Red Hat Insights 1-latest

RHEL システムでのマルウェアシグネチャーの評価および報告

RHEL インフラストラクチャーのシステムがマルウェアのリスクにさらされる状況を把握する

Last Updated: 2024-03-27

Red Hat Insights 1-latest RHEL システムでのマルウェアシグネチャーの評価および報告

RHEL インフラストラクチャーのシステムがマルウェアのリスクにさらされる状況を把握する

法律上の通知

概要

Insights for Red Hat Enterprise Linux マルウェア検出サービスと IBM X-Force 脅威インテリジェンスシグネチャーを使用して、インフラストラクチャー内のシステムがマルウェア攻撃の被害を受けているかを把握します。 Red Hat では、コード、ドキュメント、Web プロパティーにおける配慮に欠ける用語の置き換えに取り組んでいます。まずは、マスター (master)、スレーブ (slave)、ブラックリスト (blacklist)、ホワイトリスト (whitelist) の 4 つの用語の置き換えから始めます。この取り組みは膨大な作業を要するため、今後の複数のリリースで段階的に用語の置き換えを実施して参ります。詳細は、Red Hat CTO である Chris Wright のメッセージ をご覧ください。

目次

第1章 INSIGHTS FOR RHEL マルウェア検出サービスの概要

Red Hat Insights for Red Hat Enterprise Linux のマルウェア検出サービスは、RHEL システムをスキャンしてマルウェアの存在を監視および評価するツールです。マルウェア検出サービスには、YARA パターンマッチングソフトウェアとマルウェア検出シグネチャーが組み込まれています。シグネチャーは、Red Hat 脅威インテリジェンスチームと密接に連携している IBM X-Force 脅威インテリジェンスチームと提携して提供されます。

マルウェア検出サービス UI では、User Access を許可された管理者およびビューアーが、以下を行うことができます。

- RHEL システムのスキャン時に照合されるシグネチャーのリストを確認する。
- Insights クライアントで、マルウェア検出が有効になっているすべての RHEL システムの集約結果を確認する。
- 各システムの結果を確認する。
- システムにマルウェアの存在を示す証拠がある場合に、それを把握する。

これらの機能により、セキュリティー脅威の評価者や IT インシデント対応チームは、対応準備のための貴重な情報を得ることができます。

マルウェア検出サービスでは、マルウェアのインシデントを解決または修正する解決策を推奨していません。

マルウェアの脅威に対処する戦略は、多くの基準と、各システムおよび各組織固有の考慮事項に従います。組織のセキュリティーインシデント対応チームは、状況ごとに効果的な緩和および修復戦略を設計し、実装する上で最適な資格を有しています。

1.1. YARA マルウェアシグネチャー

YARA シグネチャー検出は、Insights for Red Hat Enterprise Linux マルウェア検出サービスの基盤です。YARA シグネチャーは、マルウェアタイプをパターンとして表現したものです。各説明は、文字列のセットと、ルールを定義するブール式で構成されます。シグネチャーの条件のうち、スキャンした RHEL システムに 1 つ以上の条件が存在する場合、YARA はそのシステムに検出を記録します。

1.2. IBM X-FORCE 脅威インテリジェンスシグネチャー

Insights for Red Hat Enterprise Linux マルウェア検出サービスには、RHEL システムで動作しているマルウェアを発見するために、IBM X-Force Threat Intelligence チームが開発した定義済みのシグネチャーが組み込まれています。X-Force 脅威インテリジェンスチームがコンパイルしたシグネチャーは、マルウェア検出サービスで **XFTI** 接頭辞 (**XFTI_FritzFrog** など) によって識別できます。

第2章 INSIGHTS FOR RHEL マルウェア検出サービスの使用

マルウェア検出サービスの使用を開始するには、次のアクションを実行する必要があります。この章では、各アクションの手順を説明します。

注記

手順によっては、システムで sudo アクセスが必要になる場合や、アクションを実行する管理者が、**マルウェア検出管理者ロール** を持つ User Access グループのメンバーでなければならない場合があります。

