FAQ sur la fin de service de Cisco Secure Endpoint Global Threat Alert (GTA)

Table des matières

Introduction

Ce document vise à fournir des réponses aux questions fréquemment posées concernant le retrait de la fonctionnalité Global Threat Alerts de Cisco Secure Endpoint.

Annonce de fin de service

Cisco Secure Endpoint retire la fonctionnalité Global Threat Analytics (GTA). Les clients ne pourront plus s'inscrire à GTA à partir du 1er février. Les clients ne recevront plus les données d'événements générées par GTA à partir du 31 juillet.

Forum aux questions

Délai de fin de service

- 6 février 2024 - Les clients ne pourront plus s'inscrire aux fonctionnalités GTA.
- 31 juillet 2024 - Le service cloud GTA cessera d'ingérer des données. Le back-end et le tableau de bord GTA seront désactivés, aucun nouvel événement client ne sera généré.

Quels sont les produits concernés ?

- Cisco Secure Endpoint AKA AMP for Endpoints
- Cisco Global Threat Analytics
- Cisco Secure Network Analytics, alias Stealth Watch Enterprise

Quels produits remplaceront cette fonctionnalité ?

- XDR sera l'alignement le plus proche en termes de fonctionnalités, mais ne remplacera pas de 1 à 1 la fonctionnalité fournie par Global Threat Analytics.

Quelles mesures les clients doivent-ils prendre ?

- Terminaux sécurisés Cisco
  - Aucune action du client n'est requise.
  - À quoi s'attendre : à partir du 31 juillet, Secure Endpoint cessera de présenter les alertes générées par la fonctionnalité GTA.
- Analyses des menaces mondiales
  - Aucune action du client n'est requise.
  - À quoi s'attendre : à partir du 31 juillet, les données ne seront plus ingérées par le service GTA, le traitement des données s'arrêtera et aucun événement supplémentaire ne sera généré. Il est conseillé aux clients de désactiver l'envoi de données à GTA sur leurs appareils pris en charge.

Serai-je affecté par ce changement ?

- Si vous possédez Secure Endpoint ou Secure Network Analytics et avez activé la fonction GTA, vos produits seront affectés par cette modification.

Quel est l'impact sur mon produit ?

- Terminaux sécurisés
  - Secure Endpoint ne recevra plus d'alertes et de données télémétriques provenant de Global Threat Analytics. Il en résultera moins de notifications de console liées au trafic réseau corrélé aux adresses IP et URL malveillantes.

- Analyses réseau sécurisées
  - Le widget Alertes de menaces globales du tableau de bord SNA ne sera plus disponible après la version 7.5.1. Pour les versions précédentes, le widget GTA du tableau de bord SNA reste et ne se charge pas. Les clients de Cisco Secure Network Analytics peuvent obtenir des résultats similaires à ceux du service GTA en utilisant la fonctionnalité Central Analytics disponible avec l'architecture Data Store et en l'intégrant au flux Talos Threat Intelligence. o Pour plus d'informations sur l'impact du SNA, reportez-vous à la FAQ relative à la fin du service Global Threat Alerts (GTA)

Quel est l'impact actuel sur mon service ?

- Les clients utilisant la fonctionnalité GTA ne seront pas affectés avant la date de mise hors service du 31 juillet 2024.

Que dois-je faire pour me préparer à la mise hors service de cette fonctionnalité ?

- Secure Endpoint : aucune action du client n'est requise.
- Secure Network Analytics : aucune action du client n'est requise.

Dois-je prendre des mesures après la mise hors service de la fonctionnalité ?

- Les clients doivent envisager de désactiver l'envoi de journaux au service GTA à partir de leur appareil de sécurité Web (WSA) ou de leur proxy F5.
- Pour SNA :
  - Désactiver la fonctionnalité dans la gestion centralisée (SMC)
  (Accédez à Inventory > sélectionnez votre SMC > Appliance Configuration > General > External Services> décochez la case Enable Global Threat Alerts.)
  - Répétez l'opération avec vos collecteurs de flux (FC).
  OU
  - Mise à niveau vers la version 7.5.1 si disponible à l'été 2024

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.