傘の中の潜在的に有害なセキュリティカテゴリの理解

内容

はじめに

このドキュメントでは、Cisco Umbrellaの潜在的に有害なセキュリティカテゴリについて説明します。

前提条件

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、Cisco Umbrellaに基づくものです。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

概要

包括ユーザは、セキュリティに関して異なるレベルのリスク耐性を持っています。業種や業務の種類によっては、潜在的に有害な活動を予防的に監視してブロックすることが有益な場合があります。新しい「Potentially Problect」セキュリティ設定は、「Other Security Settings」の横の「Prevent」で確認できます。デフォルトでは「Allow」に設定されています。

Potentially Harmful Domains

Domains that exhibit suspicious behavior and may be part of an attack.

115011476788

詳細

潜在的に有害とは、悪意のある可能性のあるドメインを含むセキュリティカテゴリです。これは、Umbrellaの「マルウェア」カテゴリとは異なります。Umbrellaは、実際に悪意があるかどうかについて低い信頼レベルでマルウェアをランク付けしたためです。別の言い方をすると、これらのドメインは、シスコの調査アナリストや、全体を判断するために使用するアルゴリズムによると疑わしいと見なされますが、悪意があると必ずしも認識されているわけではありません。

このカテゴリの使用は、潜在的に良好なドメインをブロックするリスクに対する許容度によって異なります。セキュリティの高い環境では、このカテゴリがブロックに適しています。環境の安全性が低い場合は、許可と監視を行うだけで済みます。

いずれに該当するかわからない場合は、レポートで「潜在的に有害」と確認されたアクティビティをモニタできます。このカテゴリを使用可能にすると、トラフィックの分類がさらに細かくなり、可視性が向上し、保護が強化されてインシデント対応が改善されます。 たとえば、マシンがマルウェアに感染していると考えられる場合は、そのマシンがアクセスしている潜在的に有害なドメインを調べることで、侵害のレベルをより適切に評価できます。

Umbrellaは、ドメインが明らかに悪意のあるものではないが、脅威を引き起こす可能性があることを示すいくつかの要因を評価することで、「潜在的に有害」な要素を判断します。たとえば、さまざまなタイプのDNSトンネリングサービスがあります。これらのサービスの一部は、良性、悪意、およびDNSトンネリングVPNのカテゴリに分類されますが、一部は不明で、これらのカテゴリのいずれにも分類されません。トンネリングのユースケースが不明で疑わしい場合、宛先は潜在的に有害なカテゴリに分類される可能性があります。

もう1つの例は、UmbrellaのSpikeランクモデルです。UmbrellaのSpikeランクモデルは、大量のDNS要求データを活用し、音波グラフを使用してDNS要求パターンがスパイクしているドメインを検出します。スパイクのランクのドメインで高いトラフィックは自動的に悪意のあるトラフィックとして分類され、しきい値を下回るトラフィックは潜在的に有害なカテゴリに分類される可能性があります。

次のいずれかのカテゴリで不要な検出をレポートするには、次の手順を実行します。

- データ分類に関するすべてのリクエストは、Talos Supportを通じてCisco Talosに送信してください。
- Cisco Talosにリクエストを送信する一般的な手順については、「How to: Submit A Categorization Request」を参照してください。

潜在的に有害なカテゴリについては、Umbrellaは、ドメインが絶対に正当であることを保証することなく、安全として再分類しません。

どちらのカテゴリも、他のセキュリティカテゴリと同様に、レポートでフィルタ処理できます。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。