IPS 集約の設定例

目次

概要

この資料は Cisco 侵入防御システム（IPS）で集約の設定用に説明、長所および例を提供したものです。

前提条件

要件

次の項目に関する知識が推奨されます。

- Cisco 適応型セキュリティ アプライアンス（ASA）ソフトウェア（ASA） 5500 または 5500x Cisco 侵入防御システム（IPS）モジュール
- IPS 4200、4300、か 4500 シリーズ IPS アプライアンス
- NME-IPS モジュール
- IPS シグニチャ アラート

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- ASA 5500 または 5500x IPS モジュール
- IPS 4200、4300 または 4300 シリーズ IPS アプライアンス
- NME-IPS モジュール

本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。 稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

背景説明

IPS 集約は単一アラートに集約イベントにセンサーによって発信されるアラートの音量が減少させることができるように、モードを提供します。 各シグニチャは好まれる反映するデフォルトで、正常挙動作成されます。 ただし、各シグニチャにアラートがどのように処理される、従ってシグニチャのデフォルトの動作は各エンジンタイプのための制約の内で調整することができますか影響を及ぼす特別なパラメータがあります。

メタ エンジンがコンポーネント イベントを処理した後集約および検知時のアクションは処理されます。 これはセンサーが一連のイベント上の不審な行動のために視聴するようにします。

基本的な集約は 2 つのモードを提供します:

- **簡単なモード**-アラートが発信される前に会う必要があるシグニチャのためのヒットの閾値を設定します。
- **拡張モード**-アラートが発信される前に会う必要があるシグニチャのためのヒット毎秒（一定間隔数）の閾値を設定します。

集約オプション

- **適用すべて**-シグニチャが引き起こされるたびにアラートを始動させます。 しきい値が集約のために設定される場合、アラートは各実行のために集約が発生するまで起動 されます。 集約が開始した後、各サマリ間隔のための 1 アラートだけが各アドレス セットのために起動 します。 他のアドレス セットのためのアラートは完全に見られるか、または別々に要約されます。 シグニチャは適用**すべての**モードに後そのシグニチャのアラートの期間戻しませんでした。
- **要約**-シグニチャが引き起こされる時最初にアラートを始動させます。 そのシグニチャのための追加アラートはサマリ間隔時間の間要約されます。 各サマリ間隔が各アドレス セットで起動 する必要がある 1 アラートだけ。 グローバル なサマリしきい値が達する場合、シグニチャはグローバル**集約**モードに入ります。
- **グローバル集約**-各サマリ間隔のためのアラートを始動させます。 シグニチャはグローバル**集約**のために前もって構成することができます。
- **適用**-各アドレス セットのためのアラートを始動させます。 このモードはグローバル**集約**モ

ードにアップグレードすることができます。

イベント集約

一般的なシナリオはハイパー警告シグニチャを識別するために調整するベースラインの期間を経ることです。 頻繁にトラフィック ミックスに基づいて集約を必要とするいくつかの低レベルおよび情報レベル シグニチャがあります。 適切なしきい値を判別するためにこれらのシグニチャを検討して下さい。

> **注:** アラートの量を減らす時はいつでも、高い重大度シグニチャからの特にアラート注意して下さい。 セキュリティが危殆化されないこと、そして適切な操作が要約されるあらゆるシグニチャのためにきちんと整っていることを確認して下さい。

設定

> **注:** このセクションで使用されているコマンドの詳細を調べるには、Command Lookup Tool（登録ユーザ専用）を使用してください。

SSH Brute Force Attack -シグニチャ 3653

急速なセキュア シェル（SSH）セッションは、アクティブに警告 するとき、すぐにイベント ストアを一杯にできます。 現在、SSH Brute Force 試みは否定されています。

5 分毎にアラートだけを必要とする場合、300 秒の要約間隔とアラート周波数のために**サマリ** オプションを使用して下さい:

```
sensor# configure terminal
sensor(config)# service signature-definition sig0
sensor(config-sig)# signatures 3653 0
sensor(config-sig-sig)# alert-frequency
sensor(config-sig-sig-ale)# summary-mode summarize
sensor(config-sig-sig-ale-sum)# summary-interval 300
sensor(config-sig-sig-ale-fir-yes)# exit
sensor(config-sig-sig-ale-sum)# show settings
alert-frequency
-----------------------------------------------
summary-mode
-----------------------------------------------
summarize
-----------------------------------------------
summary-interval: 300 default: 15
summary-key: Axxx <defaulted>
specify-global-summary-threshold
-----------------------------------------------
yes
-----------------------------------------------
global-summary-threshold: 240 <defaulted>
-----------------------------------------------
-----------------------------------------------
-----------------------------------------------
```

```
sensor(config-sig-sig-ale-fir)# exit
sensor(config-sig-sig-ale)# exit
sensor(config-sig-sig)# exit
sensor(config-sig)# exit
Apply Changes:?[yes]:
```

