Analyse des rapports d'informations sur les menaces

Le tableau de bord **Threat Intelligence** (Informations sur les menaces) fournit l'ensemble des données les plus récentes au processus de Cisco Secure Workload qui identifie et met en quarantaine les menaces en inspectant les charges de travail du centre de données par rapport aux adresses de commande et de contrôle des logiciels malveillants connues de l'extérieur, aux failles de sécurité dans les processus et à l'emplacement géographique.

Pour gérer les renseignements sur les menaces, dans le volet de navigation, choisissez **Manage (Gestion)** > **Service Settings (Paramètres de service)** > **Threat Intelligence (Informations sur les menaces)**.

Le tableau de bord des informations sur les menaces affiche l'état mis à jour des ensembles de données d'informations sur les menaces. Ces ensembles de données sont mis à jour automatiquement.

Avertissement La fonctionnalité de renseignements sur les menaces nécessite une connexion aux serveurs Cisco Cisco Secure Workload pour se mettre à jour automatiquement. Votre requête HTTP sortante Enterprise peut nécessiter :

- D'autoriser le domaine suivant dans les règles de sortie du pare-feu d'entreprise : `uas.tetrationcloud.com`
- De configurer votre connexion HTTP sortante.

Dans les environnements sans connexion sortante, importez directement les ensembles de données. Pour en savoir plus, consultez la section **Téléversements manuels**.

Tableau 1 : Ensembles de données

Jeu de données	Description
CVE de NVD	Défaillances logicielles liées à la sécurité, note de base CVSS, configuration de produits vulnérables et catégorisation des vulnérabilités
Zone géographique MaxMind	L'identification de l'emplacement et d'autres caractéristiques des adresses IP source
RDS NIST	Ensemble de données de référence NIST de signatures numériques d'applications logicielles connues et traçables

Jeu de données	Description
Équipe Cymru	Informations sur plus de 3 000 adresses IP de commandes et de contrôles pour réseaux de zombies
Verdict de condensé	Verdict de Cisco Secure Workload sur les condensés de processus (uniquement disponible avec la sectionMises à jour automatiques).

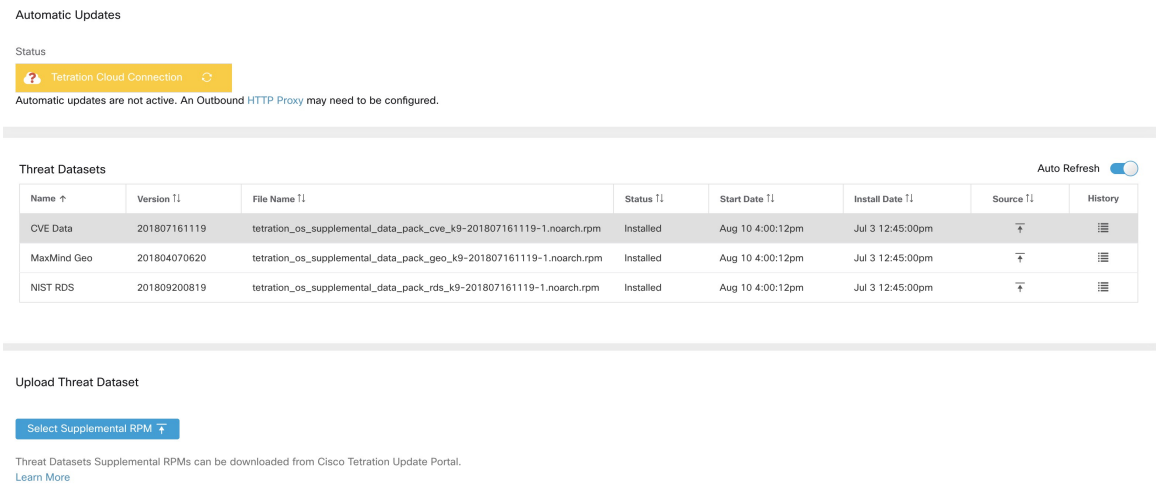
Remarque Si l'ensemble de données MaxMind Geo est téléversé manuellement dans une version antérieure, vous devez téléverser à nouveau le RPM correspondant pour afficher l'emplacement et les informations connexes sur la page Flow Visibility (Visibilité des flux).

- Mises à jour automatiques, on page 2
- Chargements manuels, on page 3

Mises à jour automatiques

Les mises à jour des ensembles de données sur les menaces sont déclenchées par l'appareil pour se synchroniser avec l'ensemble de données mondial hébergé sur Internet à l'adresse uas.tetrationcloud.com, tous les jours entre 3 h et 4 h UTC. L'ensemble mondial de données est actualisé chaque semaine, le vendredi ou le lundi. Le tableau de bord des informations sur les menaces répertorie les ensembles de données et la date à laquelle l'ensemble de données a été mis à jour pour la dernière fois.

Figure 1: Tableau de bord



Chargements manuels

Attention **Planification des téléchargements manuels** : les fichiers RPM des ensembles de données sont publiés sur une mise à jour hebdomadaire du portail Cisco Secure Workload. Il est recommandé d'installer les dernières versions régulièrement en configurant un calendrier l'administrateur.

Téléchargement des ensembles de données mis à jour

Les ensembles de données peuvent être téléchargés à partir du portail des mises à jour Cisco Secure Workload.

Chargement manuel d'ensembles de données

Pour charger les fichiers RPM d'ensembles de données :

Before you begin

Connectez-vous en tant **qu'administrateur de site** ou **service d'assistance à la clientèle**.

Procedure

Étape 1 Dans le volet de navigation de gauche, cliquez sur **Manage(Gestion)** > **Service Settings (Paramètres de service)** > **Threat Intelligence** (Informations sur les menaces).

Étape 2 Dans la section **Upload Threat Dataset** (Charger l'ensemble de données sur les menaces), cliquez sur **Select Supplemental RPM** (Sélectionner un RPM supplémentaire).

Étape 3 Chargez le fichier RPM téléchargé à partir du portail de mise à jour Cisco Secure Workload.

Étape 4 Cliquez sur **Upload** (Téléverser).

Le processus de téléversement du RPM est lancé et l'état est affiché dans une barre de progression. Après le téléchargement, le fichier RPM est traité et installé en arrière-plan. La table est mise à jour une fois l'installation terminée.

Figure 2: Ensembles de données sur les menaces

À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d’incohérence, la version anglaise du présent contenu prévaudra.