Red Hat Insights 2022

Insights for RHEL Malware Service を使用した RHEL システムでのマルウェア署名の評価および報告

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: 2022-06-19

Red Hat Insights 2022 Insights for RHEL Malware Service を使用した RHEL システムでのマルウェア署名の評価および報告

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

Enter your first name here. Enter your surname here.
Enter your organisation's name here. Enter your organisational division here.
Enter your email address here.

法律上の通知

概要

IBM X-Force 脅威インテリジェンス署名とともに Insights for RHEL マルウェア検出サービスを使用して、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者であるかを把握します。

目次

多様性を受け入れるオープンソースの強化

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。

RED HAT ドキュメントへのフィードバック

弊社のドキュメントに関するご意見やご感想をお寄せください。フィードバックを提供するには、ドキュメントのテキストを強調表示し、コメントを追加します。

前提条件

- Red Hat カスタマーポータルにログインしている。
- Red Hat カスタマーポータルでは、このドキュメントは **Multi-page HTML** 表示形式です。

手順

フィードバックを提供するには、以下の手順を実施します。

1. ドキュメントの右上隅にある **フィードバック** ボタンをクリックして、既存のフィードバックを確認します。

注記

フィードバック機能は、**マルチページ HTML** 形式でのみ有効です。

2. フィードバックを提供するドキュメントのセクションを強調表示します。
3. ハイライトされたテキスト近くに表示される **Add Feedback** ポップアップをクリックします。ページの右側のフィードバックセクションにテキストボックスが表示されます。
4. テキストボックスにフィードバックを入力し、**Submit** をクリックします。ドキュメントに関する問題が作成されます。
5. 問題を表示するには、フィードバックビューで問題リンクをクリックします。

第1章 RHEL マルウェア検出サービスのインサイトの概要

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は、YARA パターンマッチングソフトウェアおよびマルウェア検出署名を組み込みます。署名は、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、ユーザーアクセス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 システムがスキャンされる署名の一覧を参照してください。
- 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表示します。
- 各システムの結果を参照してください。
- システムにマルウェアの存在を示す証拠がある場合は、それを知ることができます。

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、実装するのに最善の資格を有しています。

1.1. YARA マルウェア署名

YARA 署名検出は、RHEL マルウェア検出サービスの Insights の基盤です。YARA 署名は、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。署名の条件のうち、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署名

Insights for RHEL マルウェア検出サービスには、IBM X-Force 脅威インテリジェンスチームが開発した定義済み署名が含まれており、RHEL システムで実行しているマルウェアを公開します。X-Force 脅威インテリジェンスチームがコンパイルした署名は、マルウェア検出サービスで **XFTI**- 接頭辞 (**XFTI_FritzFrog** など) で識別できます。

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、以下のアクションを実行する必要があります。本章では、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 アクセスを必要とするものと、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ユーザーアクセスグループのメンバーであることが必要です。

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 malware-detection 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 コンソールでのユーザーアクセスの設定	Red Hat Hybrid Cloud Console > 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ユーザーアクセス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 と malware-detection コントローラーをインストールし、test スキャンと完全 malware-detection スキャンを実行して、Insights for RHEL 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、RHEL7 または RHEL8 にする必要があります。
- 管理者は、システムで sudo アクセスが必要です。
- 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、RHEL の Insights に登録されている必要があります。

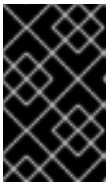
手順

1. YARA 4.1 以降をインストールします。
   RHEL7 および RHEL8 の Yara RPM は、EPEL で利用できます。たとえば、RHEL8 に YARA をインストールするには、次のコマンドを入力します。

```
$ sudo yum install https://dl.fedoraproject.org/pub/epel/epel-release-latest-8.noarch.rpm
$ sudo yum install yara
```

または、このリンク の手順に従って、ソースコードから yara をインストールできます。マルウェア検出コントローラーには、YARA バージョン 4.1.0 以降が必要です。

2. 完了していない場合は、Insights for RHEL にシステムを登録します。



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がシステムにインストールされ、Insights for RHEL に登録されているシステムにインストールされている必要があります。

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 RHEL への接続をテストします。

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

c. Insights for RHEL にシステムを登録します。

```
$ 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用いて、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、インストール、操作、およびアップロードが、マルウェア検出サービスに対して正しく機能していることを確認するために行います。一致するものがいくつか見つかりますが、これは意図的なもので、心配するものではありません。初期テストスキャンの結果は、malware-detection サービス UI に表示されません。

4. ファイルシステムのフル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
```

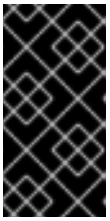
スキャン時間を最小限にとどめるため、以下のオプションを設定することを検討してください。

- **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します
- **filesystem_scan_exclude** - 特定のディレクトリーをスキャンから除外します
- **filesystem_scan_since** - 最近変更されたファイルのみをスキャンします

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。ファイルシステムおよびプロセスのスキャンが完了したら、Red Hat Enterprise Linux > Malware detection で結果を表示します。

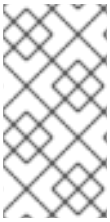


重要

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 **が、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

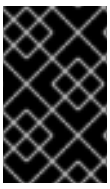
そこにいる間にこれらのプロセス関連オプションを設定することを検討してください (processes_scan_only - システム上の特定のプロセスのみをスキャン、processess_scan_exclude - スキャンから特定のプロセスを除外、processes_scan_since - 最近開始されたプロセスのみをスキャン)。

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. ユーザーアクセスでマルウェア検出グループ、ロール、およびメンバーの設定