表2.1 マルウェア検出サービスを設定するための手順とアクセス要件

アクション	詳細	必要な特権
YARA のインストールと Insights クライアントの設定	YARA アプリケーションをインストールし、Insights クライアントがマルウェア検出サービスを使用するように設定します。	sudo アクセス
Red Hat Hybrid Cloud コンソールでの User Access の設定	Red Hat Hybrid Cloud Console > **Settings** アイコン (⚙) > Identity & Access Management > User Access > Groups で、マルウェア検出グループを作成し、適切なロールとメンバーをグループに追加します。	Red Hat アカウントの組織管理者
結果の表示	Hybrid Cloud Console でシステムスキャンの結果を表示します。	マルウェア検出ビューアーロールを持つ User Access グループのメンバーシップ

2.1. YARA のインストールおよび INSIGHTS クライアントの設定

以下の手順に従って、RHEL システムに YARA およびマルウェア検出コントローラーをインストールし、テストスキャンおよび完全なマルウェア検出スキャンを実行して、Insights for Red Hat Enterprise Linux アプリケーションにデータを報告します。

前提条件

- システムのオペレーティングシステムのバージョンは、RHEL8 または RHEL9 でなければならない。
- 管理者は、システムで sudo アクセスがある。
- システムには Insights クライアントパッケージがインストールされており、Insights for Red Hat Enterprise Linux に登録されている必要がある。

手順

1. YARA をインストールします。
   RHEL8 および RHEL9 の YARA RPM は、Red Hat カスタマーポータル から入手できます。

```
$ sudo dnf install yara
```

注記

Insights for Red Hat Enterprise Linux のマルウェア検出は、RHEL7 ではサポートされていません。

2. まだ完了していない場合は、システムを Insights for Red Hat Enterprise Linux に登録します。

重要

マルウェア検出サービスを使用する前に、Insights クライアントパッケージをシステムにインストールし、システムを Insights for Red Hat Enterprise Linux に登録する必要があります。

a. Insights クライアント RPM をインストールします。

```
$ sudo yum install insights-client
```

b. Insights for Red Hat Enterprise Linux への接続をテストします。

```
$ sudo insights-client --test-connection
```

c. システムを Red Hat Enterprise Linux の Insights に登録します。

```
$ sudo insights-client --register
```

3. Insights クライアントのマルウェア検出コレクターを実行します。

```
$ sudo insights-client --collector malware-detection
```

コレクターは、この初回実行時に次のアクションを実行します。

- **/etc/insights-client/malware-detection-config.yml** でマルウェア検出設定ファイルを作成します。
- テストスキャンを実行し、結果をアップロードします。

注記

これは、簡易テストルールを使用して、システムのごく最小限のスキャンを行うものです。テストスキャンは主に、マルウェア検出サービスのインストール、操作、アップロードが正しく機能していることを確認する際に役立ちます。一致がいくつか検出されますが、これは意図的なものであり、心配する必要はありません。初期テストスキャンの結果は、マルウェア検出サービス UI には表示されません。

4. ファイルシステムの完全スキャンを実行します。

a. **/etc/insights-client/malware-detection-config.yml** を変更し、**test_scan** を false に設定します。

```
test_scan: false
```

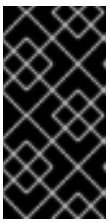
スキャン時間を最小限にとどめるため、以下のオプションを設定することを検討してください。

- **filesystem_scan_only** - システム上の特定のディレクトリーのみをスキャンする
- **filesystem_scan_exclude** - 特定のディレクトリーをスキャンから除外する
- **filesystem_scan_since** - 最近変更されたファイルのみをスキャンする

b. クライアントコレクターを再実行します。

```
$ sudo insights-client --collector malware-detection
```

5. 必要に応じて、プロセスをスキャンします。まずファイルシステムをスキャンし、次にすべてのプロセスをスキャンします。ファイルシステムとプロセスのスキャンが完了したら、Security > Malware で結果を表示します。

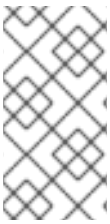


重要

デフォルトでは、スキャンプロセスは無効になっています。Linux システムでは、システムパフォーマンスが低下する可能性がある YARA およびスキャンプロセスに関する 問題 があります。この問題は、YARA の次期リリースで修正される予定です。**それまではプロセスをスキャンしないことが推奨されます。**

a. プロセススキャンを有効にするには、**/etc/insights-client/malware-detection-config.yml** で **scan_processes: true** を設定します。

```
scan_processes: true
```



