CrowdStrike.CCFA-200.v2023-03-31.q34

試験コード：	CCFA-200
試験名称：	CrowdStrike Certified Falcon Administrator
認証ベンダー：	CrowdStrike
無料問題の数：	34
バージョン：	v2023-03-31
ページの閲覧量：	944
問題集の閲覧量：	7419

https://www.jpnshiken.com/shiken/CrowdStrike.CCFA-200.v2023-03-31.q34.html

質問: **1**
次のロールのうち、Falcon ユーザーがリアルタイム レスポンス カスタム スクリプトを作成できるのはどれですか?
A. リアルタイム レスポンダー - 読み取り専用アナリスト
B. リアルタイム レスポンダー - アクティブ レスポンダー
C. リアルタイム レスポンダー - スクリプト開発者
D. リアルタイム レスポンダー - 管理者
正解: **(**正解を表示します**)**

質問: **2**
検疫ファイルを管理できるのはどの役割ですか?
A. エンドポイント マネージャー
B. Falcon アナリスト - 読み取り専用
C. Falcon セキュリティ リード
D. 検出例外マネージャー
正解: **(**正解を表示します**)**

質問: **3**
あなたは Falcon 管理者ですが、「ホストへの接続」機能を使用して、ホストでのみ利用可能な追加情報を収集できないことに気付きました。この機能を使用するには、ユーザー アカウントにどの役割を追加する必要がありますか?
A. エンドポイント マネージャー
B. リアルタイム レスポンダー
C. ファルコン捜査官
D. 修復マネージャー
正解: **(**正解を表示します**)**

質問: **4**
Windows センサーが実行されている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. netstat -f
B. sc クエリ csagent
C. regedit myfile.reg
D. ps -ef | grepファルコン
正解: **(**正解を表示します**)**

質問: **5**
Falcon Cloud でセンサーのバージョンの変更をプッシュする必要がありますが、センサーのバージョンがいつアップグレードまたはダウングレードされるかを手動で制御することも必要です。Sensor の更新ポリシーで、これらの要件を満たすための最適な Sensor バージョン オプションはどれですか?
A. 自動 - N-1
B. 特定のセンサーのバージョン番号
C. センサーのバージョン アップデート オフ
D. 自動 - TEST-QA
正解: **(**正解を表示します**)**

質問: **6**
API クライアントを作成するときに、クライアントの作成後に再度表示できないため、すぐに保存する必要があるのは次のうちどれですか?
A. ベース URL
B. クライアント名
C. クライアント ID
D. シークレット
正解: **(**正解を表示します**)**

質問: **7**
センサーのインストール時に各センサーに割り当てられる Falcon の一意のホスト識別子の名前は?
A. エージェント ID (AID)
B. セキュリティ ID (SID)
C. エンドポイント ID (EID)
D. コンピュータ ID (CID)
正解: **(**正解を表示します**)**

質問: **8**
あなたの環境には、偽陽性である機械学習の検出が多数あると判断しました。これらは、ベンダーによってカスタム作成された単一のバイナリが原因であり、そのバイナリは多くのエンドポイントで実行されています。将来これらを防ぐ最善の方法は何ですか？

A. IOC 管理を使用して、問題のバイナリのハッシュを追加し、アクションを "ブロック、検出を非表示"に設定します。
B. IOC 管理を使用して、問題のバイナリのハッシュを追加し、アクションを "許可"に設定します。
C. IOC 管理を使用して、問題のバイナリのハッシュを追加し、アクションを "アクションなし"に設定します。
D. サポートに連絡して、この検出が含まれないように機械学習の設定を変更するよう依頼してください。
正解: **(**正解を表示します**)**

質問: **9**
防止ポリシーで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. 機械学習のデバッグ
C. Falcon UI監査証跡
D. 機械学習防止の監視
正解: **D (**コメントを発表する**)**

質問: **10**
エンド ユーザーに通知するポリシー設定がオンになっている場合、次のうちどれが正しいですか?
A. 悪意のあるアクターに検出を通知したくないため、エンド ユーザーには通知されません。この設定は存在しません
B. エンド ユーザーは、保留中の検疫を確認または拒否できるポップアップを受け取ります。
C. エンドユーザーは、防止アクションが発生したときにポップアップ通知を受け取ります
D. エンド ユーザーは、マシンがネットワーク内で隔離されていることをポップアップで即座に通知されます。
正解: **C (**コメントを発表する**)**

質問: **11**
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の詳細を開き、[新しいパスワードの生成] を選択します。
B. ユーザー固有の秘密/公開キー生成用の証明書が無効になっているため、管理者はユーザー管理からアカウントを再構築する必要があります。
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、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。
正解: **(**正解を表示します**)**

質問: **12**
1つまたは複数のホストグループに対する特定の防止ポリシーの調整は、Falcon内の次のどの場所で完了できますか?
A. ポリシーの調整は、ホスト アプリケーションの [ホスト管理] セクションで構成されます。
B. ポリシーの調整は、[構成] メニューの [一般設定] セクションで構成されます。
C. ポリシーの配置は、[割り当てられたホスト グループ] タブの各ポリシーで構成されます。
D. ポリシーの調整は、[Create New Policy] ポップアップ ウィンドウでポリシーを最初に作成するときに 1 回だけ構成されます。
正解: **(**正解を表示します**)**

