Meilleures pratiques de demande de couverture des terminaux sécurisés Cisco

Table des matières

Introduction

Différentes sources d'information

- Portail des vulnérabilités Cisco
- Portail Talos
- Blogs Talos

Enquête supplémentaire avec les produits Cisco

- Cisco XDR Investigate
- Blogs Cisco utiles

Étapes suivantes

Aperçu

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 : Portail des vulnérabilités Cisco

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 : Portail Talos

Blogs Talos

Les blogs Cisco Talos fournissent également des informations sur les menaces évaluées et étudiées par Talos : Blogs Talos

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 XDR Investigate

Cisco XDR offre des fonctionnalités améliorées d'analyse des vecteurs de menace. Pour plus d'informations sur ces fonctionnalités, consultez le site : Cisco XDR Investigate

Blogs Cisco utiles

Veuillez consulter ces blogs au fur et à mesure qu'ils passent en revue certaines fonctionnalités abordées dans la section précédente, telles que la détection et la réponse étendues de Cisco

Étapes suivantes

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

Afin d'accélérer l'évaluation et l'enquête pour la demande de couverture, nous vous demandons les renseignements suivants :

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

Remarque : Pour les demandes de couverture liées aux tests de pénétration ou à l'association rouge, les exigences peuvent varier en fonction du type de test. Dans certains cas, des informations supplémentaires peuvent être demandées au client. Une fois les informations nécessaires fournies, Talos examine, évalue et étudie la demande en conséquence.

Aperçu

Une fois les informations requises reçues, nous entamons un processus d'examen spécialisé. Pour garantir le niveau de protection le plus élevé, le calendrier de livraison est guidé par plusieurs facteurs critiques :

Analyse personnalisée
Étant donné que chaque scénario de menace et chaque environnement client sont uniques, nous effectuons une validation personnalisée pour garantir une couverture de sécurité efficace sans perturber les opérations de votre entreprise.

Réponse pilotée par les données
La vitesse de notre analyse est directement soutenue par la disponibilité d'échantillons pertinents de données télémétriques, d'artefacts ou de programmes malveillants.

Assurance Qualité Rigoureux
Pour préserver la stabilité et la fiabilité du produit, chaque solution est soumise à des tests complets et à un déploiement progressif.

Gestion des versions sécurisées
Nous alignons les mises à jour sur les cycles de versions établis pour garantir que toutes les protections sont fournies de manière contrôlée et fiable.

Protection adaptative
La sécurité est un processus continu. Après le déploiement, nous surveillons et ajustons en permanence nos détections pour anticiper l'évolution des menaces.

Hiérarchisation des problèmes critiques
Nous évaluons chaque demande individuellement. Les problèmes impliquant des vulnérabilités de gravité élevée, une exploitation active ou des faux positifs critiques sont automatiquement traités rapidement par le biais de workflows accélérés afin de réduire votre exposition aux risques.

Nous apprécions votre partenariat alors que nous nous efforçons d'offrir une protection robuste et précise, conçue pour garantir la sécurité et la productivité de votre entreprise.

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.