイルドカード 『」はドットの前の任意の文字に一致し、「」演算子は式の前後のいずれの文字にも一致します。この構文は、カスタムIOCまたはカスタムIOAルールで使用して、悪意のあるドメインへのネットワーク接続を検出または防止できます。

最新問題: **25**
アナリストから、ここ数日、ワークフローによってトリガーされた通知を受信していないという報告がありました。
潜在的な障害を最初にどこで確認する必要がありますか?
A. カスタムアラート履歴
B. ワークフロー実行ログ
C. ワークフロー監査ログ

D. Falcon UI 監査証跡
Answer: B (メーッセージを残す**)**
ワークフロー管理オプションのワークフロー実行ログでは、検出イベントによってトリガーされたワークフロー実行のステータスと結果を確認できます。ログは、ワークフロー名、ステータス、開始時刻と終了時刻、検出IDでフィルタリングできます。また、実行されたアクション、受信した出力、発生したエラーなど、各実行の詳細も確認できます。このログは、ワークフローの潜在的な障害や問題のトラブルシューティングに役立ちます。

最新問題**: 26**
ワークフローを表示、作成、編集できるデフォルトのロールは何ですか?
A. Falcon管理者、ワークフロー作成者
B. Falcon管理者、Falconセキュリティリーダー、ワークフロー作成者
C. Falcon管理者、ワークフロー作成者、Falconセキュリティリーダー、Falcon調査員
D. Falcon管理者、Falconセキュリティリーダー
Answer: B (メーッセージを残す**)**

最新問題**: 27**
Falcon Sensor が Red Hat Enterprise Linux ホストにインストールされている場合、インストール トークンはどのように設定されますか?
A. インストール中にインストールトークンの入力が求められます。
B. sudo yum install --cid= --provisioning-token=ABCD1234
C. sudo /opt/CrowdStrike/falconctl -s -t ABCD1234
D. sudo /opt/CrowdStrike/falconctl -s --cid= --provisioning-token=ABCD1234
Answer: D (メーッセージを残す**)**

最新問題**: 28**
インターネット接続が遅いホストにFalconセンサーをインストールしようとしましたが、20分後にインストールに失敗します。次のパラメータのうち、どれを使用して上書きできますか？
デフォルトのプロビジョニングウィンドウは 20 分ですか?
A. 拡張ウィンドウ=1
B. タイムアウト=0
C. ProvNoWait=1
D. タイムアウト=30
Answer: (解答を表示する**)**
"ProvNoWait=1
センサーは、20分以内にCrowdStrikeクラウドに接続できない場合（Falconセンサーバージョン6.21以前では10分）でもインストールを中止しません。 デフォルトでは、ホストがクラウドに接続できない場合、20分間接続を再試行します。その後、ホストはセンサーを自動的にアンインストールします。）

"ProvWaitTime=3600000
センサーはインストール時に CrowdStrike クラウドに接続するまで 1 時間待機します (デフォルトは 20 分です)。

最新問題: **29**
新入社員のラップトップにFalconを正常にインストールした後、作成したカスタム防御ポリシーではなく、デフォルトの防御ポリシーがマシンに割り当てられていることに気づきました。Falconセンサーが正常に動作していることを確認し、カスタムポリシーが有効化され、1,000台を超える他のFalconホストで正常に動作していることを確認しました。
この問題の原因は何でしょうか?
A. Falcon では、新しくインストールされたホストにカスタムポリシーを適用するには 24 時間の待機期間が必要です。
B. ホストベースのファイアウォールルールにより、カスタムポリシーが正常に適用されません。
C. 新しい防止ポリシーを適用するプロンプトが手動で拒否されました
D. ラップトップは、カスタムポリシーに割り当てられたホストグループのメンバーではありません
Answer: D (メーッセージを残す**)**

最新問題: **30**
疑わしいVBAマクロを監視する機能が必要です。防止ポリシー設定の中で、どのセンサーの可視性設定をオンにする必要がありますか？
A. スクリプトベースの実行監視
B. 通訳のみ
C. 追加のユーザーモードデータ
D. エンジン（完全な可視性）
Answer: A (メーッセージを残す**)**
スクリプトベースの実行監視防止ポリシー設定をオンにすると、 Falconセンサーは、ホスト上で悪意のあるコードを実行するための一般的なメカニズムであるスクリプトとシェルの内容を監視します。この設定では、スクリプトが強制終了またはブロックされることはありません。」スクリプト言語：
Excel 4.0 マクロ
JScript
VBAマクロ
VBスクリプト
疑わしいVBAマクロを監視するために、防止ポリシー設定内でオンにする必要があるセンサーの可視性設定は、スクリプトベースの実行モニタリングです。スクリプトベースの実行モニタリングは、FalconセンサーがWindowsシステム上で悪意のあるスクリプトの実行を監視・防止できるようにする機能です。この機能は、機械学習と行動分析を使用して、PowerShell、WScript、CScript、Bashなどのさまざまなスクリプトインタープリターに

よって実行される疑わしいスクリプトやコマンドを検出します。VBA（Visual Basic for Applications）は、WordやExcelなどのMicrosoft Officeドキュメントに埋め込むことができるスクリプト言語です。VBAマクロは、タスクを自動化したり、ドキュメント内でアクションを実行したりするために使用できますが、攻撃者がマルウェアを配信したり、悪意のあるコードを実行したりするために悪用される可能性もあります。スクリプトベースの実行モニタリングは、VBAマクロの内容を監視して悪意のあるコンテンツが実行されないようにすることで、このような攻撃を検出・防止するのに役立ちます。

最新問題: **31**
Windows センサーが実行中かどうかを確認するには、どのコマンドを実行する必要がありますか?
A. regedit myfile.reg
B. sc クエリ csagent
C. netstat -f
D. ps -ef | grep falcon
Answer: B (メーッセージを残す**)**
Windows センサーが実行中かどうかを確認するために実行する必要があるコマンドは、sc query csagent です。
このコマンドは、Falconセンサーサービスであるcsagentサービスのステータスと情報を表示します。他のコマンドは正しくないか、Windowsセンサーには適用できません。