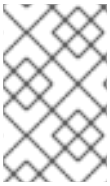
組織管理者は、Red Hat Hybrid Cloud Console > User Access > Groups でマルウェア検出グループを作成し、必要なマルウェア検出ロールとメンバー (アカウントの登録ユーザー) を追加する必要があります。



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または制御設定を表示できるようにするには、以下のいずれかのロールを持つ 1 つ以上の User Access グループのメンバーである必要があります。

- **マルウェア検出ビューアー**
- **マルウェア検出管理者**



注記

現在、これらのロールにより付与される特権に違いはありませんが、今後数か月で新しい機能が登場すると、特定のアクションは admin ユーザーのみが利用できるようになります。

Resources

Red Hat Hybrid Cloud Console でのユーザーアクセスの設定に関する完全なドキュメントは、**ロールベースのアクセス制御(RBAC)の『User Access Configuration Guide』** を参照してください。

2.2.1. ユーザーアクセスでのマルウェア検出グループの作成および設定

以下の手順では、アカウントの組織管理者がユーザーアクセスグループを作成し、そのグループに**マルウェア検出管理者の ロール** を追加してから、マルウェア検出サービスの管理者特権を持つ **メンバー** を追加する方法を示しています。

目的、ロール、またはメンバーに関係なく、以下の手順は、ユーザーアクセスでグループを作成する場合と同じです。組織管理者は、管理者用に 1 つのグループを作成し、ビューアー用に別のグループを作成する必要があります。

重要

現在、マルウェア検出管理者が付与する特権とビューアーロールには違いはありません。ただし、今後のリリースでは変更になります。

前提条件

組織管理者として Red Hat Hybrid Cloud Console アカウントにログインしている必要があります。

手順

1. アプリケーションウィンドウの右上にある **ギアアイコン** をクリックし、**Settings** を選択します。

2. Red Hat Hybrid Cloud Console > User Access > Groups に移動します。
3. **Create Group** をクリックします。
4. **マルウェア管理者** などの **グループ名** と説明を入力し、**次** をクリックします。
5. このグループに追加するロール (**マルウェア検出管理者** など) を選択します。そのロールのチェックボックスをクリックしてから、**Next** をクリックします。
6. グループにメンバーを追加します。個々のユーザーを検索するか、ユーザー名、メール、またはステータスでフィルタリングします。対象となる各メンバーの名前の横にあるチェックボックスにチェックを入れてから、**Next** をクリックします。

7. 詳細を確認して、すべてが正しいことを確認します。戻って変更する必要がある場合は **Back** をクリックします。

8. **Submit** をクリックしてグループの作成を終了します。

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 および Insights クライアントは、本書の第 2 章で説明されている手順に従って RHEL システムにインストールおよび設定します。
- Hybrid Cloud コンソールにログインしている必要があります。
- **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** を使用する Hybrid Cloud Console User Access Group のメンバーになっています。

手順

1. Red Hat Enterprise Linux > Malware detection > Systems に移動します。
2. ダッシュボードを表示して、マルウェア検出を有効にし、結果を報告している RHEL システムの概要を簡単に確認できます。
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

3.1. システムスキャン

リリースで、マルウェア検出管理者は、RHEL 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。または、管理者は、Playbook、または別の自動化方法を使用して、コレクター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 RHEL 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、以下の手順を実行します。スキャンが完了すると、データは Insights for RHEL マルウェア検出サービスに報告されます。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 アクセスが必要です。

手順

1. **$ sudo insights-client --collector malware-detection** を実行します。
2. Red Hat Enterprise Linux > Malware detection に結果を表示します。

3.2. 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 でマルウェア検出スキャンを実行すると、署名が一致するものがありません。つまり、既知のマルウェア署名セットをスキャンに含まれるファイルと比較すると、YARA が一致する文字列やブール式を検出できませんでした。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。また、システムスキャンの詳細と、Insights for RHEL マルウェア検出サービス UI で一致の欠如を確認できます。

YARA によるマルウェア検出スキャンで一致した場合は、その結果が Red Hat Insights に送信され、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することができます。システムスキャンと署名の一致履歴は過去 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、あるスキャンで署名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。

3.3. マルウェア検出コレクターの追加設定オプション

/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、基本的にホワイト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、またはアイテムの一覧 (アイテムの一覧を指定する 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、基本的にはブラック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一覧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) がある可能性が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) する一覧は自由に変更できます。

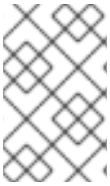
  同じ項目が filesystem_scan_only と filesystem_scan_exclude の両方で指定されている場合 (例: /home)、filesystem_scan_exclude が「優先」されます。つまり、/home はスキャンされません。別の例として、親ディレクトリー (例:/ var) を filesysem_scan_only してから、その中の特定のディレクトリー (例: /var/lib や /var/log/Insights-client) を filesystem_scan_exclude することができます。これにより、/var/lib および /var/log/insights-client 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' が変更されたファイルのみをスキャンします。ここで、since には日数を表す整数、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 日前以降に作成または変更したファイルのみを意味します（最後の日）。filesystem_scan_since: 7 は、7 日前以降に作成/変更したファイルのみを意味します（最後の週）。および filesystem_scan_since: last は、malware-client の最後の成功した filesystem_scan 以降に作成または変更したファイルのみをスキャンします。

- **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** オプションに一覧表示されています。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一覧に追加されます。**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、および Chrome の値は、文字列 'chrome' を含むプロセス名に対して PID 123、1000 から 2000 までの PID、および PID 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、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」で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「last」は、マルウェアクライアントの最後の成功したプロセススキャン以降を意味します。

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
```

Resources

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