質問: **13**
[ホストのセットアップと管理] > [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. 地方
C. OU
D. BIOS バージョン
正解: **(**正解を表示します**)**

質問: **14**
悪意はないが、あなたの会社が職場のコンピューターには不適切であると見なした 100 個のハッシュのリストが提供されました。彼らは、あなたの環境での実行が許可されていないことを確認するように依頼しました. これを行うために Falcon を使用することを選択しました。これを達成するための最良の方法はどれですか?
A. IOC 管理を使用して、各バイナリの SHA256 または MD5 ハッシュのリストを収集し、アップロードします。すべてのハッシュを 「ブロック」に設定し、これらのコンピューターが使用している防止ポリシーに、実行ブロックの下に 「カスタム ブロック」のオプションが含まれていることを確認します。
B. サポート ポータルを使用して、サポート チケットを作成し、バイナリ ハッシュのリストを含めて、これらのプロセスが実行されないように 「実行防止」ルールを作成するようサポートに依頼します。
C. Investigate アプリでカスタム アラートを使用し、テンプレート 「プロセス実行」を使用して新しいアラートを作成し、そのルール内で 「実行をブロックする」オプションを選択します。

D. API を使用して、各バイナリの SHA256 または MD5 ハッシュのリストを収集し、それらをアップロードして、すべて 許可しない」に設定します。
正解: **A** (コメントを発表する)

質問: **15**
環境に最適な防止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 [積極的] に構成します。この構成でセンサーを 1 週間テストした後、どの監査レポートを確認して、組織に最適な機械学習スライダー設定を決定する必要がありますか?
A. 機械学習防止の監視
B. 防止ハッシュは無視されます
C. 防止ポリシーの監査証跡
D. 防止ポリシーのデバッグ
正解: (正解を表示します)

質問: **16**
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どこで変更できますか?
A. 封じ込め方針
B. 防止ポリシー
C. ファイアウォール設定
D. ホスト設定
正解: (正解を表示します)

質問: **17**
Falcon センサーは、証明書のピン留めを使用して中間者攻撃を防御します。Falcon センサー証明書の検証に関して正しいのはどれですか?
A. 証明書のピニングに対する干渉の一般的な原因には、プロトコルの競合状態やリソースの競合などがあります
B. SSL 検査は、すべての Falcon トラフィックで発生するように構成する必要があります。

C. ディープ パケット インスペクションなどの一部のネットワーク構成は、証明書の検証に干渉します。
D. 証明書の検証を続行するには、HTTPS インターセプトを有効にする必要があります。
正解: **(**正解を表示します**)**

質問: **18**
センサーのアップグレード プロセスを手動で制御し、許可されていないユーザーがセンサーをアンインストールまたはアップグレードするのを防ぐために、センサー更新ポリシーのどの設定がこの基準を満たすでしょうか?
A. センサーのバージョン更新がオフで、アンインストールとメンテナンス保護がオフになっています
B. センサーのバージョンが N-2 に設定され、一括メンテナンス モードがオンになっている
C. センサーのバージョンが固定され、アンインストールとメンテナンス保護がオンになっています
D. センサーのバージョンが N-1 に設定され、一括メンテナンス モードがオンになっている
正解: **(**正解を表示します**)**

質問: **19**
次のうち、カスタム ブロック防止ポリシーの設定に当てはまるものはどれですか?
A. ハッシュ ブロックリストによってブロックされた実行は、ハッシュ計算プロセスの修正が必要になる前に部分的に実行された可能性があります
B. ブロックリストはハッシュ、IP アドレス、およびドメインに適用されます
C. このポリシーでハッシュをブロックする前に、[防止ハッシュ] ページにハッシュを入力する必要があります。
D. API 経由でのみハッシュをブロックリストに登録できます
正解: **(**正解を表示します**)**

質問: **20**
次のうち、[ホスト管理] ページで利用できないフィルターはどれですか?
A. ユーザー名
B. ホスト名
C. グループ
D. OS バージョン
正解: **(**正解を表示します**)**

質問: **21**
特定のホスト グループにポリシーを割り当てるにはどうすればよいですか?

A. ホスト管理で目的のホストにタグを割り当てます。そのタグに基づく割り当てルールでグループを作成します。目的のポリシーの [割り当て] タブに移動し、[グループをポリシーに追加] をクリックします。目的のグループを選択します。
B. 「動的割り当て」を使用して、目的のホストを含むグループを作成します。目的のポリシーの [割り当てられたホスト グループ] タブに移動し、OU、OS、ホスト名パターンなどの条件を選択します。
C. 「静的割り当て」を使用して、目的のホストを含むグループを作成します。目的のポリシーの [割り当てられたホスト グループ] タブに移動し、[グループをポリシーに追加] をクリックします。目的のグループを選択します。
D. 目的のポリシーの [割り当て] タブで、[静的] 割り当てを選択します。次のウィンドウから、目的のホストを選択し (必要に応じてフィッターを使用)、[追加] をクリックします。
正解: **(**正解を表示します**)**