最新問題: **32**
Windows 上の Falcon Sensor のトラブルシューティングを行う際に、ログ ディレクトリを指定されたファイルに出力するための正しいパラメーターは何ですか?
A. ログ=log.txt
B. \log log.txt
C. C:\CSSensorInstall\LogFiles
D. /log log.txt
Answer: D (メーッセージを残す**)**
WindowsでFalcon Sensorのトラブルシューティングを行う際に、ログディレクトリを指定のファイルに出力するための正しいパラメータは/log log.txtです。このパラメータは、セン

サーインストールコマンドを実行したフォルダと同じフォルダにlog.txtというログファイルを作成します。ログファイルには、使用されたパラメータ、実行されたアクション、発生したエラーなど、センサーのインストールプロセスに関する情報が含まれます。

最新問題: **33**
既存の IOA 除外を編集する場合、編集できないものは何ですか?
A. IOA名
B. 除外のすべての部分を変更できます
C. 除外名
D. ホストグループ
Answer: A (メーッセージを残す**)**
既存のIOA除外を編集する場合、IOA名は編集できません。IOA（攻撃指標）除外を使用すると、プロセス実行、ファイル書き込み、ネットワーク接続、レジストリイベントに基づいて、疑わしい動作を検知または防御から除外するためのカスタムルールを定義できます。IOA名は、除外するIOA動作の種類を識別するための定義済みの名前です（例：「疑わしいプロセス実行 - スクリプトインタープリタによるファイル実行」）。IOA名はFalconプラットフォーム内の特定のIOAルールにリンクされているため、既存のIOA除外を編集する際には変更できません。ただし、除外名、ホストグループ、フィルター条件など、IOA除外の他の部分は編集できます。

最新問題: **34**
異なるセンサー更新および防止ポリシーが適用された新しいホストグループにサーバーが追加されました。サーバーがオンラインになってから30分以上経過しているにもかかわらず、ポリシーがまだ適用されていません。
なぜポリシーが適用されないのですか?
A. 新しいグループは、グループの順序を変更し、PRECEDENCE 1に配置することで優先順位が付けられます。
B. ホストは複数のグループに所属することができ、サーバーには現在、より高い優先順位のポリシーが割り当てられています。
C. グループに変更を加えた場合、ポリシーの変更を有効にするにはホストの再起動が必要です。
D. 新しいグループは有効化されておらず、ホストは現在デフォルトのポリシーを適用しています
Answer: (解答を表示する**)**

最新問題: **35**
顧客 ID + チェックサム (CIDC) を参照する必要がある場合の例は何ですか?
A. 新しいFalcon Sensorをインストールする場合
B. ホスト管理で特定のホストを探す必要がある場合
C. ホストグループの割り当て基準を定義する場合

D. Falcon Sensorをアンインストールする場合
Answer: (解答を表示する**)**

最新問題**: 36**
センサーのインストール時に、各センサーにどのような一意の識別子が割り当てられますか?
A. セキュリティID (SID)
B. エージェントID (AID)
C. コンピュータID (CID)
D. エンドポイントID (EID)
Answer: B (メーッセージを残す**)**

最新問題**: 37**
次の機械学習 (ML) スライダーのうち、信頼性が高い悪意のあるアイテムのみを検出または防止するものはどれですか?
A. 攻撃的
B. 慎重
C. 最小限
D. 中程度
Answer: B (メーッセージを残す**)**
機械学習（ML）スライダーは、悪意のあるアイテムの確度が高い場合にのみ検出または阻止します。MLスライダーでは、FalconセンサーのMLエンジンの感度と攻撃性を調整できます。このエンジンは、人工知能を用いて未知の脅威を識別・阻止します。
「慎重」設定では、センサーは信頼性の高い悪意のあるイベントのみを検知・阻止し、信頼性の低いイベントはそのまま実行します。また、「中程度」や「非常に積極的」といった高い設定よりも、ノイズや誤検知が少なくなります。

最新問題**: 38**
CrowdStrike Falcon でセンサー更新ポリシーを持つグループを使用する目的は何ですか?
A. 同じビジネスユニット内の他のホストとホストをグループ化する
B. Falcon がインストールされた順序に従ってホストをグループ化し、アップデートが毎回同じ順序でインストールされるようにします。
C. Falcon アップデートのインストール順序を優先し、アップデートが一度にインストールされてネットワークの混雑が発生しないようにします。
D. 特定のホストへのセンサーバージョンの制御された割り当てを許可する
Answer: D (メーッセージを残す**)**
CrowdStrike Falconでセンサー更新ポリシーをグループに適用する目的は、特定のホストへのセンサーバージョンの割り当てを制御できるようにすることです。これにより、ユーザーはテスト環境、ステージング環境、本番環境など、ニーズや設定に応じて、異なるホス

トのセンサー更新を管理できます。その他のオプションは、正しくないか、センサー更新ポリシーをグループに適用することに関連しません。

最新問題: **39**
センサー更新ポリシー内のアンインストールおよびメンテナンス保護設定の制御内容を最もよく表しているのは次のうちどれですか。
A. センサーの自動更新を防止します
B. センサーが機能制限モードに入るのを防ぎます
C. センサー更新ポリシーの変更を防止します
D. センサーの不正なアンインストールを防止します
Answer: D (メーッセージを残す**)**
センサー更新ポリシー内の 「アンインストールとメンテナンスの保護」設定で制御される内容を最もよく表すオプションは、センサーの不正なアンインストールを防止することです。「アンインストールとメンテナンスの保護」設定は、センサーを手動でアンインストールまたは更新する際にメンテナンストークンを要求することで、センサーのセキュリティをさらに強化する機能です。メンテナンストークンは、Falcon管理者またはReal Time Response管理者がFalconコンソールで生成できる一意のコードです。有効なメンテナンストークンがないと、ローカル管理者やマルウェアを含むいかなるユーザーもセンサーをアンインストールまたは更新できません。

