脅威インテリジェンス

脅威インテリジェンスを管理するには、左側のナビゲーションバーで **[管理（Manage）]** > **[脅威インテリジェンス（Threat Intelligence）]** をクリックします。

[脅威インテリジェンス（Threat Intelligence）] 機能セットは、Secure Workload パイプラインに最新のデータセットを提供します。このパイプラインは、外部の既知のマルウェア コマンド アンド コントロール アドレス、プロセスのセキュリティフローと地理的位置に関してデータセンターのワークロードを検査することにより、脅威を識別および検疫します。

脅威インテリジェンス ダッシュボードには、脅威インテリジェンス データセットの最新の更新ステータスが表示されます。これらのデータセットは自動的に更新されます。

警告 脅威インテリジェンス機能を自動更新するには、Cisco Secure Workload サーバーへの接続が必要です。エンタープライズアウトバウンドHTTPリクエストには、次が必要になる場合があります。

1. エンタープライズファイアウォールのアウトバウンドルールから次のドメインを許可します。
   - uas.tetrationcloud.com
2. アウトバウンド HTTP 接続を設定します。

アウトバウンド接続のない環境では、これらのデータセットを直接アップロードできます。「手動アップロード」の項を参照してください。

データセット

データセット	説明
NVD CVE	セキュリティ関連のソフトウェアの欠陥、CVSSベーススコア、脆弱な製品設定、および弱点の分類
MaxMind Geo	送信元 IP の場所および他の特性の特定

データセット	説明
NIST RDS	既知の追跡可能なソフトウェアアプリケーションのデジタル署名の NIST 参照データセット
Team Cymru	3,000 を超えるボットネット コマンド アンド コントロール IP に関する知見
ハッシュ判定	プロセスハッシュに関する Secure Workload の判定（[自動更新（Automatic Updates）] セクションでのみ利用可能）。

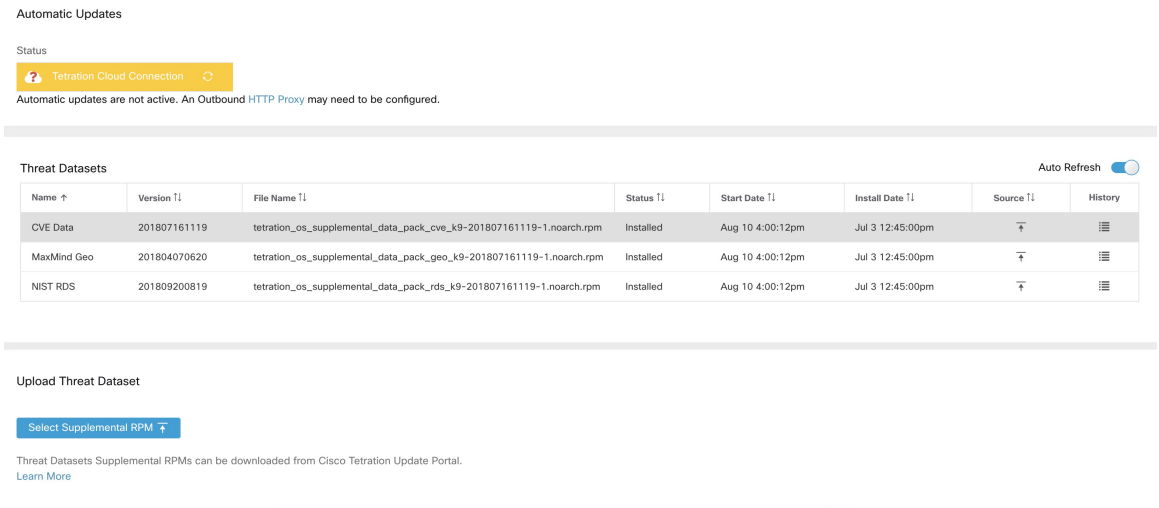
（注） MaxMind Geo データセットが以前のリリースで手動でアップロードされた場合は、対応する RPM を再アップロードして、フロー可視性のページで場所と関連情報を表示してください。

- 自動更新 （2 ページ）
- 手動アップロード （3 ページ）

自動更新

脅威データセットの更新はアプライアンスからトリガーされ、毎日午前 3 時から 4 時（UTC）に、uas.tetrationcloud.com のインターネット上でホストされているグローバルデータセットで入手可能なグローバルデータセットと同期されます。グローバルデータセットは、毎週金曜日または月曜日に更新されます。脅威インテリジェンス ダッシュボードには、データセットとデータセットの最終更新日が一覧表示されます。

図 *1:* ダッシュボード



手動アップロード

注目 **手動アップロードのスケジューリング** データセット rpm ファイルは、毎週 Cisco Secure Workload Update Portal に公開されます。最新のリリースを定期的にインストールし、管理者がインストールするようにスケジュールを設定することを推奨します。

更新されたデータセットのダウンロード

データセットは Secure Workload 更新ポータルからダウンロードできます。

Cisco Secure Workload へのアップロード

このセクションでは、データセット rpm ファイルをアップロードする方法について説明します。

始める前に

[サイト管理者（Site Admin）] または [カスタマーサポート（Customer Support）] としてシステムにログインする必要があります。

手順

ステップ 1 左側のナビゲーションバーで、**[管理（Manage）] > [脅威インテリジェンス（Threat Intelligence）]** をクリックします。

ステップ 2 [脅威データセットのアップロード（Upload Threat Dataset）] セクションまでスクロールします。

ステップ 3 [補足RPMを選択（Select Supplemental RPM）] をクリックします。

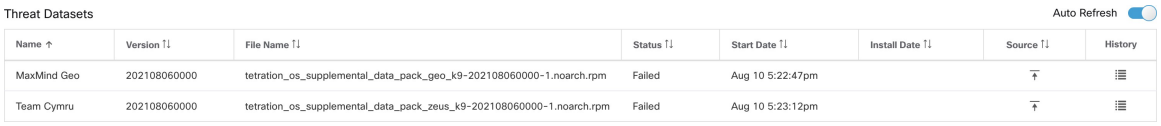
ステップ 4 Secure Workload 更新ポータルからダウンロードした rpm ファイルを選択します。

ステップ 5 準備ができると、確認ダイアログが表示されます。[アップロード（Upload）] をクリックします。

ステップ 6 rpm がアップロードされます。進行状況バーが表示されます。アップロードが完了すると、ダイアログが閉じます。

ステップ 7 その後、rpm が処理され、バックグラウンドでインストールされます。インストールが完了すると、テーブルが更新されます。

図 *2:* テーブルの更新


Threat Datasets
Auto Refresh
Name
Version
File Name
Status
Start Date
Install Date
Source
History
MaxMind Geo
202108060000
tetration_os_supplemental_data_pack_geo_k9-202108060000-1.noarch.rpm
Failed
Aug 10 5:22:47pm
Team Cymru
202108060000
tetration_os_supplemental_data_pack_zeus_k9-202108060000-1.noarch.rpm
Failed
Aug 10 5:23:12pm

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。