注記

ここで、これらのプロセス関連オプションを設定することを検討してください (processes_scan_only - システム上の特定のプロセスのみをスキャン、processess_scan_exclude - スキャンから特定のプロセスを除外、processes_scan_since - 最近開始されたプロセスのみをスキャン)。

a. 変更を保存し、コレクターを再実行します。

```
$ sudo insights-client --collector malware-detection
```

2.2. USER ACCESS に関する考慮事項

アカウントの組織管理者は、User Access で設定を行い、Red Hat Insights for Red Hat Enterprise Linux 機能へのアクセスを制御します。アカウントのどのユーザーも、Insights for Red Hat Enterprise Linux のほとんどのデータにアクセスできます。ただし、一部のアクションを実行するには、ユーザーのアクセス権の昇格が必要です。

アクセスは、Red Hat Insights for Red Hat Enterprise Linux の User Access で付与されます。アクセスを付与または変更するには、組織管理者または User Access 管理者は、Red Hat Hybrid Cloud Console > **Settings** アイコン (⚙) > Identity & Access Management > User Access > Users で必要なロールを持つ

User Access グループにユーザーを追加する必要があります。

重要

このドキュメントでは、手順の前提条件で、その手順を実行するためにアクセス権の昇格が必要かどうかを示しています。

User Access を理解するうえで重要な事前定義済みグループおよびロールは次のとおりです。

- **デフォルトのアクセスグループ**
- **Default admin access グループ**
- **組織管理者ロール**

一部の事前定義済みグループおよびロールの概要

アクセスには、以下の事前定義済みのグループおよびロールが関連します。

- **デフォルトのアクセスグループ**: アカウント上のすべてのユーザーが、デフォルトアクセスグループのメンバーです。デフォルトのアクセスグループのメンバーには読み取り専用アクセス権があります。これにより、Insights for Red Hat Enterprise Linux のほとんどの情報を表示できます。
- **デフォルトの管理者アクセスグループ**: アカウント上の組織管理者であるすべてのユーザーは、このグループのメンバーです。ユーザーは、Red Hat が管理するデフォルト管理者アクセスグループのロールを変更できません。デフォルト管理者アクセスグループのメンバーには読み取り/書き込みアクセス権があります。これにより、Insights for Red Hat Enterprise Linux で他のアクションを表示および実行できます。
- **組織管理者ロール**: アカウント上の組織管理者であるすべてのユーザーは、User Access グループを作成および変更し、他のアカウントユーザーにアクセス権利を付与できます。組織管理者であるかどうかを確認するには、画面の右上にある Red Hat Hybrid Cloud Console ヘッダーで自分の名前をクリックして、"Org.Administrator" がユーザー名の下に表示されるかどうかを確認します。

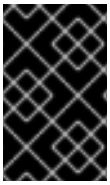
重要

アクセス権の昇格のリクエスト 必要な機能にアクセスできない場合は、以下を実行できます。

- カスタマーサービス に連絡して、アカウントの組織管理者の詳細を取得します。
  - リクエストを送信する際に、アカウント番号を提供してください。
- 組織管理者に連絡し、次の情報を提供してアクセス権の付与を依頼します。
  - アクセスする必要があるロールの名前 (Remediations 管理者など)。
  - User Access に関するすべてのドキュメント へのリンク。アクセス権を付与する方法について組織管理者に知らせるのに役立ちます。

2.2.1. マルウェア検出サービスのユーザーアクセスロール

Red Hat Hybrid Cloud Console の次の事前定義済みロールを使用すると、Insights for Red Hat Enterprise Linux のマルウェア検出機能にアクセスできます。



重要

マルウェア検出サービスユーザーには "default-group" ロールがありません。マルウェア検出サービスのデータの表示や設定の制御を実行できるようにするには、次のいずれかのロールを持つ User Access グループのメンバーである必要があります。

- **Malware detection viewer**
- **Malware detection administrator**

2.3. RED HAT HYBRID CLOUD CONSOLE でのマルウェア検出スキャンの結果の表示

Hybrid Cloud Console でシステムスキャンの結果を表示します。

前提条件

- YARA と Insights クライアントが RHEL システムにインストールされ、設定されている。
- Hybrid Cloud コンソールにログインしている必要がある。
- **マルウェア検出管理者** または **マルウェア検出ビューアー** ロールを持つ Hybrid Cloud Console User Access Group のメンバーである。