最新問題: **40**
Fusion SOAR ワークフロー条件の必須の 3 つの部分は何ですか?
A. パラメータ、演算子、値
B. 通知、アラート、API
C. トリガー、アクション、アラート
D. 値、トリガー、制約
Answer: A (メーッセージを残す**)**

最新問題: **41**
Linux センサー ダッシュボードにはどのような種類の情報がありますか?
A. カーネルバージョンによるホスト、ルートによって生成されたシェル、Wget/Curlの使用状況
B. 隠しファイルの実行、ゴミ箱からのファイルの実行、コンピュータ名で実行されているバージョン
C. 実行中のバージョン、Spotlight で非表示にされたディレクトリ、参照、表示、または変更されたログ/監査
D. 個人情報へのアクセス、アーカイブツールによる情報漏洩、実行可能ファイルの作成
Answer: (解答を表示する**)**
Linuxセンサーダッシュボードに表示される情報の種類は、カーネルバージョン別のホスト、ルートによって生成されたシェル、Wget/Curlの使用状況です。Linuxセンサーダッシュ

ボードは、環境内でFalconセンサーがインストールされているLinuxホストの概要を提供するダッシュボードです。
このダッシュボードを使用すると、カーネル バージョン、ルート シェルの使用状況、ネットワーク通信、検出、防止など、Linux ホストの健全性とアクティビティを監視できます。

最新問題: **42**
包含ポリシーに IP アドレスを追加する場合を最もよく表すシナリオは次のどれですか。
A. ホストのIPアドレスに基づいてネットワーク封じ込めプロセスを自動化したい
B. 組織には、Falconコンソールにアクセスする必要がある追加のIPアドレスがあります。
C. 新しいアナリストグループは、ホストをネットワーク封じ込め下に配置できる必要があります。
D. 組織には、ホストがネットワークに含まれているときにアクセスする必要があるリソースがあります。
Answer: D (メーッセージを残す**)**
IPアドレスを封じ込めポリシーに追加する最も適切なシナリオは、ホストがネットワーク封じ込めされている状態でもアクセス可能なリソースが組織に存在する場合です。前の質問で説明したように、IPアドレスを封じ込めポリシーに追加することで、封じ込められたホストと通信できる信頼できるIPアドレスの許可リストを作成できます。これは、潜在的な侵害や調査のためにホストをネットワークから隔離する必要があるものの、組織の運用やセキュリティに不可欠な特定のリソースやサービスへのアクセスは許可したい場合に役立ちます。

最新問題: **43**
センサーのインストール失敗をトラブルシューティングする際の有効な手順は次のどれですか?
A. システム上で必要なすべてのサービスが実行されていることを確認します
B. Windowsファイアウォールを有効にする
C. ホスト上のSSLとTLSを無効にする
D. 利用可能なアプリケーションクラッシュログファイルを削除します
Answer: A (メーッセージを残す**)**
センサーのインストール失敗をトラブルシューティングする際の有効な手順は、システム上で必要なすべてのサービスが実行されていることを確認することです。これは、センサーが正常に機能するために必要なセンサーサービス、Windows Management Instrumentationサービス、またはWindowsリモート管理サービスに問題があるかどうかを特定するのに役立ちます。その他のオプションは、センサーのインストール失敗のトラブルシューティングには不適切であるか、役に立ちません。

最新問題: **44**
MacOS に Falcon Sensor をインストールする一般的なプロセスを最もよく表すオプションはどれですか?

A. Falcon パッケージにフルディスクアクセスを許可し、Falcon パッケージをインストールし、falconctl を使用してセンサーのライセンスを取得します。
B. コマンドラインでインストールトークンを渡してFalconパッケージをインストールします。
C. Falcon パッケージをインストールし、falconctl を使用してセンサーのライセンスを取得し、システム拡張を承認し、センサーにフルディスクアクセスを許可します。
D. Falcon パッケージにフルディスクアクセスを許可し、Falcon パッケージをインストールし、コマンド 'falconctl stats' を使用して Falcon Sensor をロードします。
Answer: C (メーッセージを残す**)**
macOS に Falcon Sensor をインストールする一般的な手順は、Falcon パッケージをインストールし、falconctl を使用してセンサーのライセンスを取得し、システム機能拡張を承認し、センサーにフル ディスク アクセスを許可するというものです。Falcon パッケージにはセンサー バイナリとカーネル機能拡張が含まれており、これをダブルクリックするか、インストーラなどのコマンド ライン ツールを使用してインストールできます。falconctl ツールは、macOS システムでセンサーを設定および管理できるコマンド ライン ユーティリティです。falconctl を使用してカスタマー ID (CID) と、オプションでセンサー グループ ID (SGID) を入力することで、センサーのライセンスを取得できます。センサーのライセンスを取得したら、システム環境設定のセキュリティとプライバシー設定でシステム機能拡張を承認する必要があります。この承認には再起動が必要です。最後に、システム環境設定のプライバシー設定でセンサーにフル ディスク アクセスを許可する必要があります。これにより、センサーがファイルとフォルダーを監視および保護できるようになります。

最新問題**: 45**
Falcon Next-Gen AntiVirus (NGAV) に関して正しいのは次のうちどれですか?
A. Falcon NGAVはシグネチャベースの検出に依存しています
B. Falcon NGAV を有効にすると、ポリシー全体のすべての検出および防止設定も有効になります。
C. 検出スライダーは防止スライダーよりも低い値に設定することはできません。
D. Falcon NGAV は Windows Defender や他のウイルス対策プログラムの代替ではありません
Answer: C (メーッセージを残す**)**
Falcon Next-Gen AntiVirus (NGAV) では、検出スライダーを予防スライダーよりも低い値に設定することはできません。これは、予防は検出の一部であり、検出されない脅威を予防しても意味がないためです。その他のオプションは、Falcon NGAV では正しくないか、または該当しません。

