Kennenlernen der potenziell schädlichen Sicherheitskategorie unter Umbrella

Inhalt

Einleitung

In diesem Dokument wird die Sicherheitskategorie "Potenziell schädlich" in Cisco Umbrella beschrieben.

Voraussetzungen

Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

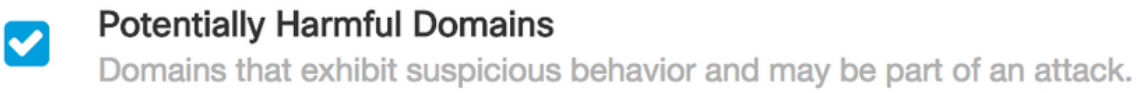
Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf Cisco Umbrella.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Überblick

Umbrella-Kunden können in puncto Sicherheit unterschiedlich hohe Risikotoleranz vorweisen. Je nach Branche und Art Ihrer Arbeit kann es von Vorteil sein, potenziell schädliche Aktivitäten proaktiv zu überwachen und zu blockieren. Die neue Sicherheitseinstellung "Potenziell schädlich" befindet sich unter Verhindern neben anderen Sicherheitseinstellungen und ist standardmäßig auf Zulassen eingestellt:



115011476788

Details

Potenziell schädlich ist eine Sicherheitskategorie, die Domänen enthält, die wahrscheinlich schädlich sind. Es unterscheidet sich von Umbrellas "Malware"-Kategorien, da Umbrella sie mit einem geringeren Grad an Vertrauen in die tatsächliche Schadsoftware eingestuft hat. Eine weitere Möglichkeit, es zu formulieren, ist, dass diese Domains nach unseren Forschungsanalysten und die Algorithmen, die wir verwenden, um zu bestimmen, aber nicht unbedingt als schädlich bekannt, als verdächtig angesehen werden.

Die Verwendung dieser Kategorie hängt von Ihrer Toleranz für das Risiko ab, potenziell gute Domains zu blockieren. Wenn Sie über eine hochsichere Umgebung verfügen, ist dies eine gute Kategorie, die Sie blockieren sollten. Wenn Ihre Umgebung lockerer ist, können Sie sie einfach zulassen und überwachen.

Wenn Sie sich nicht sicher sind, unter welche Kategorie Sie fallen, können Sie Aktivitäten überwachen, die in Ihren Berichten als "Potenziell schädlich" bestätigt werden. Diese Kategorie bietet zusätzliche Präzision bei der Klassifizierung des Datenverkehrs, erhöht die Transparenz und sorgt für einen besseren Schutz sowie für eine bessere Reaktion auf Vorfälle. Wenn Sie beispielsweise glauben, dass ein Computer mit Malware infiziert ist, können Sie mithilfe eines Einblicks in die potenziell schädlichen Domänen, die er besucht hat, besser beurteilen, wie hoch die Gefährdung ist.

Umbrella ermittelt, was "potenziell schädlich" ist, indem mehrere Faktoren gegeneinander abgewogen werden, die darauf hindeuten, dass die Domain zwar nicht eindeutig schädlich ist, aber eine Bedrohung darstellen könnte. Es gibt beispielsweise verschiedene Arten von DNS-Tunneling-Diensten. Einige dieser Services fallen in die Kategorien "Gutartig", "bösartig" und "DNS-Tunneling-VPN", andere dagegen noch unklar und nicht in eine dieser Kategorien. Wenn der Anwendungsfall für das Tunneling unbekannt und verdächtig ist, kann das Ziel in die Kategorie "Potenziell schädlich" fallen.

Ein weiteres Beispiel ist Umbrella's Spike Rang-Modell. Das Spike-Rank-Modell von Umbrella nutzt große Mengen an DNS-Anforderungsdaten und erkennt Domänen mit Spitzen in ihren DNS-Anforderungsmustern mithilfe von Soundwellendiagrammen. Der Datenverkehr, der in der Spike-Ranking-Domäne hoch auftritt, kann automatisch als schädlich klassifiziert werden, und Datenverkehr, der niedriger als der Schwellenwert ist, kann in die Kategorie "Potenziell schädlich" fallen.

So melden Sie unerwünschte Entdeckungen in einer der folgenden Kategorien:

- Bitte senden Sie alle Anfragen zur Datenkategorisierung an Cisco Talos über den Talos Support.
- Allgemeine Informationen zum Senden von Anfragen an Cisco Talos finden Sie unter Gewusst wie: Kategorisierungsanfrage einreichen.

Für die potenziell schädliche Kategorie, Umbrella nicht neu kategorisieren sie als sicher, ohne zu versichern, dass die Domain ist absolut legitim.

Beide Kategorien können in Ihren Berichten wie jede andere Sicherheitskategorie gefiltert werden.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.