IPSの誤検出の確認または係争（傘を使用）

内容

はじめに

このドキュメントでは、侵入防御サービス(IPS)の誤検出をCisco Umbrellaで確認または阻止する方法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

Cisco Umbrellaの侵入防御システム(IPS)は、既知の脅威である脆弱性に関連すると見なされるパケットを検出（およびオプションでブロック）しますが、単純にパケットの形式が異常である場合にもブロックします。

管理者は、次のデフォルトリストに基づいて、脅威の検出に使用するIPSシグニチャリストを選択します。

- セキュリティを介した接続
- セキュリティと接続のバランス
- 接続を介したセキュリティ
- 最大検出

選択したシグニチャリストがIPS False Positiveの発生数に大きく影響する可能性があることを覚えておくことが重要です。最も安全なモード（Maximum DetectionやSecurity Over Connectivityなど）では、セキュリティが重視されるため、望ましくないIPS検出が作成されることが予想されます。最も安全なモードは、完全なセキュリティが必要な場合にのみ推奨され、管理者は大量のIPSイベントを監視および確認する必要性を予測する必要があります。

各種モードの詳細については、『IPSに関するドキュメント』を参照してください。

IPS検出の確認

IPSイベントを表示するには、Umbrellaダッシュボードのアクティビティ検索を使用します。各イベントには、次の2つの重要な情報があります。

- IPSシグニチャID/カテゴリ/名前。https://snort.orgで検索可能
- CVE番号（該当する場合）https://www.cve.org/で検索可能

すべてのIPS検出が既知の不正利用/攻撃を示すわけではありません。シグニチャの多く（特にMax Detectionモード）は、単に特定のタイプのトラフィックが存在すること、またはプロトコル違反を示すだけです。イベントに関するその他の詳細（送信元/宛先など）とともに、前述の情報ソースを確認して、イベントがセキュリティチームによる詳細な調査を必要とするかどうかを判断することが重要です。

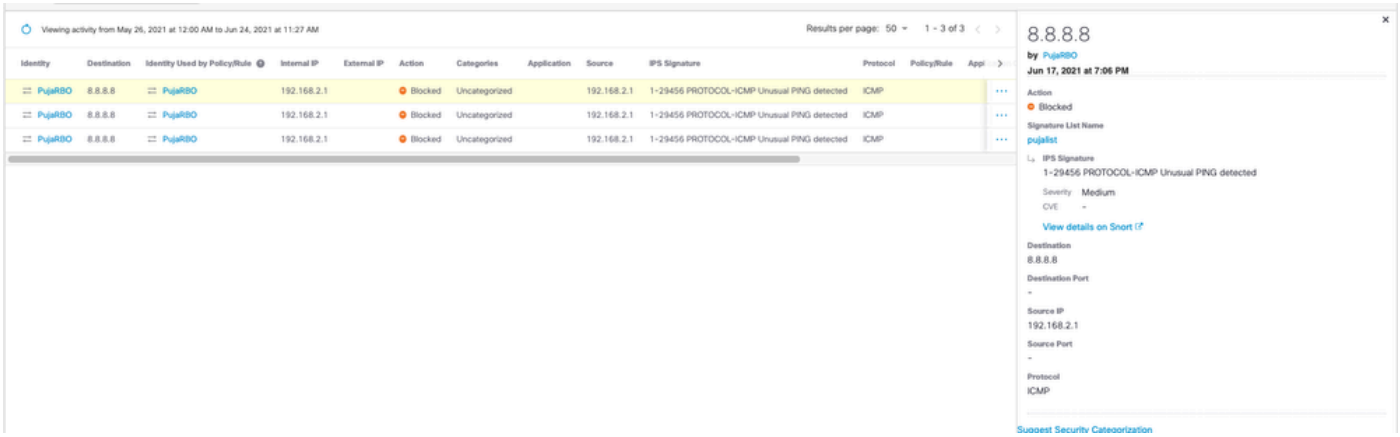
シグニチャカテゴリは、IPS検出のタイプに関する追加のコンテキストを提供する際に役立ちます。snort.orgで入手できるカテゴリを確認してください。

プロトコル違反

次の例では、IPSイベントがこのシグニチャにリンクされています（このシグニチャはIPSイベントを示します）。
https://www.snort.org/rule_docs/1-29456

シグニチャの説明は次のとおりです。

「ルールは、通常のPINGの形式に従っていないネットワークに着信するPINGトラフィックを探します。」



4403885889428

この場合、Snortルールは必ずしも特定の不正利用を検出しているわけではなく、ブロックされた不正なICMPパケットを検出しています。snort.orgで入手できる情報とイベントに関するその他の詳細（送信元/宛先など）に基づいて、管理者はこのイベントにそれ以上の調査は必要ないと判断できます

アプリケーションの互換性

一部の正規のアプリケーションは、特にアグレッシブな（最大検出）モードが設定されている場合、IPSシグニチャと互換性がありません。このようなシナリオでは、「プロトコル違反」セクションで説明した理由により、アプリケーションがブロックされる可能性があります。アプリケーションが予期しない方法でプロトコルを使用したり、通常は他のトラフィック用に予約されているポートを介してカスタムプロトコルを使用したりすることがあります。

アプリケーションが正当であっても、これらの検出は有効であることが多く、シスコが常に修正できるとは限りません。

正当なアプリケーションがIPSによってブロックされる場合、Umbrellaはイベント/シグニチャの詳細をアプリケーションのベンダーに連絡することを推奨します。サードパーティアプリケーションは、snort.orgでIPSシグニチャとの互換性をテストする必要があります。

現在、個々のアプリケーション/宛先をIPSスキャンから除外することはできません。

IPSシグニチャの無効化

サードパーティ製アプリケーションとの互換性の問題を引き起こすシグニチャが見つかった場合は、そのシグニチャを（一時的または永続的に）無効にすることができます。 これは、アプリケーションを信頼し、そのアプリケーションの価値が特定のシグニチャのセキュリティ上の利点を上回ると判断した場合にのみ実行する必要があります。

カスタムシグニチャリストの作成の詳細については、「カスタムシグニチャリストの追加」の手順を実行します。現在の設定をテンプレートとして使用し、目的のルールをLog OnlyまたはIgnoreに設定して無効にすることができます。

サポート

過去のイベント

Umbrellaサポートでは、過去のIPSイベントに関する詳細を提供できません。IPSイベントは、トラフィックがIPSシグニチャに一致しなかったことを通知します。シグニチャの詳細は、snort.orgで公開されています。Umbrellaは未加工のトラフィックやパケットのコピーを保存しないため、IPSイベントの性質に関する詳細なコンテキストや確認を提供できません。

IPSの問題/誤検出

現在の IPSの問題（誤検出など）について異議を唱える場合は、Umbrellaサポートに連絡してください。

これらの問題を調査するには、Umbrellaサポートによるパケットキャプチャが必要です。トラフィックがIPS検出をトリガーした方法を判別するには、パケットの未加工の内容が必要です。パケットキャプチャを生成するには、問題を再現できる必要があります。

チケットを発行する前に、Wiresharkなどのツールを使用して、問題の複製時にパケットキャプチャを生成します。 手順については、ナレッジベースを参照してください。

または、Umbrellaサポートがパケットキャプチャの生成をサポートします。影響を受けるユーザまたはアプリケーションの問題を再現できる時間をスケジュールする必要があります。

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。