最新問題**: 46**

エージェントのインストール後、エージェントはポート 443 経由で永続的な___接続を開き、エンドポイントがオフになるかネットワーク接続が終了するまでその接続を開いたままにします。
A. SSH
B. TLS
C. HTTP
D. TCP
Answer: (解答を表示する**)**
エージェントのインストール後、エージェントはポート443を介して永続的なTLS接続を確立し、エンドポイントの電源がオフになるかネットワーク接続が終了するまでその接続を維持します。TLS（Transport Layer Security）は、エージェントとFalconクラウド間の安全で暗号化された通信を提供するプロトコルです。ポート443は、HTTPS（Hypertext Transfer Protocol Secure）トラフィックの標準ポートです。エージェントはこの接続を使用して、Falconクラウドとの間でデータ、コマンド、ポリシー、およびアップデートを送受信します。

最新問題**: 47**
次のオプションのうち、センサーベースの機械学習 (ML) にのみ備わっている機能はどれですか。
A. 次世代アンチウイルス (NGAV) 保護
B. アドウェアおよび潜在的に不審なプログラムの検出と防止
C. リアルタイムオフライン保護
D. 未知の実行ファイルの識別と分析
Answer: D (メーッセージを残す**)**
ドキュメント (documentation/detections/technique/sensor-based-ml-cst0007) によると:
CrowdStrikeのセンサーベースの機械学習（ML）は、ホスト上で実行される未知の実行ファイルを識別・分析します。この手法は、既知のマルウェアに関連付けられたファイルとファイル属性によって実行されます。これは[クラウドベースML](/support/documentation/detections/technique/cloud-based-ml)手法に類似しています。クラウドベースMLは、実行ファイルのグローバル分析に基づいてマルウェアを分類・識別します。主な違いは、ホストがオフラインの場合には実行されないことです。

最新問題: **48**
防止ポリシーに設定する適切な機械学習レベルを決定するのに役立つレポートはどれですか?
A. センサーレポート
B. 機械学習による予防監視
C. Falcon UI 監査証跡
D. 機械学習デバッグ
Answer: B (メーッセージを残す**)**
「防止ポリシー管理」オプションの「機械学習防止モニタリング」レポートを使用すると、機械学習（ML）防止設定が環境に与える影響を監視できます。ML検出数と防止数を、重大度、ポリシー、ホストグループ別に確認できます。また、特定のイベントやホストにドリルダウンして詳細を確認することも可能です。このレポートは、リスク許容度とセキュリティ体制1に基づき、防止ポリシーで設定すべき適切なMLレベルを決定するのに役立ちます。

最新問題: **49**
センサーは CrowdStrike Cloud と通信するためにどのポートとプロトコルを使用しますか?
A. TCP ポート 22 (SSH)
B. TCP ポート 443 (HTTPS)
C. TCP ポート 80 (HTTP)
D. TCP UDP ポート 53 (DNS)
Answer: B (メーッセージを残す**)**
センサーはCrowdStrike Cloudとの通信にTCPポート443（HTTPS）を使用します。このポートとプロトコルは、検知情報、ポリシー、アップデート、コマンドなどのデータをセンサーとクラウド間で安全に送受信するために使用されます。その他のオプションは正しくないか、センサーによって使用されていません。

最新問題: **50**
あなたのリーダーシップは、Overwatch による検出に対して即座に対応するための制御を導入したいと考えています。
ホストを速やかに封じ込め、適切なスタッフに通知するにはどうすればよいでしょうか?
A. Overwatchプレイブックを使用してFusion SOARワークフローを作成し、ホストを封じ込めてSOCチームにメールを送信します。
B. Overwatch検出時にトリガーするFusion SOARワークフローを作成し、検出をブロックするように設定します。
C. Fusion SOARワークフローを作成してOverwatchの検出を作成し、SOCチームにメールを送信します。
D. ホストを包含し、Overwatch チームに電子メールを送信する Fusion SOAR ワークフローを作成します。

Answer: (解答を表示する)

最新問題: **51**
Falcon コンソール内のホストのセットアップと管理を使用して、機能制限モード (RFM) でセンサーを表示するにはどうすればよいですか?
A. ホスト管理からRFMをフィルタリング
B. ホストステータスからRFMをフィルタリング
C. センサーの状態から、列見出し 『センサーの状態」を使用して並べ替えます。
D. センサーステータスからウィジェットをクリックします: RFM
Answer: D (メーッセージを残す)

最新問題: **52**
Falcon プラットフォームのどこで、特定のホストにインストールされているセンサー ビルド バージョンを確認できますか?
A. エグゼクティブサマリーダッシュボードを表示するダッシュボード
B. センサービルドをフィルタリングし、ホストを選択することでセンサーダウンロードページが表示されます。
C. ホスト管理ページでホストをフィルタリングして選択する
D. センサーレポートツールをダウンロードしてツールダウンロードページにアクセスします
Answer: C (メーッセージを残す)

最新問題: **53**
『次世代アンチウイルス: クラウド機械学習」設定には 2 つのカテゴリがあり、1 つは 『クラウド アンチマルウェア」で、もう 1 つは次のカテゴリです。
A. アドウェアとPUP
B. 高度な機械学習
C. センサーマルウェア対策
D. 実行ブロッキング
Answer: A (メーッセージを残す)
EDRライセンスをお持ちの場合、『監査ログ > 機械学習による防御モニタリング」に移動すると、クラウドマルウェア対策、センサーマルウェア対策、アドウェア＆PUPの3つのオプションが表示されます。したがって、答えはAです。

