Prácticas recomendadas para la solicitud de cobertura de terminales seguros

Contenido

Introducción

Este documento describe el proceso que se debe utilizar cuando se solicita Talos Coverage para una amenaza conocida que ya ha sido identificada pero que actualmente no es detectada por Secure Endpoint.

Diferentes fuentes de información

Puede haber varias fuentes desde las que se identifican y publican estas amenazas. A continuación se indican algunas de las plataformas más utilizadas:

- CVE de Cisco publicado
- CVE publicado (exposiciones y vulnerabilidades comunes)
- Recomendaciones de Microsoft
- Inteligencia de amenazas de terceros

Cisco quiere asegurarse de que las fuentes de datos son legítimas antes de que consigamos que Talos revise la información e identifique la cobertura relevante.

Para revisar la postura de Cisco y la cobertura de las amenazas en cuestión, tenemos varias fuentes de Cisco/Talos que deben revisarse antes de solicitar una nueva solicitud de cobertura.

Portal de vulnerabilidades de Cisco

Para cualquier CVE relacionado con productos de Cisco, consulte este portal para obtener más información: https://sec.cloudapps.cisco.com/security/center/publicationListing.x

Portal Talos

Talos Intelligence Portal debe ser el primer punto de referencia para revisar si esta amenaza se ha investigado o está siendo investigada por Talos: https://talosintelligence.com/

Blogs de Talos

Los blogs de Cisco Talos también proporcionan información sobre las amenazas que Talos evalúa e investiga: https://blog.talosintelligence.com/

Podríamos encontrar la mayor parte de la información pertinente en **"Información de vulnerabilidad"** que también incluye todos los **"Asesores de Microsoft" publicados.**

Investigación adicional con productos de Cisco

Cisco ofrece varios productos que pueden ayudarle a revisar los vectores/hashes de las amenazas e identificar si Secure Endpoint proporciona cobertura para las amenazas.

Investigación Cisco SecureX Cisco Threat Response Investigation (CTR)

Podemos investigar los vectores de amenazas como parte de las investigaciones del CTR, y se puede consultar más información aquí: https://docs.securex.security.cisco.com/Threat-Response-Help/Content/investigate.html

Investigación de Cisco XDR

Cisco XDR proporciona funciones mejoradas para investigar vectores de amenazas, y puede encontrar más información sobre esta funcionalidad aquí: https://docs.xdr.security.cisco.com/Content/Investigate/investigate.htm

Blogs útiles de Cisco

Revise estos blogs a medida que revisan algunas de las funcionalidades que se trataron en la sección anterior:

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

Pasos siguientes

Si no encontramos los vectores de amenaza cubiertos siguiendo los pasos anteriores, podemos solicitar la cobertura de Talos para la amenaza presentando una solicitud de asistencia del TAC.

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

Para acelerar la evaluación y la investigación de la solicitud de cobertura, solicitamos la siguiente información sobre la amenaza:

- Fuente de inteligencia de amenazas (CVE/Advisory/$^{\text{Investigación}}$ de terceros/Technotes/Blogs)
- Hashes SHA256 asociados
- Ejemplo del archivo (si está disponible).

Una vez que la información está disponible, Talos evalúa e investiga la solicitud en consecuencia.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).