VMware.5V0-91.20.v2021-12-14.q42

試験コード：	5V0-91.20
試験名称：	VMware Carbon Black Portfolio Skills
認証ベンダー：	VMware
無料問題の数：	42
バージョン：	v2021-12-14
ページの閲覧量：	108
問題集の閲覧量：	422

https://www.jpnshiken.com/shiken/VMware.5V0-91.20.v2021-12-14.q42.html

質問: **1**

EDRユーザーインターフェイス内でフィードレポートを無視する3つの方法は何ですか？ 3つ選択してください。）

A. 脅威レポートの詳細ページ

B. 脅威インテリジェンスフィードページ

C. 調査ページ

D. 脅威レポートの検索ページ

E. アラートダッシュボードページ

F. フィードアラートを誤検知としてマークした後

正解 :(正解を表示します)

リファレンス：

防止−誤陽性/ ta-p / 64413

質問: **2**

[プロセス検索]ページでクエリを実行した後、この結果を確認します。丸で囲んだ黒い点に注意してください。

タグの下に表示される黒い点の意味は何ですか？

A. プロセスのイベントは調査でタグ付けされました。

B. プロセスの実行により、フィードヒットが発生しました。

C. プロセスの実行により、ウォッチリストがヒットしました。

D. プロセスのイベントもSyslogサーバーに送信されました。

正解 :(正解を表示します)

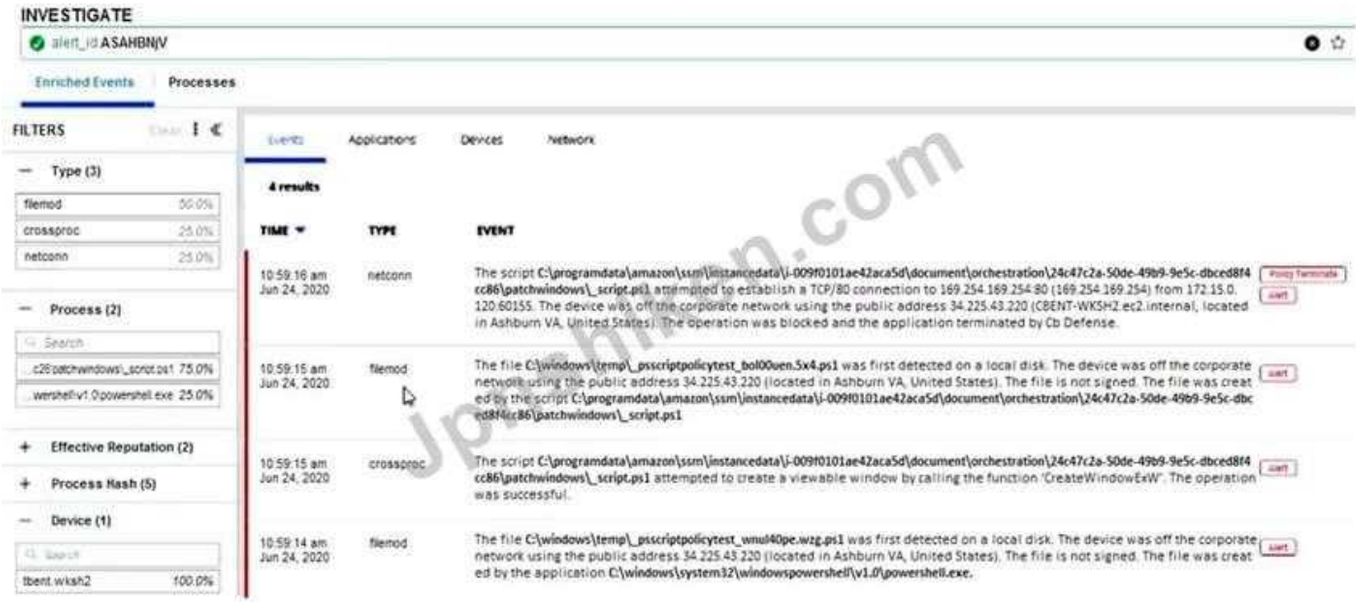
質問: **3**

Carbon Black Audit and Remediation管理者は、どの3つの頻度でライブクエリの実行をスケジュールできますか？ 3つ選択してください。）
A. 隔週
B. 毎週
C. 毎月
D. 毎日
E. 任意の頻度
F. 毎時
正解 :**(**正解を表示します**)**