質問: **22**
エスカレーション チームに電子メールを送信する重大な検出でトリガーされる既存のワークフローがあります。あなたの CISO は、カスタマイズされたメッセージを含む電子メールで通知を受けることも求めています。ワークフローを更新する最良の方法は何ですか?
A. CISO にカスタム メールを送信する並列アクションを追加します。
B. ワークフローを複製し、既存の電子メールを CISO の電子メールに置き換えます。
C. CISO の電子メールを既存のアクションに追加します。
D. カスタム メールを CISO に送信するシーケンシャル アクションを追加します。
正解: **(**正解を表示します**)**

質問: **23**
Falconでグループとポリシーを管理するには、どの役割が必要ですか?
A. 防止ハッシュ マネージャー
B. Falcon ホスト セキュリティ リード
C. Falcon ホスト管理者
D. Falcon ホスト アナリスト
正解: **(**正解を表示します**)**

質問: **24**
除外を作成する管理者は、いくつのホスト グループにルールを適用することに制限されていますか?
A. ファイルの除外がグループまたはホストに合わせられていません
B. 各除外は、ホストの 1 つのグループにのみ配置できます。
C. 制限はなく、一部またはすべてのグループに除外を適用できます
D. 除外に適用されるホストのグループは 3 つに制限されています
正解: **(**正解を表示します**)**

質問: **25**
次のオプションのうち、センサーベースの機械学習 (ML) でのみ使用できる機能はどれですか?
A. アドウェアおよび不審なプログラムの検出と防止
B. 未知の実行可能ファイルの識別と分析
C. リアルタイムのオフライン保護
D. 次世代アンチウイルス (NGAV) 保護
正解: **B (**コメントを発表する**)**

質問: **26**
Falconコンソールのどのページでセンサーグループを作成しますか?
A. ホスト グループ
B. ユーザー管理
C. ホスト管理
D. センサー更新ポリシー
正解: **(**正解を表示します**)**

質問: **27**
Windows センサー更新ポリシーで使用できる "自動" センサー バージョン更新オプションはいくつありますか?
A. 2
B. 1
C. 0
D. 3
正解: **(**正解を表示します**)**

質問: **28**
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. 正規表現
B. ヤラ
C. PowerShell
D. グロブ
正解: **(**正解を表示します**)**

質問: **29**
デフォルトのセンサー更新ポリシーを最もよく表しているのは次のうちどれですか?
A. デフォルトのセンサー更新ポリシーはデフォルトで無効になっています
B. デフォルトのセンサー更新ポリシーは 「キャッチオール」ポリシーです。
C. デフォルトのセンサー更新ポリシーは、センサー更新のテストにのみ使用されます

D. デフォルトのセンサー アップデート ポリシーには、「アンインストールとメンテナンス保護」機能がありません。
正解: **(**正解を表示します**)**

質問: **30**
機能制限モード (RFM) の Windows ホストが複数あることに気付きました。これらのホストが RFM 状態になる原因として最も可能性が高いのは何ですか?
A. センサー更新ポリシーが正しく構成されていません
B. パッチが夜間にすべての Windows システムにプッシュされました
C. ホストが 24 時間以上オフラインだった
D. ホストは、検出によりネットワーク封じ込めに配置されました
正解: **B (**コメントを発表する**)**

質問: **31**
[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 マルウェア対策」で、もう 1 つは次のとおりです。
A. 高度な機械学習
B. 実行ブロッキング
C. センサー アンチマルウェア
D. アドウェア & PUP
正解: **(**正解を表示します**)**

質問: **32**
次の機械学習 (ML) スライダーのうち、信頼性の高い悪意のあるアイテムのみを検出または防止するのはどれですか?
A. 注意
B. 最小
C. 普通
D. アグレッシブ
正解: **B (**コメントを発表する**)**

質問: **33**
セキュリティを強化するために、ドメインと IP アドレスのリストに基づいて検出およびブロックする必要があります。この目的を達成するために IOC マネジメントをどのように活用できますか?
A. IOC 管理を使用して、ハッシュと IP アドレスのリストをインポートし、アクションを防止/ブロックに設定します。
B. IOC 管理を使用して、ハッシュと IP アドレスのリストをインポートし、アクションを [検出のみ] に設定します。
C. ドメインと IP アドレスのブロックは、IOC 管理の機能ではありません。代わりにカスタム IOA ルールを使用する必要があります
D. IOC 管理を使用して、ハッシュと IP アドレスのリストをインポートし、アクションを [アクションなし] に設定します。
正解: **(**正解を表示します**)**

質問: **34**
環境内のすべてのワークステーションのホスト グループを作成する場合、すべてのワークステーション ホストを確実にグループに追加するには、どのような方法が最適ですか?
A. Type=Workstation Assignment で動的グループを作成します。
B. 動的グループを作成し、すべてのワークステーションをインポートします
C. Type=Workstation Assignment で静的グループを作成します。
D. 静的グループを作成し、すべてのワークステーションをインポートします
正解: **(**正解を表示します**)**