各 Firepower 不正侵入 Base ポリシーのためのデフォルト Ruleset を判別するのに使用されるメトリックはである何

目次

概要

最新の脅威および脆弱性に対処する Cisco Talos リリース Snort ルール更新（SRU）。 新しい SRU リリースは各々の基礎ポリシーのための更新済 rulesets が含まれているかもしれません。 この資料はルールが Firepower デバイスに各不正侵入ベース ポリシーにどのように割り当てられるか決定するために Talos によって使用されるプロセスを説明したものです。

Talos はルール メタデータで定義されるポリシー インテントを基づかせています

基礎ポリシーは SRUs 内のメタデータ自身によって維持されます。 の状態はルール本文のメタデータ部分でデフォルトポリシーの何れかのルールを定義されます与えます。 次に、例を示します。

```
alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"MALWARE-CNC 1.php outbound connection
attempt"; sid:38753; gid:3; rev:1; classtype:trojan-activity; metadata:engine shared, soid
3|38753, policy balanced-ips drop, policy security-ips drop, impact_flag red; )
```

上に示されているルール例の表記はメタデータ セクション **ポリシー平衡型 IPS ドロップするが、ポリシー セキュリティ IPS ドロップする**含まれています。ありますこれは示しますこのルール 1:38753 は ***平衡型接続 ポリシー上のセキュリティおよび接続 ポリシー***、また ***セキュリティ***で廃棄する有効に なり、設定 されます。

デフォルトのルールセットを決定するために使用するメトリック

- 使用される主要なメトリックは、ルールの適用対象である各脆弱性に割り当てられる Common Vulnerability Scoring System（CVSS）スコアです。
- 2 番目のメトリックは、特定の脆弱性の経過期間に関連する時間ベースのメトリックです。

- 最後のメトリックは、ルールが適用される特定の領域です。 たとえば SQL インジェクション ルールは、ポリシーに組み込む対象として考慮する際に、影響が十分大きいため重要なルールであると見なされます。

  注: これらのカテゴリのルールの適用対象である脆弱性は、その経過期間に関係なく重要であると見なされます。

Connectivity over Security ベース ポリシー

注: 接続 ポリシーは特別にポリシーの緊急制御上のデバイスパフォーマンスを支持するように設計されています。 それは顧客が最小 false positive が付いているデバイスおよびほとんどのネットワーク配置のボックスの完全な評価されるパフォーマンスの 1 つを展開することを可能にする必要があります。 さらに、このポリシーはもっとも一般的なを検出する必要があり、顧客が経験するほとんどの流行する脅威。

1. CVSS スコアは 10 である必要があります。

2. 脆弱性は最後の 2 年からです (含んだ)。 次に、例を示します。

   - 今年 (2019 たとえば)
   - 昨年 (この例の 2018)
   - 最後 (この例の 2017) の前の年
3. ルール カテゴリ

   - このポリシーには使用されません

Balanced ベース ポリシー

注: 平衡型ポリシーは初期配置のために推奨されるデフォルトポリシーです。 このポリシーはシステムのセキュリティ必要および性能特性のバランスをとるように試みます。 顧客はこのポリシーから開始し、公共評価ツールとの非常に高いブロック比率、および比較的 評価およびテスト ツールとの高いパフォーマンス 比率を得られますはずです。 さらに、このポリシーは野生ネットワーキング状態で標準の下でデバイスの評価されるキャパシティの 80% で実行する必要があります。 平衡型ポリシーと常に留意するべき主な事柄はそれらに false positive との悪い工クスペリエンスがあればこれが顧客 開始点、限られた検出であるか、または貧弱なパフォーマンスはほとんどの顧客 インフラストラクチャの配備のためのその他のデバイスを調査することです。 それは Snort.org で販売されるオープンソース Snort のための Snort サブスクライバ ルール セットのデフォルト配布状態です。

1. CVSS スコアが 9 以上

2. 脆弱性は最後の 2 年からです (含んだ)。 次に、例を示します。

   - 今年 (2019 たとえば)
   - 昨年 (この例の 2018)
   - 最後 (この例の 2017) の前の年

3. ルール カテゴリ

- Malware-CnC
- Blacklist
- SQL インジェクション
- Exploit-kit

4. ルールが**接続** ポリシーにあれば

Security over Connectivity ベース ポリシー

> **注: セキュリティポリシーは**組織セキュリティについて特別に心配する客層の小さいセグメントのために設計されています。 顧客は保護されたネットワークのこのポリシーを展開します、それにより低い帯域幅の要求、ずっと高いセキュリティ要件があります。 さらに、顧客は false positive および騒々しいシグ二チャをより少なく気遣います。 アプリケーション制御はまたこのポリシーを展開している顧客へ、ネットワーク 使用状況の下でロックされて問題であり。 それは最大限の防御およびアプリケーション制御を提供する必要がありましたりネットワークをダウンさせるべきではありません。

1. CVSS スコアが 8 以上

2. 脆弱性は最後の 3 年からです（含んだ）。 次に、例を示します。

- 今年（2019 たとえば）
- 昨年（この例の 2018）
- 最後（この例の 2017）の前の年
- 前の年（この例の 2016）

3. ルール カテゴリ

- Malware-CnC
- Blacklist
- SQL インジェクション
- Exploit-kit

4. ルールが**平衡型**および**接続** ポリシーにあれば

最大値検出（最大検出） Base ポリシー:

> **注: 最大検出** ruleset はテスト環境で使用されるために意味され、パフォーマンスのためにそのように最適化されません。 このポリシーのルールの多数のための False positive は容認されますおよび/または期待されたおよび FP 調査は普通引き受けられません。

1. 内野テストにカバレッジが必要となります。

2. ルールが**セキュリティ**で、**バランスをとられる**、および**接続**ルール セット含まれています。

3. SID の上のすべてのアクティブなルールが含まれています: 10000、他に特に規定がなければ。

ポリシー更新頻度

すべての新しいルールはこれらの基準に基づいてポリシーに置かれます。 毎年ポリシーは再査定され、ポリシーを一時的な選択基準と対応保存するために脆弱性が老化するように、前年からのルールはポリシーから取除かれます。

もし CVSS スコアがルールによって力バーされる特定の脆弱性のために変更すれば、CVSS メトリックに基づいてポリシーの存在再査定されますです。

ポリシーは絶えず育ちます。 特定の目標にそれらを一直線に並べるためにバランスをとり直される主要から離れてポリシーからのルールの主要なド口ップはルールの数および製品のポリシーのパフォーマンスに満足する場合常に起こりません

> **注:** 基礎ポリシーは年次メジャーから離れてバランスをとり直します特定の目標にそれらを一直線に並べるために育つことができます。 ポリシーからのルールの主要なド口ップは Talos がルールの数および正常なネットワークの状態の下の製品のポリシーのパフォーマンスに満たされる場合常に起こりません。 リストされるポリシーのルールは、ルール単位で評価されます。 一部のルールは古く、デフォルト ポリシーに含めるための前述の基準に該当しないことがあります。 上記はデフォルト ルールの選択基準であり、脅威にまつわる状況に基づいて変更されることがあります。

> **注:** リストされるポリシーのルールは、ルール単位で評価されます。 一部のルールは古く、デフォルト ポリシーに含めるための前述の基準に該当しないことがあります。 上はデフォルトのルールのための選択基準で、脅威状況に基づいて変更に応じて常にあります