最新問題: **54**
環境内のホストがネットワークで隔離されている間も、新しいパッチサーバーにアクセスできるようにする必要があります。サーバーのIPアドレスは静的で、変更されません。これを可能にするために隔離ポリシーを更新する最適な方法は、次のうちどれですか？
A. 個々のサーバーのMACアドレスの許可リストエントリを追加します
B. サーバーが属するホストグループを含む許可リストエントリを追加します

C. 個々のサーバーのIPアドレスの許可リストエントリを追加します
D. サーバーが属する /24 ネットワークの CIDR 表記を含むホワイトリストエントリを追加します。
Answer: (解答を表示する**)**
環境内のホストがネットワークで隔離されている間もアクセス可能な新しいパッチサーバーを許可するように隔離ポリシーを更新する最適な方法は、個々のサーバーのIPアドレスに対してホワイトリストエントリを追加することです。ホワイトリストエントリを使用すると、隔離されたホストと通信できる信頼できるIPアドレスのリストを定義できます。これにより、パッチサーバーなどの重要なリソースやサービスへのアクセスを許可しながら、ホストをネットワークから分離できます。サーバーのIPアドレスが静的で変更されない場合は、ホストグループやネットワーク範囲を追加するよりも、個々のIPアドレスを追加する方が正確かつ安全です。

最新問題: **55**
ホスト上の検出を無効にすると、API にどのような影響がありますか?
A. 検出が無効になっているエンドポイントは、検出が再度有効になるまで何も警告しません。
B. エンドポイントの検出を個別に無効にすることはできません
C. DetectionSummaryEvent は、そのホストのストリーミング API への送信を停止します。
D. 検出が無効になっているエンドポイントは、設定が変更された場合、24時間（デフォルト）またはそれ以上の間、何も警告しません。
Answer: C (メーッセージを残す**)**
ホスト上の検出を無効にすると、そのホストのストリーミングAPIへのDetectionSummaryEventの送信が停止されます。つまり、ホストはストリーミングAPIに検出イベントを送信しなくなります。ストリーミングAPIは、Falcon Cloudから外部アプリケーションやシステムへのデータストリーミングに使用されます。その他のオプションは、正しくないか、ホスト上の検出の無効化とは関係ありません。

最新問題: **56**
検出を無効にする機能が役立つのはなぜですか?
A. ユーザーにホストからセンサーをアンインストールする機能を提供します
B. ユーザーはホストを設定して検出をテストし、後でコンソールから削除することができます。
C. ユーザーに誤検出を許可リストに登録する機能を提供します
D. アンインストールされたホストからすべてのデータを削除する権限をユーザーに付与します。
Answer: (解答を表示する**)**

最新問題: **57**

センサーが CrowdStrike Cloud と通信できるようにするには、必要な許可リストにどのインターネット ドメインを追加する必要がありますか?
A. cloudprotect-cs.net
B. csfalcon.net
C. cloudsink.net
D. falconcloud.net
Answer: C (メーッセージを残す)

最新問題: **58**
ホスト管理ページから、ドメイン コントローラーがセンサーのバージョン情報を取得するためにフィルター処理するのに最適なフィールドは何ですか?
A. センサーバージョン
B. プラットフォーム
C. OSバージョン
D. タイプ
Answer: (解答を表示する)

最新問題: **59**
ログオンアクティビティレポートに関して正しいのは次のうちどれですか?
A. ユーザーのログオンアクティビティとユーザーが接続したホストのグラフィカルビューを表示します。
B. レポートはコンピュータ名でフィルタリングできます
C. ユーザーのすべてのログオンアクティビティの詳細なリストを表示します。
D. ユーザーの最後のログオンアクティビティの概要のみを表示します。
Answer: (解答を表示する)
ログオンアクティビティレポートは、ユーザーのログオンアクティビティとユーザーが接続したホストをグラフで表示しますが、表示されるのはユーザーの最後のログオンアクティビティの概要のみです。ユーザーのすべてのログオンアクティビティの詳細なリストは表示されず、コンピュータ名でフィルタリングすることもできません。その他のオプションは、レポートの内容に誤りがあるか、または該当しません。

最新問題: **60**
ホスト上のペンテストおよびセキュリティ ツールを使用して検出をテストします。ペンテストに関連する検出をリアルタイムで自動的に自分に割り当てるワークフローを作成するにはどうすればよいでしょうか?
A. テストが完了するまでホストの検出を無効にするワークフローを作成します
B. EPP検出時にトリガーされ、その検出を自分に割り当てるアクションを含むイベントトリガーワークフローを作成します。

C. EPP検出時にトリガーされるイベントトリガーワークフローを作成します。このワークフローでは、必要なホスト名を検索する条件が設定されます。その後、アクションによって検出が自分自身に割り当てられます。
D. 1日に1回実行されるワークフローをスケジュール設定します。このワークフローは、EPP検出時にトリガーされ、条件として指定されたホスト名を検索します。アクションによって、検出結果が自分自身に割り当てられます。
Answer: (解答を表示する**)**

最新問題**: 61**
センサー更新ポリシーに関する優先順位の目的は何ですか?
A. 優先順位は防止ポリシーに適用され、センサー更新ポリシーには適用されません。
B. 複数のポリシーに割り当てられたホストは、リスト内で最も高いランクのポリシー（最も番号の小さいポリシー）が適用されます。
C. 複数のポリシーに割り当てられたホストは、リスト内で最も低いランクのポリシー（最も高い番号のポリシー）が適用されます。
D. 優先順位により、競合するポリシー設定が同じポリシーに設定されないようにします。
Answer: B (メーッセージを残す**)**
センサー更新ポリシーに関する優先順位の目的は、複数のポリシーに割り当てられたホストが、リスト内で最もランクの高いポリシー (番号が最も小さいポリシー) を想定することです。
つまり、ホストが複数のグループに属し、それぞれに異なるセンサー更新ポリシーが割り当てられている場合、それらのグループの中で最も優先順位が高い（最も低い番号）ポリシーが使用されます。その他のオプションは正しくないか、優先順位とは関係ありません。