質問**: 4**
EDRサーバーのUIを検索するときに正しい説明はどれですか？
A. 検索語間の空白はOR演算子を意味します。
B. 感嘆符！否定を表す文字です。
C. パーセント記号%は、ワイルドカードを表す文字です。
D. 円記号\は、文字をエスケープする文字です。
正解 :**C (**コメントを発表する**)**

質問**: 5**
以下のリストのうち、App Controlポリシーのすべての施行レベルを示していますか？
A. クリティカル、ロックダウン、監視、追跡、禁止
B. 高執行、中執行、低執行
C. 高施行、中施行、低施行、なし（可視性） なし（無効）
D. 制御、ローカル承認、無効
正解 :**(**正解を表示します**)**
リファレンス：
sa = t&rct = j&q = &esrc = s&source = web&cd = &ved = 2ahUKEwiFsPPz04XvAhWRsnEKHV4lBukQFjABegQIAhAD&url = https%3A%2F%2Fcommunity.carbonblack.com%2Fgbouw27325%2Fattachments%2Fgbouw2732Fproduct-docs-news%2F2961%2F1%2FVMware%2520Carbon%2520Black%2520App%2520Control%25208.5.0%2520User%2520Guide.pdf&usg = AOvVaw3es_0JTc8-_BifNR4iFiGl 6）

質問**: 6**
アナリストは、EndpointStandardで特定のアラートを調査しています。アナリストは、アラートトリアージページから調査ボタンを選択し、次の情報を確認します。



この状況を正確に特徴付けるステートメントはどれですか？

A. ポリシーにブロックルールと分離ルールが設定されていません。

B. リストされた各イベントは、全体的なアラートスコアと重大度に寄与しました。

C. 表示されるイベントはすべて同じイベントIDを持ち、アラートに関連付けられます。

D. これらのイベントは、ユーザーインターフェイス内で監視されたアラートに関連付けられています。

正解 :(正解を表示します)

質問: **7**

次のクエリがあるとします。

SELECT * FROMユーザーWHEREUID> = 500;

どのステートメントが正しいですか？

A. このクエリには有効性のパラメータがありません。

B. このクエリは、クラウドに送信された結果をフィルタリングします。

C. このクエリは、システムで見つかったすべてのアカウントを返します。

D. このクエリは、結果に表示する列の数を制限します。

正解 :**D** (コメントを発表する)

質問: **8**

組織は、一般的に使用されるソフトウェア配布ツールを活用して、エンタープライズソフトウェアの展開と更新を管理します。カスタムルールは、このツールによって配信されるファイルの承認を確実にするための適切なオプションです。

組織がこれらのファイルの大規模な承認のために構成できる他の信頼メカニズムはどれですか？

A. Windows Update

B. 信頼できるディストリビューター

C. Rapid Config

D. ローカル承認モード

正解 :**D** (コメントを発表する)

質問: **9**
未承認のファイルをブロックしないが、特に禁止されているファイルをブロックする施行レベルはどれですか？
A. 中程度の執行
B. 無効
C. 可視性
D. 低い施行
正解 :**B** (コメントを発表する)
説明
AppControlを実行しているコンピューターに適用される保護レベル
エージェント。高（ブロック未承認）からなしまでのレベルの範囲
（無効）必要ファイルブロックのレベルを指定できます。

質問: **10**
ライブレスポンスに関して正しい2つのステートメントはどれですか？（2つ選択してください。）
A. Live Responseは、リモートデバイスとのSSHセッションを開きます。
B. ライブレスポンスはユーザーインターフェースからのみ開始できます。
C. Live Responseは、エンドポイントのセッションごとに1人のユーザーをサポートします。
D. Live Responseは、センサーとサーバーの通信に同じチャネルを利用します。
E. Live Responseを使用するには、表示と管理の両方の権限が必要です。
正解 :**B,D** (コメントを発表する)

