Tableau de bord FTD

À propos du Tableau de bord FTD

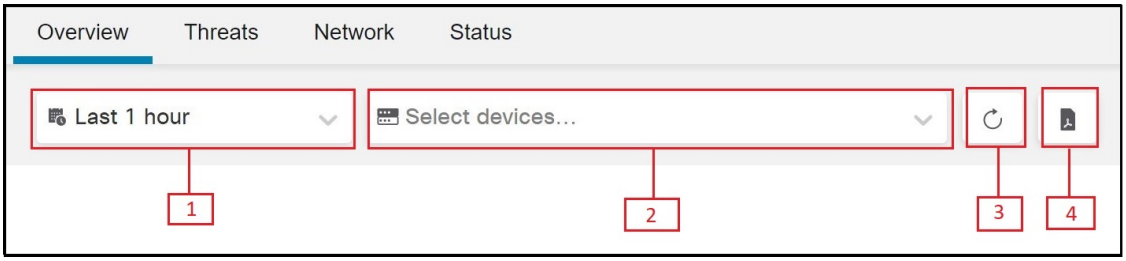
Le tableau de bord FTD vous fournit un aperçu de l'état, y compris les données d'événements collectées et générées par tous les périphériques défense contre les menaces gérés par CDO.

Vous pouvez utiliser ce tableau de bord pour afficher les informations collectives liées à l'état des périphériques et à l'intégrité générale des périphériques de votre déploiement. Les informations fournies par le tableau de bord FTD dépendent de la licence que vous utilisez, de la configuration et du déploiement des périphériques de votre système. Bien que le tableau de bord FTD affiche les données pour tous les périphériques gérés par défense contre les menaces CDO , vous pouvez choisir de filtrer les données par appareil. Vous pouvez également choisir la plage temporelle à afficher pour une plage temporelle spécifique.

Ce tableau de bord utilise des onglets pour afficher des gadgets prédéfinis : de petits composants autonomes qui donnent un aperçu des différents aspects du système. Par exemple, le gadget Activité réseau vous affiche des graphiques d'événements qui affichent des informations sur tous les événements de connexion, les programmes malveillants et les intrusions. Les gadgets du tableau de bord sont prédéfinis et ne peuvent pas être personnalisés. Ce tableau de bord est visible par tous les utilisateurs de CDO qui ont accès à un détenteur CDO.

- Le tableau de bord n'affiche aucune statistique pour les événements historiques.
- Étant donné que le lot du service d'agrégation traite les événements pour les agréger toutes les cinq minutes, vous pouvez vous attendre à une latence de cinq minutes entre le moment où les événements sont agrégés et celui où les statistiques sont affichées.

Illustration 1 : Tableau de bord FTD



Nombre	Description
1	Vous permet de modifier la plage temporelle afin de refléter une période aussi courte que la dernière heure ou aussi longue que l'année dernière. Lorsque vous modifiez la plage temporelle, les gadgets mettent automatiquement à jour les données des événements pour refléter la nouvelle plage temporelle.
2	Vous permet de filtrer les données d'événements en fonction des périphériques sélectionnés. Si aucun périphérique n'est sélectionné, les gadgets affichent toutes les données d'événements disponibles.
3	Réinitialise la requête de données des événements
4	Affiche les données des événements au format de sortie PDF. Vous pouvez choisir de télécharger ou d'enregistrer une copie de ce fichier PDF sur votre ordinateur local.

Afficher le Tableau de bord FTD

Dans le menu CDO, choisissez **Analyses** > **Tableau de bord FTD** pour afficher le **tableau de bord FTD**.

Par défaut, la page d'accueil de votre client affiche l'onglet **Vue d'ensemble**.

Le tableau de bord comprend des gadgets qui sont répertoriés sous chaque onglet : onglet Menace, Réseau, Application et utilisateurs, et Onglet État.

Le tableau suivant répertorie les gadgets disponibles sous chaque onglet :

Nom de l'onglet	Gadgets disponibles
Aperçu	Tous les gadgets disponibles
La chasse aux menaces	• Règles d'intrusion principales • Principaux attaquants des intrusions • Principales cibles des intrusions • Signatures de programmes malveillants les plus fréquentes • Principaux expéditeurs de programmes malveillants • Principaux récepteurs de programmes malveillants • Événements de programmes malveillants par disposition

Nom de l'onglet	Gadgets disponibles
Réseau	• Activité du réseau • Activité de l'événement • Action liée au contrôle d'accès • Politiques de contrôle d'accès principales • Règles de contrôle d'accès principales • Principaux périphériques • Principaux utilisateurs
État	• Périphériques non intègres • Principaux appareils chargés

Gadgets du tableau de bord FTD

Le tableau de bord de FTD affiche des gadgets prédéfinis qui peuvent vous fournir un aperçu de l'état actuel du système. Ces affichages comprennent notamment :

- Les données sur les événements sont collectées et générées par les périphériques gérés défense contre les menaces FMC.
- Des informations sur l'état et l'intégrité générale des périphériques de votre déploiement.