手順

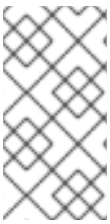
1. Security > Malware > Systems に移動します。
2. ダッシュボードを表示して、マルウェア検出が有効になっているすべての RHEL システムの概要とレポート結果を簡単に確認します。
3. 特定のシステムの結果を表示するには、**Filter by name** 検索ボックスを使用して、システムを名前で検索します。

第3章 マルウェア検出サービスのその他の概念

マルウェア検出サービスを使用する際に役立つ関連情報を以下に示します。

3.1. システムスキャン

リリース時に、マルウェア検出管理者は Insights for Red Hat Enterprise Linux マルウェア検出サービスコレクタースキャンをオンデマンドで開始する必要があります。あるいは、管理者は、Playbook として、または別の自動化方法を使用して、collector コマンドを実行できます。



注記

推奨されるスキャンの頻度はお客様のセキュリティーチームの判断となります。スキャンにはかなりの時間がかかる可能性があるため、Insights for Red Hat Enterprise Linux マルウェア検出サービスチームは、マルウェア検出スキャンを毎週実行することを推奨します。

3.1.1. マルウェア検出スキャンの開始

マルウェア検出スキャンを実行するには、次の手順を実行します。スキャンが完了すると、Insights for Red Hat Enterprise Linux マルウェア検出サービスにデータが報告されます。スキャン時間は、設定オプション、実行中のプロセス数など、多くの要因により異なります。

前提条件

Insights クライアントコマンドを実行するには、システムで sudo アクセスが必要である。

手順

1. **$ sudo insights-client --collector malware-detection** を実行します。
2. Security > Malware で結果を表示します。

3.2. マルウェアシグネチャーの無効化

マルウェアシグネチャーには、重要でないものが含まれている場合があります。その原因としては、意図的な設定やテストスキャンが挙げられるほか、マルウェア検出サービスによって組織のセキュリティー優先事項に該当しない一致が報告されるため、ノイズが多いという状況も考えられます。

たとえば、シグネチャー **XFTI_EICAR_AV_Test** および **XFTI_WICAR_Javascript_Test** は、EICAR Anti Malware Testfile および WICAR Javascript Crypto Miner テストマルウェアを検出するために使用されます。これらは意図的なテストシグネチャーであり、実際のマルウェアの脅威を表すものではありません。このようなシグネチャーを無効にして、それらとの一致が Red Hat Hybrid Cloud Console で報告されないようにすることができます。

シグネチャーを無効にすると、マルウェア検出サービスはそのシグネチャーとの既存の一致を Hybrid Cloud Console から削除し、以後のスキャンでそのシグネチャーを無視します。シグネチャーを再度有効にすると、マルウェア検出サービスは以後のマルウェア検出スキャンでそのシグネチャーを再度検索し、一致結果を表示します。

注記

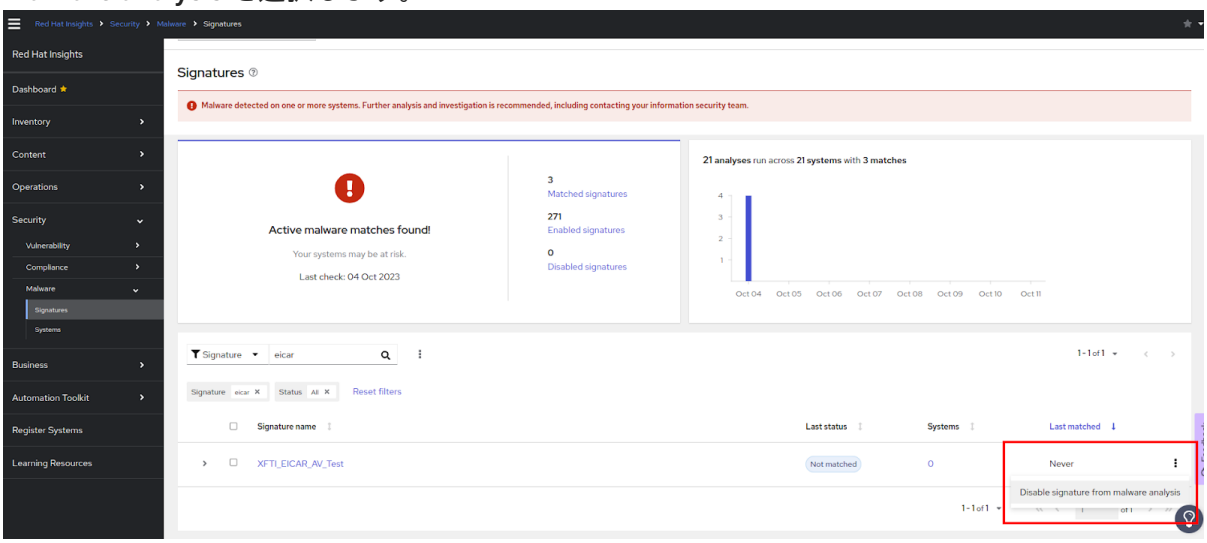
シグネチャーを無効にしても、そのシグネチャーに対する以前の一致の履歴は消去されません。

