Beste praktijken voor Secure Endpoint Coverage

Inhoud

Inleiding

Dit document beschrijft het proces dat moet worden gebruikt wanneer Talos Coverage wordt gevraagd voor een bekende bedreiging die al is geïdentificeerd maar momenteel niet door Secure Endpoint wordt gedetecteerd.

Verschillende informatiebronnen

Er kunnen meerdere bronnen zijn van waaruit deze bedreigingen worden geïdentificeerd en gepubliceerd, en hier zijn enkele van de meest gebruikte platforms:

- Gepubliceerde Cisco CVE
- Gepubliceerde CVE (Gemeenschappelijke kwetsbaarheden en blootstellingen)
- Microsoft Advisories
- Derden-bedreigingsinformatie

Cisco wil ervoor zorgen dat de gegevensbronnen legitiem zijn voordat we Talos krijgen om de informatie te beoordelen en de relevante dekking te identificeren.

Om de positie en dekking van Cisco voor de bedreigingen in kwestie te bekijken, hebben we verschillende Cisco/Talos-bronnen die moeten worden beoordeeld voordat we een nieuw Coverage-verzoek indienen.

Cisco Vulnerability Portal

Raadpleeg voor elke CVE met betrekking tot Cisco-producten deze portal voor meer informatie: https://sec.cloudapps.cisco.com/security/center/publicationListing.x

Talos-portal

Talos Intelligence Portal moet het eerste referentiepunt zijn om te beoordelen of deze dreiging is onderzocht of momenteel wordt onderzocht door Talos: https://talosintelligence.com/

Talos Blogs

Cisco Talos Blogs bieden ook informatie over de bedreigingen die worden geëvalueerd en onderzocht door Talos: https://blog.talosintelligence.com/

We zouden de meeste relevante informatie kunnen vinden onder **"Vulnerability Information",** waaronder ook alle gepubliceerde **"Microsoft Advisories".**

Aanvullend onderzoek met Cisco-producten

Cisco biedt meerdere producten die kunnen helpen bij het bekijken van de Threat vectors/hashes en het identificeren als Secure Endpoint dekking biedt voor de bedreigingen.

Cisco SecureX - Cisco-onderzoek van bedreigingsrespons (CTR)

We kunnen de Threat Vectors onderzoeken als onderdeel van CTR-onderzoeken, en meer informatie kan hier worden bekeken: https://docs.securex.security.cisco.com/Threat-Response-Help/Content/investigate.html

Cisco XDR onderzoeken

Cisco XDR biedt uitgebreide mogelijkheden voor het onderzoeken van bedreigingsvectoren. Meer informatie over de functionaliteit kunt u hier vinden: https://docs.xdr.security.cisco.com/Content/Investigate/investigate.htm

Handige Cisco-blogs

Beoordeel deze blogs bij het overlopen van een aantal van de functies die in de vorige sectie zijn besproken:

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

Volgende stappen

Als we de bedreigingsvectoren niet vinden die worden bestreken met de bovenstaande stappen, kunnen we Talos Coverage voor de bedreiging aanvragen door een TAC-ondersteuningsverzoek in te dienen.

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

Om de evaluatie en het onderzoek voor de Coverage-aanvraag te versnellen, vragen we deze informatie over de bedreiging:

- Bron van de informatie over bedreigingen (CVE/Advisory/3rd Party Investigation/Technotes/Blogs)
- Gekoppelde SHA256-hashes
- Voorbeeld van het bestand (indien beschikbaar.)

Zodra de informatie beschikbaar is, evalueert Talos het verzoek dienovereenkomstig en onderzoekt het.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.