IPS汇总配置示例

Contents

Introduction

本文为汇总的配置提供解释、优点和示例在思科入侵防御系统(IPS)。

Prerequisites

Requirements

Cisco 建议您了解以下主题：

- Cisco可适应的安全工具(ASA) 5500或5500x思科入侵防御系统(IPS)模块
- IPS 4200， 4300或者4500系列IPS工具
- NME-IPS模块
- IPS签名戒备

Components Used

本文档中的信息基于以下软件和硬件版本：

- ASA 5500或5500x IPS模块
- IPS 4200， 4300或4500系列IPS工具
- NME-IPS模块

The information in this document was created from the devices in a specific lab environment.All of the devices used in this document started with a cleared (default) configuration.If your network is live, make sure that you understand the potential impact of any command.

Conventions

有关文档规则的信息，请参阅 Cisco 技术提示规则。

背景信息

IPS汇总提供模式聚集事件到单个戒备，因此传感器发送的戒备的容量可以被减少。每个签名用反射一种首选的默认值创建，正常行为。然而，每个签名有影响的特殊参数戒备如何被处理，因此签名默认行为可以在每种引擎类型的约束内被调整。

在阶引擎处理了组分事件后，汇总和事件动作被处理。这让传感器注意在一系列的事件的可疑活动。

基本的聚合提供两个模式：

- **简单的模式**-配置命中阈值数字必须满足的签名的，在发送前戒备。
- **Advanced模式**-配置命中阈值数字每秒(计时的间隔计数)必须满足的签名的，在发送前戒备。

汇总选项

- **火所有**-，每次签名被触发，射击戒备。如果阈值为汇总设置，戒备为每执行被射击，直到汇总发生。在汇总开始后，只有每个汇总间隔火的一次戒备每地址集的。其他地址集的戒备所有被看到或分开被总结。签名恢复对火**所有**模式在一个周期之后没有戒备该签名的。
- **汇总**-，第一次签名被触发，射击戒备。该签名的另外的戒备为持续时间概略的间隔被总结。仅每个概略的间隔应该为每地址集射击的一次戒备。如果全局概略的阈值达到，签名进入全局**汇总**模式。
- **全局汇总**-射击每个概略的间隔的一次戒备。签名可以为全局**汇总**预先配置。
- **火一且**-射击每地址集的一次戒备。此模式可以被升级到全局**汇总**模式。

事件汇总

常见情况是经过调整基准的周期为了识别亢奋警告的签名。经常有需要根据数据流混合的汇总的一定数量的低级和与信息有关级的签名。查看这些签名为了确定适当的阈值。

> **Note**:小心，每当您减少相当数量戒备，从严重级别签名的特别是戒备。保证安全没有被危及，并且适当的动作为被总结的所有签名是到位。

配置

Note:使用命令查找工具（仅限注册用户）可获取有关本部分所使用命令的详细信息。

SSH暴力攻击-签名3653

迅速安全壳SSH会话，当积极地警告，能迅速填装事件存储。目前， SSH暴力尝试被拒绝。

如果只需要戒备每五分钟，请使用**概略的**选项提醒频率与汇总间隔300秒：

```
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]:
```

在HTTP请求的额外的SQL查询-签名5474

精选从在HTTP请求嵌入的SQL查询是其中一个在边缘配置的最普通的亢奋警告的签名。

为了每小时查看一个攻击者/受害者对的签名5474，使用，火**一旦提醒**频率的选项与汇总间隔3600秒：

```
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内部或外部TCP/UDP扫描程序-签名13000到13008

在本例中，签名火，当发现a扫描套作为区域被配置的目的地IP地址内部或外部的传输控制协议/用户数据报协议(UDP)扫描程序。如果IPS管理器Express (IME)发送默认值，高严重级别的事件作为电子邮件通知，那里也许在千位电子邮件。

> **Note**:确定火不是一次假善意告警攻击。更改异常情况检测的设置到“Learn模式” 48小时，然后移动它回到“发现模式”为了解决问题。

为了减少电子邮件的数量，请使用，火**一旦**选项提醒频率，与汇总间隔720秒或一次每12分钟。

```
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]:
```

Verify

当前没有可用于此配置的验证过程。

Troubleshoot

目前没有针对此配置的故障排除信息。

Related Information

- 配置提醒的频率
- IPS配置指南
- Technical Support & Documentation - Cisco Systems