Best practice per la richiesta di copertura degli endpoint sicuri Cisco

Sommario

Introduzione

Diverse fonti di informazione

- Cisco Vulnerability Portal
- Portale Talos
- Blog Talos

Ulteriori indagini sull'utilizzo dei prodotti Cisco

- Cisco XDR Investigate
- Blog Cisco utili

Fasi successive

Panoramica

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: Cisco Vulnerability Portal

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: Portale Talos

Blog Talos

I blog di Cisco Talos forniscono anche informazioni sulle minacce valutate e indagate da Talos: Blog Talos

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 XDR Investigate

Cisco XDR offre funzionalità avanzate per lo studio dei vettori di minaccia. Per ulteriori

informazioni sulle funzionalità, fare riferimento a: Cisco XDR Investigate

Blog Cisco utili

Esaminare i blog mano a mano che esaminano alcune delle funzionalità descritte nella sezione precedente, ad esempio le funzionalità di rilevamento e risposta estese di Cisco

Fasi successive

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

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

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

Nota: Per le richieste di copertura relative a Penetration Testing o Red Teaming, i requisiti possono variare a seconda del tipo di prova. In alcuni casi, possono essere richieste al cliente ulteriori informazioni. Una volta fornite le informazioni necessarie, Talos esamina, valuta ed esamina la richiesta di conseguenza.

Panoramica

Una volta ricevute le informazioni richieste, viene avviato un processo di revisione specializzato. Per garantire il massimo livello di protezione, la tempistica di consegna è guidata da diversi fattori critici:

Analisi personalizzata
Poiché ogni scenario di minaccia e ogni ambiente del cliente è unico, EMC esegue una convalida personalizzata per garantire un'efficace copertura della sicurezza senza interrompere le attività aziendali.

Risposta basata su dati
La velocità dell'analisi è direttamente supportata dalla disponibilità di telemetria, artefatti o campioni di malware rilevanti.

Controllo rigoroso della qualità
Per mantenere la stabilità e l'affidabilità del prodotto, ogni soluzione viene sottoposta a test completi e a un'implementazione graduale.

Gestione sicura delle release
Gli aggiornamenti vengono allineati ai cicli di rilascio stabiliti per garantire che tutte le protezioni vengano fornite in modo controllato e affidabile.

Adaptive Protection
La sicurezza è un processo continuo. In seguito all'installazione, EMC monitora e ottimizza continuamente le rilevazioni per tenere il passo con l'evoluzione del panorama delle minacce.

Assegnazione di priorità ai problemi critici
Valutiamo ogni singola richiesta. I problemi relativi a vulnerabilità ad alta gravità, sfruttamento attivo o falsi positivi critici vengono automaticamente monitorati attraverso flussi di lavoro più rapidi per ridurre al minimo l'esposizione al rischio.

La collaborazione con EMC è molto importante per offrire una protezione affidabile e precisa, progettata per garantire la sicurezza e la produttività dell'organizzazione.

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).