Begrijp de potentieel schadelijke beveiligingscategorie in Paraplu

Inhoud

Inleiding

Dit document beschrijft de categorie Potentieel schadelijke beveiliging in Cisco Umbrella.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

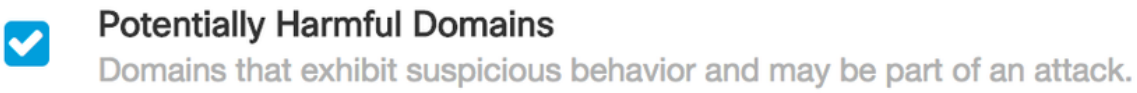
Gebruikte componenten

De informatie in dit document is gebaseerd op Cisco Umbrella.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Overzicht

Paraplu-klanten hebben verschillende niveaus van risicotolerantie als het gaat om beveiliging. Afhankelijk van de branche en het soort werk dat u doet, kan het nuttig zijn om potentieel schadelijke activiteiten proactief te monitoren en te blokkeren. De nieuwe beveiligingsinstelling "Potentieel schadelijk" kunt u vinden onder Voorkomen naast andere beveiligingsinstellingen en is ingesteld op Toestaan standaard:



115011476788

Details

Potentieel schadelijk is een beveiligingscategorie die domeinen bevat die waarschijnlijk kwaadaardig zijn. Het is anders dan Umbrella's "malware" categorieën omdat Umbrella hen met een lager niveau van vertrouwen heeft gerangschikt over de vraag of ze daadwerkelijk kwaadaardig zijn. Een andere manier om het te formuleren is dat deze domeinen als verdacht worden beschouwd volgens onze onderzoeksanalisten en de algoritmen die we gebruiken om het geheel te bepalen, maar niet noodzakelijkerwijs bekend staan als kwaadaardig.

Het gebruik van deze categorie hangt af van uw tolerantie voor het risico van het blokkeren van potentieel goede domeinen. Als u een zeer veilige omgeving hebt, is dit een goede categorie om te blokkeren en als uw omgeving losser is, kunt u dit eenvoudig toestaan en controleren.

Als u niet zeker weet onder welke van deze u valt, kunt u activiteiten controleren die in uw rapporten zijn bevestigd als "Potentieel schadelijk". Het beschikbaar hebben van deze categorie kan extra granulariteit bieden bij het classificeren van verkeer, het vergroten van de zichtbaarheid en het bieden van meer bescherming en het verbeteren van de respons op incidenten. Als u bijvoorbeeld van mening bent dat een machine is geïnfecteerd met malware, kan het bekijken van de potentieel schadelijke domeinen die het heeft bezocht u helpen om het compromisniveau beter te beoordelen.

Umbrella bepaalt wat "potentieel schadelijk" is door verschillende factoren te wegen die erop wijzen dat het domein weliswaar niet duidelijk kwaadaardig is, maar wel een bedreiging kan vormen. Er zijn bijvoorbeeld verschillende soorten DNS-tunneldiensten. Sommige van deze diensten vallen in de categorieën van goedaardige, kwaadaardige en DNS-tunneling VPN, maar sommige zijn meer onduidelijk en vallen niet in een van deze categorieën. Als de use case voor de tunneling onbekend en verdacht is, kan de bestemming in de categorie Potentieel Schadelijk vallen.

Een ander voorbeeld komt uit Umbrella's Spike rank model. Het Spike-rankmodel van Umbrella maakt gebruik van enorme hoeveelheden DNS-verzoekgegevens en detecteert domeinen met pieken in hun DNS-verzoekpatronen met behulp van geluidsgolfgrafiek. Het verkeer dat hoog op de Spike rank domein raakt kan automatisch worden geclassificeerd als kwaadaardig, en het verkeer dat lager op de drempel kan vallen in de categorie Potentieel Schadelijk.

Om ongewenste detecties in een van deze categorieën te melden:

- Stuur alle aanvragen voor gegevenscategorisatie naar Cisco Talos via Talos Support.
- Voor algemene stappen voor het indienen van aanvragen bij Cisco Talos, raadpleegt u How

To: Submit A Categorization Request.

Voor de categorie Potentieel Schadelijk hercategoriseert Umbrella het niet als veilig zonder garanties te nemen dat het domein absoluut legitiem is.

Beide categorieën kunnen worden gefilterd in uw rapporten, net als elke andere beveiligingscategorie.

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.