質問: **11**
エンドポイント（エージェント）を特定のポリシーに割り当てることができる、VMware Carbon Black App Controlで使用可能な3つの方法は何ですか？（3つ選択してください。）
A. DASCLIコマンド経由
B. 手動によるポリシーの割り当て
C. ブランド/ポリシー固有のインストーラーによる
D. SCCMを介してエージェントをインストールする
E. 指定されたGPOスクリプトをプッシュする
F. ActiveDirectoryマッピングによる
正解 :**B,D,F** (コメントを発表する)

質問: **12**
管理者は脅威インテリジェンスレポートをウォッチリストに変換して更新し、古い脅威インテリジェンスレポートを無効にする（無視する）必要があります。
UIのどこで、このアクションを実行できませんか？
A. 脅威レポートページ

B. 脅威レポートの検索ページ
C. トリアージアラートページ
D. 脅威インテリジェンスフィードページ
正解 :**D** (コメントを発表する)

質問: **13**
次のクエリがあるとします。
SELECT hostname、cpu_type、cpu_brand、cpu_physical_cores、cpu_logical_cores、cpu_microcode、
(1.0 * physical_memory / (1000 * 1000 *
1000)) AS physical_mem_gb、hardware_vendor、hardware_model、hardware_version、hardware_serial
FROM system_info; どのステートメントが正しいですか？
A. このクエリは、いくつかの異なるテーブルからのデータを結合します。
B. このクエリにはフィルターオプションがありません。
C. このクエリは、システムから返される結果をカスタマイズします。
D. このクエリは、physical_mem_gb列のデータを表示します。
正解 :**B** (コメントを発表する)

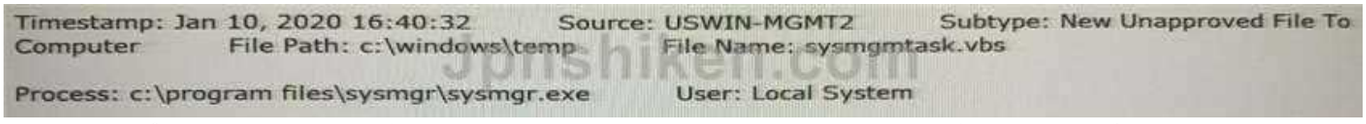
質問: **14**
展示を参照してください :

カーボンブラックライブレスポンス（CBLR）について正しい2つのステートメントはどれですか？ (2つ選択してください。)
A. CBLRセッションはすでに存在します。
B. CBLRセッションが接続されていません。
C. CBLRセッションが確立されます。
D. CBLRは無効です。
E. CBLRが有効になっています。
正解 :(正解を表示します)

質問: **15**
管理者は、SOCチームがApp ControlAPIを介してグローバルファイル禁止を作成できるようにするよう指示しました。
これはAppControl Consoleでどのように構成されますか？

A. ロールを作成し、対応するSOCグループにマップし、「ファイルの管理」権限をロールに追加して、グループ内の各ユーザーのAPIトークンを作成します。
B. 役割を作成し、対応するSOCグループにマップして、役割に「ファイルの管理」権限を追加します。
C. 「ファイルの管理」権限を追加し、SOCユーザーごとにAPIトークンを作成します。
D. ロールを作成し、対応するSOCグループにマップし、「ファイルの管理」権限を追加して、ロールのAPIトークンを作成します。
正解 :**D** (コメントを発表する)

質問: **16**
プロセスは、次のイベントで詳細に説明されているように実行可能ファイルを書き込みました。



将来そのプロセスによって書き込まれる同じ名前とパスのファイルが実行時にブロックされないようにするには、どのルールタイプを使用する必要がありますか？
A. Advances（書き込み無視）
B. ファイル作成制御
C. 信頼できるパス
D. 信頼できる発行元
正解 :**B** (コメントを発表する)

