Meilleures pratiques de demande de couverture des terminaux sécurisés Cisco

Table des matières

Introduction

Ce document décrit le processus qui doit être utilisé lors de la demande de couverture Talos pour une menace connue qui a déjà été identifiée mais qui n'est pas actuellement détectée par Secure Endpoint.

Différentes sources d'information

Il peut y avoir plusieurs sources à partir desquelles ces menaces sont identifiées et publiées, et voici quelques-unes des plates-formes couramment utilisées :

- Cisco CVE publié
- CVE (Common Vulnerabilities and Exposures) publié
- Avis Microsoft
- Informations sur les menaces tierces

Cisco veut s'assurer que les sources de données sont légitimes avant que Talos n'examine les informations et identifie la couverture appropriée.

Pour examiner la position et la couverture de Cisco pour les menaces en question, nous avons plusieurs sources Cisco/Talos qui doivent être examinées avant de demander une nouvelle demande de couverture.

Portail des vulnérabilités Cisco

Pour tout CVE relatif aux produits Cisco, consultez ce portail pour plus d'informations : https://sec.cloudapps.cisco.com/security/center/publicationListing.x

Portail Talos

Talos Intelligence Portal doit être le premier point de référence pour vérifier si cette menace a fait l'objet d'une enquête ou si elle fait actuellement l'objet d'une enquête de la part de Talos : https://talosintelligence.com/

Blogs Talos

Les blogs Cisco Talos fournissent également des informations sur les menaces évaluées et étudiées par Talos : https://blog.talosintelligence.com/

Nous pourrions trouver la plupart des informations pertinentes sous la rubrique **« Informations sur les failles »** qui inclut également tous les **« Avis Microsoft » publiés.**

Enquête supplémentaire avec les produits Cisco

Cisco propose plusieurs produits qui peuvent vous aider à examiner les hashs/vecteurs de menace et à déterminer si Secure Endpoint couvre les menaces.

Cisco SecureX Cisco Threat Response Investigation (CTR)

Nous pouvons étudier les vecteurs de menace dans le cadre des enquêtes CTR. Vous trouverez plus d'informations à ce sujet à l'adresse suivante : https://docs.securex.security.cisco.com/Threat-Response-Help/Content/investigate.html

Cisco XDR Investigate

Cisco XDR offre des fonctionnalités améliorées d'analyse des vecteurs de menace. Pour plus d'informations sur ces fonctionnalités, consultez le site : https://docs.xdr.security.cisco.com/Content/Investigate/investigate.htm

Blogs Cisco utiles

Veuillez lire ces blogs pendant qu'ils passent en revue certaines des fonctionnalités discutées dans la section précédente :

https://blogs.cisco.com/tag/relevant-and-extended-detection-with-securex

Étapes suivantes

Si nous ne trouvons pas les vecteurs de menace couverts en suivant les étapes ci-dessus, nous pouvons demander une couverture Talos pour la menace en envoyant une demande d'assistance TAC.

https://www.cisco.com/c/en/us/support/index.html

Pour accélérer l'évaluation et l'enquête pour la demande de couverture, nous vous demandons les informations suivantes sur la menace :

- Source des informations sur les menaces (CVE/Advisory/3rd Party Investigation/Technotes/Blogs)
- Hachages SHA256 associés
- Exemple du fichier (si disponible).

Une fois que les informations sont disponibles, Talos les examine et examine la demande en conséquence.

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.