前提条件

- **Malware detection administrator** ロールを持つ Hybrid Cloud Console User Access Group のメンバーである。このロールを持つユーザーのみがシグネチャーを無効化および再有効化できます。

シグネチャーを無効にする手順

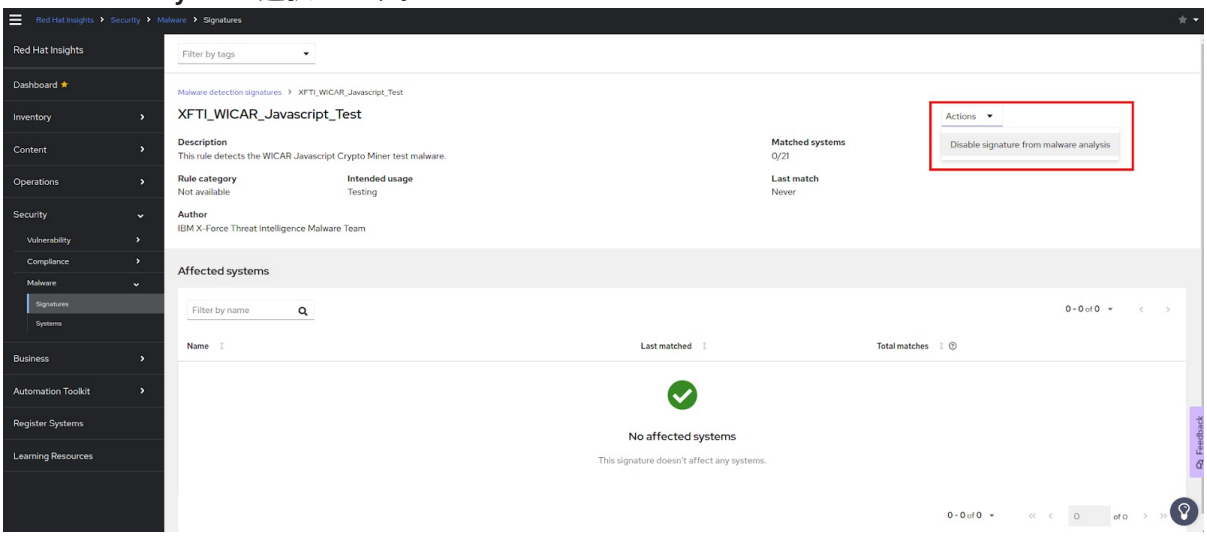
1. Security > Malware > Signatures に移動します。
2. 無効にするシグネチャーを探します。
3. シグネチャー行の最後にあるオプションアイコン (⋮) をクリックし、**Disable signature from malware analysis** を選択します。