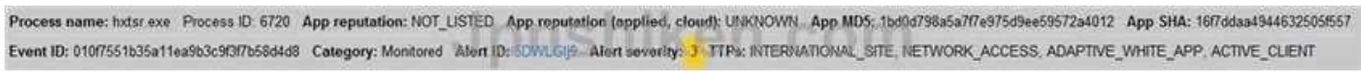
質問: **17**
Endpoint Healthのどのセンサーステータスが、システムのポリシー施行が無効になっていて、センサーがセキュリティイベントデータをクラウドに送信していないことを示していますか？
A. 検疫
B. 登録解除
C. 非アクティブ
D. バイパス
正解 :**D** (コメントを発表する)
リファレンス：
Bypass-has-been-Enabled-on-the / ta-p / 74905

質問: **18**
「任意の操作を実行する」および「任意のAPI操作を実行する」操作の試行でのみ使用できるアクションはどれですか。
A. バイパス
B. 許可とログ
C. 実行中または実行中
D. 許可する
正解 :**A (**コメントを発表する**)**
リファレンス：
sa = t&rct = j&q = &esrc = s&source = web&cd = &ved = 2ahUKEwjCIN7SwoXvAhViqnEKHbXpChUQFjAAegQIARAD&url = https%3A%2F%2Fcommunity.carbonblack.com%2Fgbouw27325%2Fattachments%2Fgbou2Fproduct-docs-news%2F1413%2F3%2Fcbd-userguide.pdf&usg = AOvVaw1CU0_RmjfwbwAh68IuEKAd（90）

質問: **19**
アナリストは、多数のHRワークステーションで複数のアラートを調査し、java.exeがPowerShellを試行していることを発見しました。問題のWindowsワークステーションのうち、アナリストはJavaが複数の場所にインストールされていることも発見しました。アナリストは、このタイプの操作からjava.exeをブロックする必要があります。
このニーズを満たすルールはどれですか？
A. ** / Program Files / * / java.exe->信頼できないプロセスを呼び出します–操作を拒否します
B. ** \ java.exe->コマンドインタープリターを呼び出します–操作を拒否します
C. ** / java.exe->信頼できないプロセスを呼び出します–>プロセスを終了します
D. ** \ Program Files \ * \ java.exe->コマンドインタープリターを呼び出します–>プロセスを終了します
正解 :**(**正解を表示します**)**

質問: **20**
別のAV /セキュリティ製品のEndpointStandardで除外を作成するために使用される戦略はどれですか？
A. バイパスモード
B. 許可規則
C. 分離ルール
D. 承認済みリスト
正解 :**D (**コメントを発表する**)**

