Procedure ottimali per la richiesta di copertura degli endpoint sicuri

Sommario

Introduzione

Questo documento descrive il processo da utilizzare quando si richiede Talos Coverage per una minaccia nota già identificata ma non attualmente rilevata da Secure Endpoint.

Diverse fonti di informazione

Le minacce possono provenire da diverse fonti, identificate e pubblicate, e di seguito sono elencate alcune delle piattaforme più comuni:

- Cisco CVE pubblicato
- CVE pubblicato (Vulnerabilità ed esposizioni comuni)
- Consulenze Microsoft
- Threat Intelligence di terze parti

Cisco desidera accertarsi che le origini dati siano legittime prima di richiedere a Talos di esaminare le informazioni e identificare la copertura pertinente.

Per rivedere la posizione di Cisco e la copertura delle minacce in questione, abbiamo diverse fonti Cisco/Talos che devono essere riviste prima di richiedere una nuova richiesta di copertura.

Cisco Vulnerability Portal

Per qualsiasi CVE relativo ai prodotti Cisco, consulta questo portale per ulteriori informazioni: https://sec.cloudapps.cisco.com/security/center/publicationListing.x

Portale Talos

Talos Intelligence Portal deve essere il primo punto di riferimento da esaminare se questa minaccia è stata indagata o è attualmente sotto indagine da Talos: https://talosintelligence.com/

Blog Talos

Anche i blog di Cisco Talos forniscono informazioni sulle minacce valutate e indagate da Talos: https://blog.talosintelligence.com/

La maggior parte delle informazioni pertinenti è disponibile in **"Informazioni sulla vulnerabilità"** che include anche tutti i **"Microsoft Advisories".**

Ulteriori indagini sull'utilizzo dei prodotti Cisco

Cisco offre diversi prodotti che possono aiutare a rivedere i vettori/hash della minaccia e a identificare se Secure Endpoint fornisce copertura per le minacce.

Cisco SecureX - Indagine sulle risposte alle minacce Cisco (CTR)

Possiamo indagare sui vettori di minaccia come parte delle indagini del CTR, e ulteriori informazioni possono essere riviste qui: https://docs.securex.security.cisco.com/Threat-Response-Help/Content/investigate.html

Cisco XDR Investigate

Cisco XDR offre funzionalità avanzate per lo studio dei vettori di minaccia. Per ulteriori informazioni sulle funzionalità, visitare il sito Web all'indirizzo https://docs.xdr.security.cisco.com/Content/Investigate/investigate.htm

Blog Cisco utili

Leggere attentamente i seguenti blog, che illustrano alcune delle funzionalità descritte nella sezione precedente:

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

Fasi successive

Se non riusciamo a trovare i vettori di minaccia descritti nei punti precedenti, possiamo richiedere la copertura Talos per la minaccia presentando una richiesta di assistenza TAC.

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

Per accelerare la valutazione e l'analisi della richiesta di copertura, è necessario fornire le seguenti informazioni sulla minaccia:

- Fonte dell'intelligence sulle minacce (CVE/Advisory/3rd Party Investigation/Technotes/Blogs)
- Hash SHA256 associati
- Esempio del file (se disponibile).

Una volta che le informazioni sono disponibili, Talos esamina e analizza la richiesta di conseguenza.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).