シグネチャーを無効にする別の手順

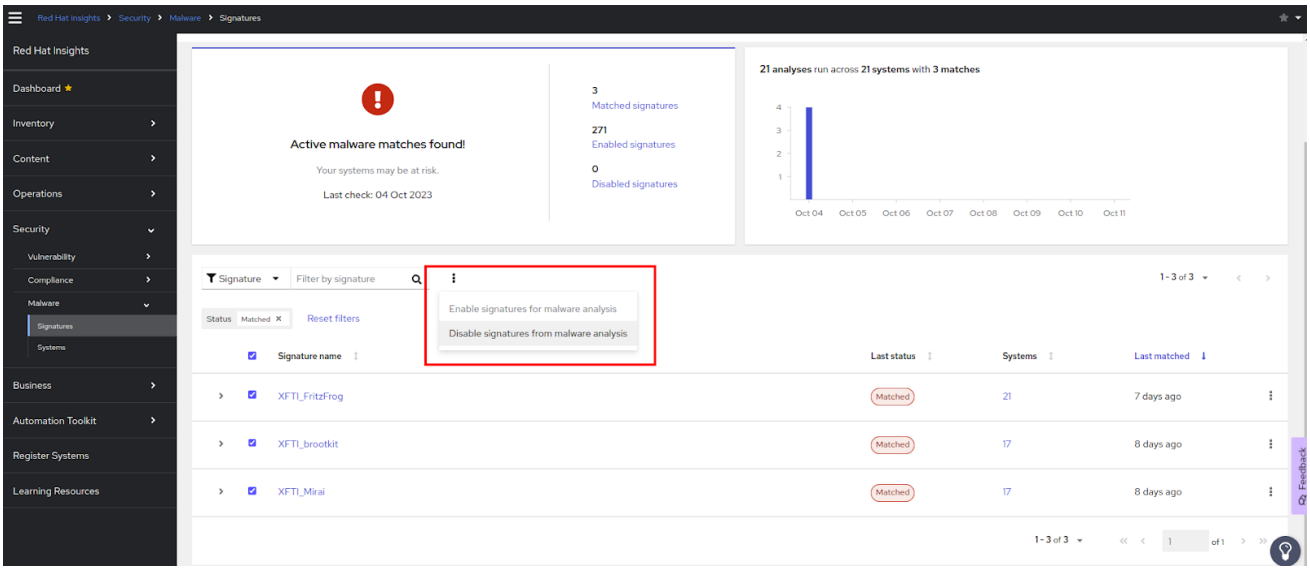
シグネチャー情報ページからシグネチャーを無効にすることもできます。

1. Security > Malware > Signatures に移動します。
2. 無効にするシグネチャーを探します。
3. シグネチャー名をクリックします。
4. シグネチャーの詳細ページで、**Actions** ドロップダウンをクリックし、**Disable signature from malware analysis** を選択します。



複数のシグネチャーを同時に無効にする

複数のシグネチャーを同時に無効にするには、各シグネチャー行の先頭にあるボックスにチェックを入れ、フィルターフィールドの横にあるオプションアイコン (⋮) をクリックして **Disable signatures from malware analysis** を選択します。



無効化されたマルウェアシグネチャーの表示

すべてのユーザーは、無効化されたマルウェアシグネチャーを表示できます。

1. Security > Malware > Signatures に移動します。ページ上部のダッシュボードで無効化されたマルウェアシグネチャーの数を確認します。
2. 無効化されたシグネチャーを表示するようにフィルターを設定します。
   a. プライマリーフィルターを **Signatures included in malware analysis**に設定します。
   b. セカンダリーフィルターを **Disabled signatures** に設定します。

マルウェアシグネチャーの再有効化

上記と同様の手順に従って、以前に無効にしたシグネチャーを再度有効にします。

3.3. マルウェア検出サービスの結果の解釈

ほとんどの場合、YARA を使用してマルウェア検出スキャンを実行すると、シグネチャーの一致なしという結果が得られます。これは、YARA が既知のマルウェアシグネチャーのセットとスキャンに含まれるファイルを比較したときに、一致する文字列またはブール式が検出されなかったことを意味します。マルウェア検出サービスは、この結果を Red Hat Insights に送信します。ユーザーは、Insights for Red Hat Enterprise Linux マルウェア検出サービスの UI で、システムスキャンの詳細と、一致が検出されなかったことを確認できます。

YARA を使用したマルウェア検出スキャンで一致が検出された場合は、その一致の結果が Red Hat Insights に送信されます。ユーザーは、マルウェア検出サービスの UI でファイルや日付などの一致の詳細を確認できます。システムスキャンとシグネチャーの一致履歴は過去 14 日間表示されるため、パターンを検出し、この情報をセキュリティーインシデント対応チームに提供できます。たとえば、あるスキャンでシグネチャーの一致が見つかったにもかかわらず、同じシステムの次のスキャンでは見つからなかった場合は、特定のプロセスが実行されているときにのみ検出可能なマルウェアが存在していることを示している場合があります。

3.4. マルウェア検出コレクターのその他の設定オプション

/etc/insights-client/malware-detection-config.yml には、いくつかの設定オプションが含まれています。

設定オプション

- **filesystem_scan_only**
  これは、基本的に許可リストオプションで、スキャンするファイル/ディレクトリーを指定します。指定した項目のみがスキャンされます。1 つのアイテム、またはアイテムのリスト (アイテムのリストを指定する yaml 構文に従う) のいずれかを指定できます。このオプションが空の場合は、基本的にすべてのファイル/ディレクトリー PID (その他のオプションによる) をスキャンすることを意味します。