最新問題**: 62**
API 監査証跡レポートではどのような情報が提供されますか?
A. アナリストのログインアクティビティのリスト
B. 予防政策の具体的な変更点のリスト
C. Falcon OAuth2ベースのAPI経由で実行されたアクションのリスト
D. 新しく追加されたホストのリスト
Answer: (解答を表示する**)**

API監査証跡レポートは、Falcon OAuth2ベースのAPIを介して実行されたアクションのリストを提供します。API監査証跡レポートを使用すると、組織内の様々なAPIクライアントとユーザーによるFalcon APIのアクティビティと使用状況を表示および監査できます。このレポートを使用して、Falcon APIを介して誰が、いつ、どのようにデータにアクセスしたかを監視できます。

最新問題: **63**
リアルタイム レスポンス (RTR) 監査ログにはどのような情報が含まれていますか?
A. 監査ログではリアルタイムレスポンス（RTR）情報は収集されません
B. セッションの開始時刻、期間、ユーザー、ホスト名、使用されたコマンド、取得されたファイル
C. セッション終了時刻、コマンドの戻り値、ファイルアクティビティ
D. IP アドレス、防止ポリシー、最近の検出、ホスト グループの割り当て
Answer: B (メーッセージを残す**)**

最新問題: **64**
ホスト上のファイルを隔離するには、どのような防止ポリシー設定を有効にする必要がありますか?
A. 行動ベースの脅威防止スライダーと高度な修復アクションを有効にする
B. マルウェア対策とWindowsマルウェア対策実行ブロックを有効にする
C. 次世代アンチウイルス対策スライダーと 隔離とセキュリティセンター登録」を有効にする
D. マルウェア対策とカスタム実行ブロックを有効にする
Answer: C (メーッセージを残す**)**
次世代アンチウイルス対策のスライダーと 隔離とセキュリティセンターへの登録」を有効にするオプションは、マルウェア対策とWindowsアンチマルウェア実行ブロックを有効にすることです。マルウェア対策は、次世代アンチウイルス対策のスライダーを有効にする機能で、Falconセンサーの機械学習エンジンの感度と攻撃力を調整できます。Falconセンサーは、人工知能を用いて未知の脅威を識別 阻止します。
Windows マルウェア対策実行ブロックは、 検疫とセキュリティ センター登録」設定を有効にする機能で、悪意のあるファイルを検疫し、Windows セキュリティ センターに登録することができます。

最新問題: **65**
環境内のリスクの高い RTR コマンドにセキュリティの層を追加したいと考えています。UI 内で RTR の MFA をどこで設定しますか?
A. 一般設定
B. 対応ポリシー
C. 包含ポリシー
D. ホストグループ

Answer: B (メーッセージを残す)

最新問題: **66**
ワークフロー条件はどのような 3 つの要素で構成されますか?
A. パラメータ、演算子、値
B. 始まり、中間、そして終わり
C. トリガー、アクション、アラート
D. 通知、アラート、API
Answer: A (メーッセージを残す)
ワークフロー条件は、パラメータ、演算子、および値で構成されます。ワークフロー条件とは、特定の基準またはフィルターに基づいてワークフローをトリガーするタイミングを定義するルールです。パラメータとは、重大度、戦術、ホストグループなどの検出イベントをフィルタリングまたは照合するために使用できる変数または属性です。演算子とは、パラメータと値を比較または評価する方法を指定する記号または単語です（等しい、含む、より大きいなど）。値は、高、資格情報ダンプ、デフォルトグループなど、パラメータに対して期待される結果または望ましい結果を提供する定数または式です。

最新問題: **67**
カスタムアラートを使用すると、_____が可能になります。
A. 任意の間隔でアラートを実行するようにスケジュールする
B. メールでアラートを受信する
C. アラートの防止アクションを設定する
D. リアルタイムでアクティビティを通知します
Answer: B (メーッセージを残す)
レポート間隔は事前に定義されており、変更できません。カスタムアラート機能の有効化/無効化と、アラート/検出の送信先メールクライアントの追加/削除のみ可能です。

最新問題: **68**
CrowdStrike が開発した次のツールのうち、CrowdStrike Windows Falcon Sensor の削除に役立つものはどれですか?
A. CSUninstallTool.exe
B. FalconUninstall.exe
C. CrowdStrikeRemovalTool.exe
D. UninstallTool.exe
Answer: A (メーッセージを残す)

最新問題: **69**
あなたは組織の Falcon 管理者であり、Falcon ユーザーが行うアクションに対して責任を負っていることを保証したいと考えています。
Falcon 内の監査ログの保存期間はどれくらいですか?

A. 180日
B. 30日間
C. 1年
D. 90日間
Answer: D (メーッセージを残す)

最新問題: **70**
異なる防止ポリシー設定でブロックされたアクティビティの量を判断するために使用できる Falcon のレポートはどれですか?
A. Falcon防止ポリシーのデバッグ
B. 予防ポリシー監査証跡
C. 機械学習による予防監視
D. センサーの可視性除外監査
Answer: C (メーッセージを残す)

最新問題: **71**
特定のホスト名について、過去24時間以内に行われたすべての削除リストをエクスポートする必要があります。最適な方法は何ですか？
A. ホストページのホスト管理に移動します。ホストを選択し、 検出結果をエクスポート」ボタンを使用します。
B. 検出解決ダッシュボードを活用します。フィルターを使用して適切なホスト名と時刻に絞り込み、 検出解決履歴」セクションから結果をエクスポートします。
C. 調査モジュールで 検出アクティビティ」ページにアクセスします。フィルターを使用して適切なホスト名と時刻に絞り込み、結果をエクスポートします。
D. 検出アクティビティダッシュボードを活用します。フィルターを使用して適切なホスト名と時刻に絞り込み、 ホスト別検出」セクションから結果をエクスポートします。
Answer: C (メーッセージを残す)
特定のホスト名で過去24時間内に行われたすべての削除リストをエクスポートする最適な方法は、 調査」モジュールの 検出アクティビティ」ページにアクセスし、フィルターを使用して適切なホスト名と時刻に絞り込み、結果をエクスポートすることです。これにより、その期間にそのホストで削除されたすべての検出情報を含むCSVファイルをダウンロードできます。その他のオプションは、正しくないか、削除のエクスポートとは関係ありません。

