Exemplos da configuração de sumarização IPS

Índice

Introdução

Este documento fornece explicações, vantagens, e exemplos para a configuração da sumarização no Sistema de prevenção de intrusões da Cisco (IPS).

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Ferramenta de segurança adaptável de Cisco (ASA) 5500 ou módulos do Sistema de prevenção de intrusões da Cisco 5500x (IPS)
- IPS 4200, 4300, ou dispositivos IPS do 4500 Series
- Módulo NME-IPS
- Alertas da assinatura IPS

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Módulos ips ASA 5500 ou 5500x
- IPS 4200, dispositivos IPS do 4300 ou 4500 Series
- Módulo NME-IPS

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Convenções

Consulte as Convenções de Dicas Técnicas da Cisco para obter informações sobre convenções de documentos.

Informações de Apoio

A sumarização IPS fornece modos para agregar eventos em um único alerta, de modo que o volume de alertas enviados pelo sensor possa ser diminuído. Cada assinatura é criada com os padrões que refletem preferida, comportamento normal. Contudo, cada assinatura tem os parâmetros especiais que influenciam como os alertas são segurados, assim que o comportamento padrão das assinaturas pode ser ajustado dentro das limitações para cada tipo de Engine.

As ações da sumarização e do evento são processadas depois que o motor do meta processou os eventos componentes. Isto deixa o sensor olhar para a atividade suspeita sobre uma série de eventos.

A agregação básica fornece dois modos:

- **Modo simples** - configura um número de limiar de batidas para uma assinatura que deva ser encontrada antes que o alerta esteja enviado.
- **Modo avançado** - configura um número de limiar de batidas por segundo (contagem do intervalo programado) para uma assinatura que deva ser encontrada antes que o alerta esteja enviado.

Opções da sumarização

- **fogo-todo** - Ateia fogo a um alerta cada vez que a assinatura é provocada. Se o ponto inicial é ajustado para a sumarização, os alertas estão ateados fogo para cada execução até que a sumarização ocorra. Depois que a sumarização começa, simplesmente um alerta para fogos de cada intervalo do sumário para cada grupo do endereço. Os alertas para outros grupos do endereço são considerados toda ou resumidos separadamente. A assinatura reverte a fogo-**todo** modo após um período de nenhuns alertas para essa assinatura.
- **sumário** - Ateia fogo a um alerta a primeira vez que uma assinatura é provocada. Os alertas adicionais para essa assinatura são resumidos para a duração do intervalo sumário. Somente um alerta que cada intervalo sumário deve atear fogo para cada grupo do endereço. Se o

ponto inicial sumário global é alcançado, a assinatura entra no modo da global-**sumarização**.
- **global-sumarização** - Ateia fogo a um alerta para cada intervalo sumário. As assinaturas podem ser preconfigured para a global-**sumarização**.
- **fogo-uma vez que** - Ateia fogo a um alerta para cada grupo do endereço. Este modo pode ser promovido ao modo da global-**sumarização**.

Sumarização do evento

Um cenário comum é submeter-se a um período de linha de base que ajusta a fim identificar assinaturas de alerta hyper. Há frequentemente um número de assinaturas de baixo nível e do nível informacional que precisam a sumarização baseada na mistura do tráfego. Reveja estas assinaturas a fim determinar os pontos iniciais apropriados.

> **Note**: Seja cuidadoso sempre que você reduz a quantidade de alertas, especialmente alertas das assinaturas da severidade elevada. Assegure-se de que a Segurança não esteja comprometida e que as ações apropriadas são no lugar para toda a assinatura que for resumida.

Configuração

> **Note**: Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados nesta seção.

Ataque de força bruta SSH - Assinatura 3653

As sessões rápidas do Shell Seguro (ssh), ao ativamente alertar, podem rapidamente encher a loja do evento. Atualmente, as tentativas da força bruta SSH estão sendo negadas.

Se você precisa somente alertas cada cinco minutos, use a opção **sumária** para a alerta-frequência com um sumário-intervalo de 300 segundos:

```
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]:
```

Pergunta excessiva SQL nos pedidos do HTTP - Assinatura 5474

Seleto-da pergunta SQL encaixada em um pedido do HTTP é uma das assinaturas de alerta hyper as mais comuns em um desenvolvimento da borda.

A fim ver de hora em hora a assinatura 5474 para um par do atacante/vítima, use fogo-**uma vez que** opção para a alerta-frequência com um sumário-intervalo de 3600 segundos:

```
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]:
```

Varredor interno ou externo AD TCP/UDP - Assinaturas 13000 13008

Neste exemplo, os fogos da assinatura quando detectar um varredor do protocolo de controle (TCP)/User Datagram Protocol (UDP) do transporte que faça a varredura do grupo de endereços IP de destino configurados como a zona interna ou externo. Se o gerente IPS expresso (IME) envia o padrão, os eventos da severidade elevada como notificações de Email, lá puderam ser milhares de email.

Note: Certifique-se que os fogos não são um ataque do falso positivo. Mude o ajuste para

que a detecção de anomalia “aprendem o modo” por 48 horas, a seguir movem-no de volta a “detectam o modo” a fim resolver a edição.

A fim reduzir o número de email, use fogo-**uma vez que** opção para a alerta-frequência, com um sumário-intervalo de 720 segundos ou uma vez de cada 12 minutos.

```
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]:
```

Verificar

No momento, não há procedimento de verificação disponível para esta configuração.

Troubleshooting

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.

Informações Relacionadas

- Configurando a frequência alerta
- Manuais de configuração IPS
- Suporte Técnico e Documentação - Cisco Systems