質問: **21**
管理者は、ネットワーク接続を確立しているレピュテーションが不明なアプリケーションの[調査]タブで、次のイベントの詳細を確認します。



返されたイベントの詳細をさらに確認すると、レピュテーションはNOT_LISTEDとして監視され、適用された（クラウド）レピュテーションは不明です。

適用された（クラウド）レピュテーションが不明であり、NOT_LISTEDではないのはなぜですか？

A. アプリケーションはイベントの時点では不明でしたが、後でNOT_LISTEDであると判断されました。

B. NOT_LISTEDは、クラウドレピュテーションが適用されていないことから明らかなように、クラウドレピュテーションがないことを確認した後にセンサーによって適用されました。

C. センサーは、coudレピュテーションに基づいてローカルレピュテーションをUNKNOWNからNOT_LISTEDに降格しました。

D. センサーは、クラウドレピュテーションに基づいてローカルレピュテーションをNOT_LISTEDからUNKNOWNに降格しました。

正解 :**A (**コメントを発表する**)**

質問: **22**

Carbon Black Cloud Endpoint Standardのアナリストは、さまざまな検索演算子の組み合わせをテストしています。

同じ結果を生成する2つのクエリはどれですか？（2つ選択してください。）

A. process_name :chrome.exeまたはnetconn_domain :google.comではありません

B. process_name :chrome.exeであり、netconn_domain :google.comではありません

C. process_narne :chrome.exe NOT netconn_domain :google.com

D. process_name :chrome.exeまたはnetconn_domain :google.com

E. process_name :chrome.exe netconn_domain :google.com

正解 :**(**正解を表示します**)**

質問: **23**

ソフトウェアの発行元が名前のどこかにVMwareを含む行のみを返すようにデータをフィルタリングするステートメントはどれですか？

A. WHEREパブリッシャー= "%VMware%"

B. WHEREパブリッシャーLIKE "VMware%"

C. WHEREパブリッシャーLIKE "%VMware%"

D. WHEREパブリッシャー= "%VMware"

正解 :**(**正解を表示します**)**

質問: **24**

丸で囲んだ赤い点に注意して、展示を参照してください。

[プロセス検索]ページの[ヒット]の下にある赤い点の意味は何ですか？

A. プロセスの実行がセンサーヒットをもたらしたかどうか
B. プロセスの実行により、異なるユーザーのヒットが一致したかどうか
C. プロセスの実行によってsyslogヒットが発生したかどうか
D. プロセスの実行がフィードヒットをもたらしたかどうか
正解 :**(**正解を表示します**)**

質問**: 25**
管理者は、Carbon Black EnterpriseEDRでこのクエリを使用して電子メールクライアントの子プロセスを検索しています。
parent_name :outlook.exe OR parent_name :thunderbird.exe OR parent_name :eudora.exe管理者は、カーボンブラッククラウドで既知の評判を持たない子プロセスのみを表示するようにこのクエリを変更したいと考えています。
目的の結果を表示するためにクエリに追加できる検索フィールドはどれですか？
A. process_reputation
B. process_cloud_reputation
C. process_integrity_level
D. process_privileges
正解 :**(**正解を表示します**)**

質問**: 26**
イベントが発生したときのファイルレピュテーションを判断するためにアラートを確認するときに、管理者はどの値を使用する必要がありますか？
A. クラウドレピュテーション（初期）
B. 効果的な評判
C. 地元の評判
D. クラウドレピュテーション（現在）
正解 :**A (**コメントを発表する**)**

質問**: 27**
許可された管理者が、コンピューターからAppControlエージェントを削除することを計画しています。
エージェントをアンインストールする前に、コンピューターはどの施行レベルにある必要がありますか？
A. 可視性
B. なし（無効）
C. 任意の施行レベル
D. 低い施行
正解 :**(**正解を表示します**)**

質問**: 28**

展示を参照してください：

カーボンブラックライブレスポンス（CBLR）について正しい2つのステートメントはどれですか？ 2つ選択してください。）

A. CBLRは無効です。

B. CBLRが有効になっています。

C. CBLRセッションはすでに存在します。

D. CBLRセッションが接続されていません。

E. CBLRセッションが確立されます。

正解 :**(**正解を表示します**)**

質問**: 29**

管理者が次のクエリを実行しました。

SELECT名、VERSION、install_location、install_source、publisher、install_date、uninstall_stringFROMプログラムWHEREpublisher = "Microsoft Corporation"; 管理者は、インストールされている多くのプログラムが返されないことに気づきます。

管理者はどのようにしてクエリを変更してすべての結果を表示できますか？

A. WHERE句を= "*"に変更します

B. WHERE句を削除します

C. =をLIKEに置き換えます

D. WHERE句を編集して、引用符を削除します

正解 :**D (**コメントを発表する**)**

質問**: 30**

エンドポイントが追加または削除されるたびに、イベントアラートタイプの新しいアラートがどのように作成され、これらのイベントが発生するたびにApp Control管理者に電子メールが送信されますか？