- **filesystem_scan_exclude**
  これは、基本的には拒否リストオプションで、スキャンしないファイル/ディレクトリーを指定します。多くのディレクトリーがすでにリストに記載されています。つまり、ディレクトリーはデフォルトでは除外されます。これには、仮想ファイルシステムのディレクトリー (例: /proc、/sys、/cgroup)、外部にマウントされたファイルシステム (例: /mnt、/media) が存在する可能性のあるディレクトリー、およびスキャンしないことが推奨されるその他のディレクトリー (例: /dev および /var/log/insights-client) (誤検出を防ぐため) が含まれます。ファイル/ディレクトリーを追加 (または削除) するリストは自由に変更できます。

  同じ項目が filesystem_scan_only と filesystem_scan_exclude の両方で指定されている場合 (例: /home) は、filesystem_scan_exclude が '優先' されます。つまり、/home はスキャンされません。別の例として、親ディレクトリー (例:/ var) を filesysem_scan_only してから、その中の特定のディレクトリー (例: /var/lib や /var/log/Insights-client) を filesystem_scan_exclude することができます。これにより、/var/lib および /var/log/insights-client を除く /var 内のすべてのデータがスキャンされます。

- **filesystem_scan_since**
  'since' から変更されたファイルのみをスキャンします。ここで、since は日数を表す整数、または前回のファイルシステムスキャン以降を示す 'last' にすることができます。たとえば、filesystem_scan_since: 1 は、1 日前 (最後の日のみ) 以降に作成または変更したファイルだけを、filesystem_scan_since: 7 は、7 日前から (1 週間以内に) 作成/修正されたスキャンファイルだけをスキャンすることを意味します。filesystem_scan_since: last は、malware-client の最後の filesystem_scan が成功してから作成/修正されたスキャンファイルのみを意味します。

- **exclude_network_filesystem_mountpoints and network_filesystem_types**
  exclude_network_filesystem_mountpoints: true を設定すると、マルウェア検出コレクターは、マウントされたネットワークファイルシステムのマウントポイントをスキャンしません。これがデフォルト設定で、外部ファイルシステムのスキャンを防ぐため、ネットワークトラフィックが増加し、スキャンに時間がかかります。ネットワークファイルシステムと見なされるファイルシステムは、**network_filesystem_types** オプションにリスト表示されています。そのため、そのリストにあり、マウントされているファイルシステムタイプは、スキャンから除外されます。これらのマウントポイントは、基本的には、**filesystem_scan_exclude** オプションから除外されるディレクトリーのリストに追加されます。**exclude_network_filesystem_mountpoints: false** を設定しても、**filesystem_scan_exclude** オプションでマウントポイントを除外できます。

- **network_filesystem_types**
  ネットワークファイルシステムの種類を定義します。

- **scan_processes**

注記

scan_process は、多数または大規模なプロセスをスキャンするときのシステムパフォーマンスへの影響を防ぐために、デフォルトで無効になっています。ステータスが false の場合、プロセスはスキャンされず、後続の processes_scan オプションは無視されます。

+ スキャンに実行中のプロセスを含めます。

- **processes_scan_only**
  これは filesystem_scan_only に似ていますが、プロセスに適用されます。プロセスは、単一の PID (123 など) または PID の範囲 (1000..2000 など) として指定することも、プロセス名 (Chrome など) で指定することもできます。たとえば、123、1000..2000 の値、および Chrome は、PID 123、1000 から 2000 までの PID、および文字列 chrome を含むプロセス名の PID のみがスキャンされることを意味します。

- **processes_scan_exclude**
  これは filesystem_scan_exclude に似ていますが、プロセスに適用されます。プロセスは processes_scan_only と同様に、単一の PID、PID の範囲、またはプロセス名で指定できます。プロセスが processes_scan_only と processes_scan_exclude の両方に表示される場合は、processes_scan_exclude が '優先' され、プロセスは除外されます。

- **processes_scan_since**
  これは filesystem_scan_since に似ていますが、プロセスに適用されます。'since' から開始されたプロセスのみをスキャンします。since は数日前を表す整数、または最後にマルウェアクライアントのスキャンが成功したプロセス以降を意味する 'last' にすることができます。