HTTP 要求の余分な SQL クエリー-シグニチャ 5474

HTTP 要求で組み込まれる SQL クエリー選り抜きから工ッジ配置のもっとも一般的なハイパー警告シグニチャの 1 つはです。

3600 秒の要約間隔のアラート周波数のためのオプション適用攻撃者/対象ペアのためのシグニチャ 5474 を一時間毎に表示するために、使用します:

```
sensor# configure terminal
sensor(config)# service signature-definition sig0
sensor(config-sig)# signatures 5474 0
sensor(config-sig-sig)# alert-frequency
sensor(config-sig-sig-ale)# summary-mode fire-once
sensor(config-sig-sig-ale-fir)# specify-global-summary-threshold yes
sensor(config-sig-sig-ale-fir-yes)# global-summary-threshold 3600
sensor(config-sig-sig-ale-fir-yes)# summary-interval 3600
sensor(config-sig-sig-ale-fir-yes)# exit
sensor(config-sig-sig-ale-fir)# show settings
fire-once
-----------------------------------------------
summary-key: Axxx default: Axxx
specify-global-summary-threshold
-----------------------------------------------
yes
-----------------------------------------------
global-summary-threshold: 3600 default: 240
summary-interval: 3600 default: 15
-----------------------------------------------
-----------------------------------------------
-----------------------------------------------
sensor(config-sig-sig-ale-fir)# exit
sensor(config-sig-sig-ale)# exit
sensor(config-sig-sig)# exit
sensor(config-sig)# exit
Apply Changes:?[yes]:
```

AD 内部か外部 TCP/UDP スキャナー-シグニチャ 13000 に 13008

この例では、内部か外部ゾーンで設定される宛先 IP アドレスのセットをスキャンする Transport Control Protocol（TCP）/User Datagram Protocol（UDP; ユーザ データグラム プロトコル）スキャナーを検出する場合のシグニチャ適用。 IPS Manager Express（IME）送信がディフォルトする場合、電子メール通知として高い重大度イベントは、そこにメールの桁であるかもしれません。

> **注:** 適用が false positive 不正侵入ではないことを確かめて下さい。 異常検出の設定を「学びましたり 48 時間におけるモード」を、そして移動しますに戻って問題を解決するために「検出しますモード」を変更して下さい。

メールの数を減らすために、720 秒または一度 12 分毎にの要約間隔とアラート周波数のために

適用オプション、使用して下さい。

```
sensor# configure terminal
sensor(config)# service signature-definition sig0
sensor(config-sig)# signatures 13000 0
sensor(config-sig-sig)# alert-frequency
sensor(config-sig-sig-ale)# summary-mode fire-once
sensor(config-sig-sig-ale-fir)# specify-global-summary-threshold yes
sensor(config-sig-sig-ale-fir-yes)# global-summary-threshold 720
sensor(config-sig-sig-ale-fir-yes)# summary-interval 720
sensor(config-sig-sig-ale-fir-yes)# exit
sensor(config-sig-sig-ale-fir-yes)# show settings
  fire-once
  ----------------------------------------------
     summary-key: Axxx <defaulted>
     specify-global-summary-threshold
     ----------------------------------------------
        yes
        ----------------------------------------------
           global-summary-threshold: 720 default: 240
           summary-interval: 720 default: 15
        ----------------------------------------------
     ----------------------------------------------
  ----------------------------------------------
sensor(config-sig-sig-ale-fir)# exit
sensor(config-sig-sig-ale)# exit
sensor(config-sig-sig)# exit
sensor(config-sig)# exit
Apply Changes:?[yes]:
```

確認

現在、この設定に使用できる確認手順はありません。

トラブルシューティング

現在のところ、この設定に関する特定のトラブルシューティング情報はありません。

関連情報

- アラート周波数の設定
- IPS 設定ガイド
- テクニカル サポートとドキュメント – Cisco Systems