最新問題: **72**
ホストが含まれている場合でも、ホストが常に通信できる IP アドレスを許可する構成をどこに適用しますか?
A. 対応ポリシー
B. メンテナンストークン
C. IP許可リスト管理

D. 封じ込めポリシー
Answer: D (メーッセージを残す**)**

最新問題**: 73**
組織のセキュリティ体制を改善するために、Falcon によって重大な脆弱性が検出された場合にアラートを生成する Fusion SOAR ワークフローを設計しています。
新しいワークフローを最初から作成する場合、最初にワークフローのどのコンポーネントを構成する必要がありますか?
A. 条件
B. アクション
C. トリガー
D. ワークフロー名
Answer: C (メーッセージを残す**)**

最新問題**: 74**
検出ページから動作検出を除外できるオプションはどれですか?
A. 機械学習の除外
B. IOA除外
C. IOC除外
D. センサーの可視性除外
Answer: B (メーッセージを残す**)**
IOA 除外は、CrowdStrike によって生成された検出に基づく IOA のすべての動作検出と防止を停止します。

最新問題**: 75**
Falcon UI 監査証跡レポートには、次のどれが記載されていますか?
A. APIのみによって実行されたアクションの監査記録
B. Falconインスタンスの課金の監査記録
C. ユーザーのみが実行したアクションの監査記録
D. ユーザーとAPIクライアントの両方によって実行されたアクションの監査記録
Answer: (解答を表示する**)**

最新問題**: 76**
機械学習防止監視レポートの目的は何ですか?
A. 管理者が機械学習の積極性設定と実際に隔離されたアイテムの数を簡単に把握できるように設計されています。
B. アナリストが隔離されたすべてのアイテムを表示し、悪意がないと判断されたアイテムを解放するために使用するダッシュボードです。
C. 機械学習による予防策を確認するためのダッシュボードであり、アクティビティの急増や標的型攻撃の可能性を特定するために使用されます。

D. 異なる機械学習防止設定に基づいて、環境内でブロックされるマルウェアを表示するように設計されています。
Answer: D (メーッセージを残す**)**
機械学習防止監視ダッシュボード: このダッシュボードを使用して、さまざまな機械学習防止設定 (注意、中、積極的、または非常に積極的) に基づいて、選択した期間に環境内でブロックされたマルウェアを表示します。

最新問題: **77**
リアルタイム レスポンス (RTR) による Windows システム調査中に、RTR アクティブ レスポンダーは特定のシステム アーティファクトを見つけるためのカスタム PowerShell スクリプトを実行できません。
レスポンダーが PowerShell スクリプトを実行できない原因は何でしょうか?
A. 応答者にはRTR管理者の役割が必要です
B. 応答ポリシーで Put-and-Run が有効になっていません
C. スクリプトベースの実行監視は防止ポリシーで有効になっていません
D. レスポンスポリシーでカスタムスクリプトが有効になっていません
Answer: D (メーッセージを残す**)**

最新問題: **78**
センサー更新ポリシーの「自動 - 最新」設定の目的は何ですか?
A. この設定は、オンラインになる新しいホストにこのポリシーを自動的に割り当てます。
B. この設定により、割り当てられたすべてのホストが最新バージョンが利用可能になるとすぐに更新されます。
C. この設定により、選択したエンドポイントに最新の攻撃指標 (IOA) プロファイルと次世代アンチウイルス (NGAV) 機械学習が自動的に割り当てられ、最高レベルのセキュリティが確保されます。
D. この設定は、ユーザーの確認/操作を上書きし、選択したポリシーを適用します。
Answer: (解答を表示する**)**

最新問題: **79**
「ホストの設定と管理 > ホスト管理」ページ内のフィルターはどれですか?

A. ユーザー名
B. あなた
C. BIOSバージョン
D. 地域
Answer: (解答を表示する**)**
OU（組織単位は、 Hストの設定と管理」> Hスト管理」ページ内のフィルターです。ホスト管理ページでは、環境内でFalconセンサーがインストールされているすべてのホストを表示および管理できます。ホスト名、グループ、OSバージョン、センサーバージョン、最終検出日、ヘルスイベント、検出、および防止でホストをフィルタリングできます。また、Active Directoryドメイン構造に基づいてホストを論理的にグループ化したOUでフィルタリングすることもできます。

最新問題**: 80**
ホスト管理ページからホストの 検出を無効にする」をクリックした後、コンソールの検出はどうなりますか?
A. ホストの検出はコンソールから直ちに削除されます。今後、コンソールに新しい検出は表示されません。
B. ホストの既存の検出がコンソールから削除されます。これらの検出をトリガーしたプロセスは、今後のアラートを防止するために許可リストに登録されます。他のアラートの検出には影響しません。
C. ホストの既存の検出はそのまま残ります。今後、コンソールに新しい検出は表示されません。
D. ホストからの検出は7日間一時停止されます。ホストからの既存の検出は24時間以内にコンソールから削除されます。
Answer: C (メーッセージを残す**)**