Gadget des principales règles de prévention des intrusions

Le gadget **Principales règles d'intrusions** affiche le nombre d'incidents d'intrusion qui se sont produits au cours de la plage temporelle spécifiée et sont classés par priorité. Ces nombres comprennent des statistiques sur les événements d'intrusion avec des paquets abandonnés et différentes incidences. La liste générée peut être parcourue.

Gadget des principaux attaquants générant des intrusions

Le gadget **Principaux attaquants gérant des intrusions** affiche le nombre d'incidents d'intrusion pour les adresses IP des hôtes les plus attaquants (à l'origine de ces événements) sur votre réseau surveillé.

Gadget des principales cibles d'intrusion

Le gadget **Principales cibles d'intrusions** affiche le nombre d'incidents d'intrusion pour les principales adresses IP des hôtes cibles (ciblées dans les connexions à l'origine de ces événements) sur votre réseau surveillé.

Gadget des signatures de principaux programmes malveillants

Le gadget **Signatures** les plus fréquentes affiche le nombre des signatures de programmes malveillants les plus fréquentes détectées dans le trafic réseau pour les principales adresses IP des hôtes d'envoi de fichiers.

Gadget des principaux expéditeurs de logiciels malveillants

Le gadget **Principaux expéditeurs de programmes malveillants** affiche le nombre des principales menaces de programmes malveillants détectées dans le trafic réseau pour les principales adresses IP des hôtes d'envoi de fichiers.

Gadget des principaux récepteurs de logiciels malveillants

Le gadget **Principaux récepteurs de programmes malveillants** affiche le nombre des principales menaces de programmes malveillants détectées dans le trafic réseau pour toutes les adresses IP des hôtes principaux récepteurs de fichiers.

Gadget des événements de programmes malveillants par répartition

Le gadget **Événements de programmes malveillants par disposition** affiche le nombre de tous les événements de disposition des programmes malveillants qui sont générés lorsque le périphérique géré détecte un fichier contenant un programme malveillant.

Gadget d'activité du réseau

Le gadget **Network Activity** (Activité du réseau) affiche tous les débits de données d'entrée et de sortie en fonction des informations provenant des événements de connexion.

Gadget d'activité de l'événement

Le gadget **Activité de l'événement** affiche le nombre d'événements qui se sont produits au cours de la dernière heure et le nombre total de chaque type d'événement disponible dans la base de données.

Le gadget Actions de contrôle d'accès

Le gadget **Actions de contrôle d'accès** affiche le nombre d'événements enregistrés en fonction des actions de contrôle d'accès autorisées ou bloquées pour chaque événement. Si vous passez le curseur sur le graphique à secteurs, vous pouvez afficher le pourcentage d'actions autorisées et bloquées.

Gadget des principales politiques de contrôle d'accès

Le gadget **Politiques de contrôle d'accès principales** affiche le nombre d'événements générant des politiques de contrôle d'accès principales.

Gadget des principales règles de contrôle d'accès

Le gadget **Principales règles de contrôle d'accès** affiche les cinq principales règles de contrôle d'accès utilisées pour chaque événement. Ces nombres peuvent être triés par octets ou par événements.

Gadget des principaux périphériques

Le gadget **Principaux périphériques** affiche le nombre d'événements par appareil. Ces décomptes peuvent être triés par octets ou par événements.

Gadget des principaux utilisateurs

Le gadget **Principaux utilisateurs** affiche une liste des utilisateurs de votre réseau surveillé qui sont associés au nombre d'incidents d'intrusion le plus élevé. Il tire des données principalement des tableaux des statistiques sur les utilisateurs et des incidents d'intrusion pour la détection des intrusions. Il affiche des données d'utilisateur officielles.

Gadget des périphériques non intègres

Le gadget **Périphériques non intègres** affiche l'état d'intégrité actuel compilé des périphériques défense contre les menaces gérés par CDO.

Gadget des périphériques les plus téléversés

Le gadget **Périphériques les plus téléversés** affiche une liste de périphériques Cisco Secure Firewall Threat Defense ainsi que des informations sur l'utilisation du processeur.

Modifier les paramètres horaires du tableau de bord FTD

Vous pouvez modifier la plage temporelle pour refléter une période aussi courte que la dernière heure (par défaut) ou aussi longue que la dernière année. Lorsque vous modifiez la plage temporelle, les gadgets qui peuvent être limités dans le temps sont automatiquement mis à jour pour refléter la nouvelle plage temporelle.

Le nombre maximal de points de données dans un graphique est de 300, et le paramètre de temps détermine la quantité de temps est résumé dans chaque point de données. Voici le nombre de points de données et la période de temps couverte dans le tableau de bord FTD pour chaque plage temporelle :

- 1 heure = 12 points de données de 5 minutes chacun
- 6 heures = 72 points de données de 5 minutes chacun
- 1 jour = 288 points de données de 5 minutes chacun
- 1 semaine = 300 points de données de 33,6 minutes chacun
- 2 semaines = 300 points de données de 67,2 minutes chacun
- 30 jours = 300 points de données, 144 minutes chacun
- 90 jours = 300 points de données de 432 minutes chacun

- 180 jours = 300 points de données, 864 minutes chacun
- 1 an = 300 points de données de 1 752 minutes chacun

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.