環境変数

/etc/insights-client/malware-detection-config.yml ファイル内のすべてのオプションは、環境変数を使用して設定することもできます。環境変数を使用すると、設定ファイル内の同じオプションの値が上書きされます。環境変数は設定ファイルオプションと同じ名前ですが、大文字になります。たとえば、設定ファイルオプションの **test_scan** は、環境変数の **TEST_SCAN** です。

FILESYSTEM_SCAN_ONLY、**FILESYSTEM_SCAN_EXCLUDE**、**PROCESSES_SCAN_ONLY**、**PROCESSES_SCAN_EXCLUDE**、および **NETWORK_FILESYSTEM_TYPES** 環境変数には、コンマ区切りの値のリストを使用します。たとえば、**/etc**、**/tmp**、および **/var/lib** のディレクトリーのみをスキャンする場合は、以下の環境変数を使用します。

```
FILESYSTEM_SCAN_ONLY=/etc,/tmp,/var/lib
```

コマンドラインでこれを指定する (テストスキャンを無効にする) には、以下のコマンドを使用します。

```
$ sudo FILESYSTEM_SCAN_ONLY=/etc,/tmp,/var/lib TEST_SCAN=false insights-client --collector malware-detection
```

関連情報

Insights クライアントの詳細は、**Red Hat Insights のクライアント設定ガイド** を参照してください。

3.5. マルウェアイベントの通知と統合の有効化

マルウェアサービスが少なくとも 1 つのシステムスキャンでシグネチャーの一致を検出し、アラートを生成するたびに通知を送信するように、Red Hat Hybrid Cloud Console の通知サービスを有効にすることができます。通知サービスを使用すると、Red Hat Insights for Red Hat Enterprise Linux ダッシュボード でアラートを継続的にチェックする必要がなくなります。

たとえば、通知サービスを設定して、マルウェアサービスがシステムに対する潜在的な脅威を検出するたびに電子メールメッセージを自動的に送信したり、マルウェアサービスが毎日生成するすべてのアラートの電子メールダイジェストを送信したりできます。

メールメッセージの送信に加え、他の方法でイベントデータを送信するように通知サービスを設定できます。

- 認証済みクライアントを使用して Red Hat Insights API にイベントデータをクエリーする。
- Webhook を使用して受信要求を受け入れるサードパーティーのアプリケーションにイベントを送信する。
- 通知を Splunk などのアプリケーションと統合して、マルウェアイベントをアプリケーションダッシュボードにルーティングする。

マルウェアサービスの通知には、次の情報が含まれます。

- 影響を受けるシステムの名前
- システムスキャン中に検出された署名の一致数
- Red Hat Hybrid Cloud Console で詳細を表示するためのリンク

通知サービスを有効にするには、以下の 3 つの主要なステップが必要です。

- まず、組織管理者は Notifications 管理者ロールを持つ User Access グループを作成し、そのグループにアカウントメンバーを追加します。
- 次に、通知管理者が通知サービス内のイベントの動作グループを設定します。動作グループは、通知ごとに配信方法を指定します。たとえば、動作グループは、電子メール通知をすべてのユーザーに送信するか、組織の管理者にのみ送信するかを指定できます。
- 最後に、イベントから電子メール通知を受信するユーザーは、各イベントの個別電子メールを受け取るようにユーザー設定する必要があります。

関連情報

- マルウェアアラートの通知をセットアップする方法の詳細は、**Red Hat Hybrid Cloud Console での通知の設定** を参照してください。

RED HAT ドキュメントへのフィードバック (英語のみ)

Red Hat ドキュメントに関するフィードバックをお寄せください。いただいたご要望に迅速に対応できるよう、できるだけ詳細にご記入ください。

前提条件

- Red Hat カスタマーポータルにログインしている。

手順

フィードバックを送信するには、以下の手順を実施します。

1. Create Issue にアクセスします。
2. **Summary** テキストボックスに、問題または機能拡張に関する説明を入力します。
3. **Description** テキストボックスに、問題または機能拡張のご要望に関する詳細を入力します。
4. **Reporter** テキストボックスに、お客様のお名前を入力します。
5. **Create** ボタンをクリックします。

これによりドキュメントに関するチケットが作成され、適切なドキュメントチームに転送されます。フィードバックの提供にご協力いただきありがとうございました。