最新問題**: 81**
Falcon管理者は Servers」グループに適用する新しい防止ポリシーを作成しましたが、新しい防止ポリシーを適用しても、このグループが利用可能なグループのリストに表示されません。考えられる原因は何でしょうか？
A. 新しい防止ポリシーを最初に有効にする必要があります
B. Servers」グループにはすでにポリシーが適用されています
C. まず Servers」グループを無効にする必要があります
D. ホストタイプが防止ポリシー内で正しく定義されていません
Answer: B (メーッセージを残す**)**
Servers」グループに新しい防止ポリシーを適用できない原因として最も可能性が高いのは、 Servers」グループに既にポリシーが適用されていることです。防止ポリシーとは、ホスト上のFalconセンサーの防止機能と設定を定義するポリシーです。環境内の異なるホストまたはグループに、カスタム防止ポリシーを作成して割り当てることができます。ただ

し、一度に1つのホストまたはグループに割り当てることができる防止ポリシーは1つだけです。ホストまたはグループに既に防止ポリシーが適用されている場合は、既存のポリシーを削除または置き換えない限り、別の防止ポリシーを適用することはできません。

最新問題: **82**
可視性レポートの Logan アクティビティにはどのような情報が提供されますか?
A. すべてのユーザーのすべてのログオンのリスト
B. ユーザーが最後にログインしたエンドポイントのリスト
C. ローカルIPとローカルポートに基づいてデバイスにリモートログオンしているユーザーのリスト
D. 国に基づいてデバイスにリモートログオンしている一意のユーザーのリスト
Answer: B (メーッセージを残す**)**
可視性レポートの「ログオンアクティビティ」レポートには、ユーザーが最後にログインしたエンドポイントのリストが表示されます。このレポートには、各ログオンイベントのユーザー名、ドメイン名、ログオンの種類、ログオン時刻、エンドポイント名が表示されます。その他のオプションは正しくないか、レポートに関連しません。

最新問題: **83**
除外を適用できるものは何ですか?
A. 管理者が選択した個々のホスト
B. すべてのホストまたは指定されたグループ
C. デフォルトのホストグループのみ
D. 管理者が選択したグループのみ
Answer: B (メーッセージを残す**)**
除外対象を指定するオプションは、すべてのホストまたは特定のグループに適用できることです。除外とは、Falconセンサーによる検出または防御の対象から除外するファイル、フォルダ、プロセス、IPアドレス、またはドメインを定義するルールです。除外は、Falconコンソールの「除外」ページで作成および管理できます。環境内のすべてのホスト、または選択した特定のホストグループに除外を適用できます。管理者が選択した個々のホストに除外を適用することはできません。

最新問題: **84**
API シークレットをリセットするにはどうすればよいでしょうか?
A. リセットを要求するサポートチケットを作成します
B. 一般設定経由
C. APIクライアントの3つのドットメニューから
D. シークレットをリセットできないため、新しいAPIクライアントが必要です
Answer: C (メーッセージを残す**)**

最新問題: **85**

サポートされているオペレーティング システムのバージョンに関する情報は、Falcon コンソールのどこにありますか?
A. 構成モジュール
B. インテリジェンスモジュール
C. サポートモジュール
D. モジュールの検出
Answer: (解答を表示する**)**
サポートされているオペレーティングシステムのバージョンに関する情報は、Falconコンソールのサポートモジュールで確認できます。このモジュールでは、ドキュメント、ダウンロード、FAQ、リリースノート、システムステータスなど、様々なサポートリソースにアクセスできます。このモジュールで利用できるドキュメントの一つに、CrowdStrikeセンサー互換性リストがあります。このリストには、各センサータイプとプラットフォームでサポートされているオペレーティングシステムのバージョンが記載されています。その他のオプションは、正しくないか、サポートされているオペレーティングシステムのバージョンに関する情報の検索とは関係ありません。

最新問題**: 86**
Falcon クラウドに接続しない非アクティブなホストは、何日後にホスト管理ページとゴミ箱ページから自動的に削除されますか?
A. 90日間
B. 60日間
C. 75日間
D. 45日間
Answer: (解答を表示する**)**
Falconクラウドに接続していない非アクティブなホストは、90日後にホスト管理ページとゴミ箱ページから自動的に削除されます。非アクティブなホストとは、7日間以上Falconプラットフォームと通信していないホストのことです。非アクティブなホストは、7日間非アクティブな状態が続くと、ホスト管理ページからゴミ箱ページに移動されます。非アクティブなホストは、ゴミ箱ページに90日間保存された後、Falconプラットフォームから完全に削除されます。非アクティブなホストが90日以内に再びアクティブになった場合は、ゴミ箱ページから復元できます。
90日間。

最新問題**: 87**
ホストがネットワークで封じ込められている場合でも、ネットワーク トラフィックを許可するポリシーは次のどれですか。
A. 封じ込め政策
B. レスポンスポリシー
C. ファイアウォールポリシー
D. IP許可リストポリシー

Answer: D (メーッセージを残す)

最新問題: **88**
管理者によって禁止されており、組織内でブロックする必要があるハッシュが 100 個あります。
Falcon を使用してこれを実現する最善の方法は何ですか?
A. 設定」> 「IOC管理」に移動します。このダッシュボード内で、カスタムIOを追加し、ハッシュのリストを追加します。アクションを 「ブロック」に設定します。防止ポリシーの 「実行ブロック」に 「カスタムブロック」が含まれていることを確認します。
B. 設定」> 「防止ポリシー」に移動します。このダッシュボードでIOCポリシーを追加します。ハッシュのリストをCSVファイルとして追加します。アクションを 「ブロックしてアラート」に設定します。 「実行ブロック」内の 「カスタムブロック」オプションが有効になっていることを確認します。
C. 設定」> 「IOC管理」に移動します。このダッシュボード内で、カスタム防止ポリシーを追加します。ハッシュのリストを追加します。アクションを 「ブロック」に設定します。ポリシーにカスタム実行ブロックが含まれていることを確認します。
D. 設定」> 「防止ポリシー」に移動します。このダッシュボードでIOCポリシーを追加します。ハッシュのリストをCSVファイルとして追加します。アクションを 「ブロック」に設定します。 「カスタム実行ブロック」オプションが有効になっていることを確認します。
Answer: A (メーッセージを残す)