A. サブタイプコンピューターのイベントプロパティにフィルターを追加し、コンピューターを削除しました。App Control管理者の電子メールを追加し、[作成して終了]をクリックします。

B. サブタイプコンピューターのイベントプロパティにフィルターを追加し、コンピューターを削除しました。[作成]をクリックしてAppControl管理者メールを追加し、[作成して終了]をクリックします。

C. サブタイプエンドポイントのイベントプロパティにフィルターを追加し、エンドポイントを削除しました。[作成]をクリックしてAppControl管理者メールを追加し、[作成＆]をクリックします。出口。

D. サブタイプコンピューターのイベントプロパティにフィルターを追加しました。App Control管理者の電子メールを追加し、[作成して終了]をクリックします。
正解 :**D** (コメントを発表する)

質問: **31**
[プロセス検索]ページでクエリを実行した後、この結果を確認します。丸で囲んだ黒い点に注意してください。

タグの下に表示される黒い点の意味は何ですか？
A. プロセスの実行により、フィードヒットが発生しました。
B. プロセスのイベントもSyslogサーバーに送信されました。
C. プロセスのイベントは調査でタグ付けされました。
D. プロセスの実行により、ウォッチリストがヒットしました。
正解 :**A** (コメントを発表する)

質問: **32**
エンタープライズEDR管理者には、[調査]ページの図にプロセスが表示されますが、このプロセスのアラートは表示されません。

管理者は、このウォッチリストに対する将来のヒットに対するアラートをどのように生成できますか？
A. ウォッチリストページでウォッチリストを選択し、[アラート :オフ]をクリックしてアラートをオンに切り替えます。

B. ウォッチリストページでウォッチリストを選択し、[アクションの実行]を使用して[編集]を選択し、[ヒット時にアラート]を選択します。
C. [ウォッチリスト]ページでウォッチリストを選択し、[スケジュールされたタスクの作成済み]レポートを選択し、[アクションの実行]を使用してレポートの[ヒット時にアラート]を選択します。
D. [ウォッチリスト]ページでウォッチリストを選択し、[スケジュールされたタスクの作成]レポートを選択し、[アクションの実行]を使用してヒット時のアラートをオンに切り替えます。
正解 :**B** (コメントを発表する)

質問: **33**
管理者は、ファイルがネットワーク共有から実行されることを許可したいと考えています。
管理者はどのルールタイプを設定する必要がありますか？
A. 書き込み承認（ネットワーク）
B. 信頼できるパス
C. ネットワーク実行（許可）
D. プロンプトの実行（共有パス）
正解 :(正解を表示します)

質問: **34**
管理者は、誰かがcmd.exeからの不正なコマンドを使用している可能性があることを懸念しています。これらのコマンドは疑わしいまたは悪意のあるものとは見なされず、それらに基づくポリシーはありません。
管理者はこれらのコマンドを見つけるためにどのページを使用する必要がありますか？
A. 調査する
B. アラート
C. センサー管理
D. ポリシー
正解 :**C** (コメントを発表する)

質問: **35**
管理者が[ポリシー]の[センサー設定]で[プライベートログレベルを有効にする]を選択するとどうなりますか？
A. レピュテーションが不明なスクリプトファイルはアップロードされません。
B. ライブレスポンスが無効になっています。
C. クラウドスキャンの遅延実行が無効になっています。
D. ドメイン名は難読化されています。
正解 :(正解を表示します)

質問: **36**
次のEDRクエリを確認します。

(parent_name :powershell.exe OR parent_name :cmd.exe) AND netconn_count :[1 TO *]クエリ結果に表示されるプロセスはどれですか？
A. 複数のネットワーク接続イベントでPowershell.exeまたはcmd.exeを呼び出すプロセス
B. 任意の数のネットワーク接続イベントでPowershell.exeまたはcmd.exeによって呼び出されるプロセス
C. 複数のネットワーク接続イベントを使用してPowershell.exeおよびcmd.exeを呼び出すプロセス
D. 単一のネットワーク接続イベントでPowershell.exeおよびcmd.exeによって呼び出されるプロセス
正解 :**D** (コメントを発表する)

