Práticas recomendadas de solicitação de cobertura de endpoint seguro

Contents

Introdução

Este documento descreve o processo que deve ser usado ao solicitar a cobertura do Talos para uma ameaça conhecida que já foi identificada, mas não é detectada atualmente pelo Secure Endpoint.

Diferentes fontes de informação

Pode haver várias fontes das quais essas ameaças são identificadas e publicadas, e aqui estão algumas das plataformas mais usadas:

- Cisco CVE publicado
- CVE (Common Vulnerabilities and Exposures, Vulnerabilidades e exposições comuns) publicado
- Conselhos da Microsoft
- Inteligência de ameaças de terceiros

A Cisco deseja garantir que as fontes de dados sejam legítimas antes de obter o Talos para analisar as informações e identificar a cobertura relevante.

Para analisar a postura e a cobertura da Cisco para as ameaças em questão, temos várias fontes da Cisco/Talos que devem ser analisadas antes de solicitar uma nova solicitação de cobertura.

Portal de vulnerabilidade da Cisco

Para obter mais informações sobre qualquer CVE relacionado a produtos da Cisco, consulte este portal: https://sec.cloudapps.cisco.com/security/center/publicationListing.x

Portal Talos

O Talos Intelligence Portal deve ser o primeiro ponto de referência para analisar se essa ameaça foi investigada ou está sendo investigada pelo Talos: https://talosintelligence.com/

Blogs do Talos

Os blogs do Cisco Talos também fornecem informações sobre as ameaças que são avaliadas e investigadas pelo Talos: https://blog.talosintelligence.com/

Podemos encontrar a maioria das informações pertinentes em **"Informações de vulnerabilidade"** que também inclui todos os **"Conselhos da Microsoft" publicados.**

Investigação adicional usando produtos da Cisco

A Cisco oferece vários produtos que podem ajudar a analisar os vetores de ameaças/hashes e a identificar se o Secure Endpoint oferece cobertura para as ameaças.

Investigação de resposta a ameaças (CTR) Cisco SecureX

Podemos investigar os vetores de ameaça como parte das investigações do CTR, e mais informações podem ser revisadas aqui: https://docs.securex.security.cisco.com/Threat-Response-Help/Content/investigate.html

Investigação do Cisco XDR

O Cisco XDR oferece recursos aprimorados para investigar vetores de ameaças, e mais informações sobre a funcionalidade podem ser encontradas aqui:
https://docs.xdr.security.cisco.com/Content/Investigate/investigate.htm

Blogs úteis da Cisco

Revise esses blogs à medida que analisarem algumas das funcionalidades discutidas na seção anterior:

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

Próximas etapas

Se não encontrarmos os vetores de ameaças cobertos usando as etapas acima, podemos solicitar a cobertura do Talos para a ameaça preenchendo uma solicitação de suporte do TAC.

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

Para agilizar a avaliação e a investigação da solicitação de cobertura, solicitamos estas informações sobre a ameaça:

- Fonte da inteligência de ameaças (CVE/Advisory/3Investigação de terceiros/Technotes/Blogs)
- Hashes SHA256 Associados
- Exemplo do arquivo (se disponível).

Quando as informações estiverem disponíveis, o Talos avaliará e investigará a solicitação adequadamente.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.