質問: **37**
展示を参照してください：

センサーとサーバー間の通信に関して正しい説明はどれですか？
A. センサーはデフォルト以外のポートで通信します。
B. サーバーのホストファイルにcb.yourcompany.comのエントリが必要です。
C. 通信は暗号化されていません。
D. センサーはcb.yourcompany.comという名前を解決できる必要があります。
正解 :(正解を表示します)

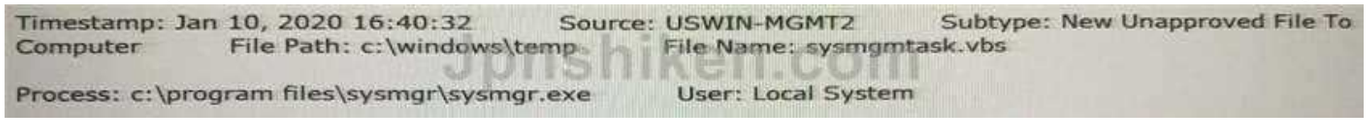
質問: **38**
管理者は、環境内の既知の必要なアプリケーションに関するアラートを確認しています。アプリケーションにはPUPのレピュテーションが与えられており、アラートの理由はPUPが検出されたことです。その結果、このアプリケーションは、環境内のPUPのポリシーのブロックと分離のルールに一致しており、期待どおりに動作していません。
この状況を修正するには、管理者はどの手順を実行する必要がありますか？
A. ファイルを禁止リストに追加してアプリケーションを削除します
B. ファイルを承認済みリストに追加します
C. ファイルを承認済みリストに追加してアラートを却下します
D. アラートを閉じます
正解 :(正解を表示します)

質問: **39**
管理者は、バイナリが署名されていないインスタンスを見つけたいと考えています。

この検索を実行する用語はどれですか？
A. process_publisher :FILE_SIGNATURE_STATE_NOT_SIGNED
B. process_publisher_state :FILE_SIGNATURE_STATE_NOT_SIGNED
C. not process_publisher :FILE_SIGNATURE_STATE_SIGNED
D. NOT process_publisher_state :FILE_SIGNATURE_STATE_SIGNED
正解 :**D** (コメントを発表する)

質問: **40**
ウォッチリストはトリアージアラートページで誤検知を生成するため、ウォッチリストを更新する必要があります。
このタスクはどのように実行する必要がありますか？
A. プロセス検索ページからウォッチリストを更新できます。
B. 鉛筆アイコンを使用して、トリアージアラートページでウォッチリストを直接更新できます。
C. ウォッチリストページを開き、ウォッチリストに関連付けられている鉛筆ボタンをクリックします。
D. プロセス分析ページを開き、[アクション]メニューから[ウォッチリスト除外の追加]オプションを選択します。
正解 :**B** (コメントを発表する)

質問: **41**
プロセスは、次のイベントで詳細に説明されているように実行可能ファイルを書き込みました。



将来そのプロセスによって書き込まれる同じ名前とパスのファイルが実行時にブロックされないようにするには、どのルールタイプを使用する必要がありますか？
A. 信頼できる発行元
B. 信頼できるパス
C. Advances（書き込み無視）
D. ファイル作成制御
正解 :**D** (コメントを発表する)

質問: **42**
フィードレポートを無視した結果を正しく定義しているステートメントはどれですか？
A. フィードレポートを無視すると、レポートのすべてのインスタンスが削除されます。
B. フィードレポートを無視すると、他の脅威レポートのすべてのインジケーターが無視されます。
C. フィードレポートを無視すると、脅威インテリジェンスフィードも無視されます。
D. フィードレポートを無視すると、そのレポートの将来のインスタンスは無視されます。
正解 :(正解を表示します)

有効的な**5V0-91.20**問題集はPasstest.jp提供され、**5V0-91.20**試験に合格することに役に立ちます！Passtest.jpは今最新**5V0-91.20**試験問題集を提供します。Passtest.jp 5V0-91.20試験問題集はもう更新されました。ここで**5V0-91.20**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.passtest.jp/5V0-91.20-exam.html 「**115**問、３０%ディスカウント、特別な割引コード:**JPNshiken**」