A ação do evento cancela o Troubleshooting

Introdução

Este documento descreve os possíveis problemas causados pela ação do evento cancela no Sistema de prevenção de intrusões da Cisco (IPS) e oferece recomendações ajustar e pesquisar defeitos sua instalação.

> Nota: A ação do evento cancela é ações globais tomadas nas assinaturas baseadas em uma avaliação de risco. Como com toda a configuração global, tome grande com alterações de configuração e adições.

Problemas da ultrapassagem da ação do evento

Descrição

A ação do evento cancela adiciona ações adicionais a um evento da assinatura quando esse evento cai dentro de uma escala especificada da avaliação de risco. A ação do evento do uso cancela com cuidado. Iif você cria uma ultrapassagem com uma escala larga da avaliação de risco para um evento que seja provocado frequentemente (ações especialmente específicas, caras, tais como ações de registro IP), você pôde causar problemas.

Impacto

Excessivo escreve à loja do evento são associados tipicamente com a utilização elevada da CPU e o unresponsiveness geral do sensor às ferramentas do acesso de gerenciamento tais como o comando line interface(cli) e o Cisco IPS Device Manager (IDM).

Ações de registro e descritores de arquivo IP

Um descritor de arquivo é uma estrutura de dados usada por um programa a fim obter um punho em um arquivo; os descritores conhecidos são 0,1,2 para o padrão dentro, o padrão para fora, e o erro padrão. Um descritor de arquivo é criado quando um processo abre um arquivo novo ou um soquete.

Se você cria uma ultrapassagem da ação do evento para uma ação de registro IP tal como log-atacante-pacotes, log-par-pacotes, ou log-vítima-pacotes, este pôde esgotar o pool dos descritores de arquivo; o desempenho total do sensor pôde ser negativamente afetado e o sensor não pode funcionar corretamente.

As ações da armadilha de SNMP e a ação do evento cancelam

Uma assinatura que tenha somente a única ação da pedido-SNMP-armadilha igualmente gerencie um evento alerta que seja escrito à loja do evento. Assim, o despedimento excessivo da ação da armadilha de Protocolo de Gerenciamento de Rede Simples (SNMP) pôde igualmente provocar os mesmos problemas considerados com ações excessivas do alerta do produto.

Ações para assinaturas do motor do normalizador

Não adicionar nenhuma ação que causar a loja do evento escreve (como o alerta, a pedido-SNMP-armadilha, ou as log-ações do produto) às assinaturas do normalizador. Isto aplica-se a todas as assinatura ID da escala 1200-1330.

Àexceção dos breves scenarios de Troubleshooting, você não deve usar a ação do evento cancela para as assinaturas do motor do normalizador. Isto pode ser particularmente problemático em:

- cenários de IP altamente fragmentados (devido às assinaturas 1200-range)
- (ooo) encenações pesadamente foras de serviço TCP (assinaturas 1300-range)

Por exemplo, uma ultrapassagem da ação do evento que cause uma escrita à loja do evento para cada pacote de TCP do ooo pode causar edições do recurso e da utilização.

A ação do evento cancela com avaliação de risco de 0-100

Geralmente, evite a ação do evento cancela com uma avaliação de risco de 0-100 porque a baixa avaliação pode pôr seu sensor em risco da falha em determinadas circunstâncias.

Do meta das assinaturas fogo componente frequentemente para (e terra comum) tipos de tráfego convenientemente benignos. As assinaturas do meta procuram uma combinação de umas ou várias assinaturas componentes do meta para provocar antes do pai a assinatura do meta que ateia fogo a um alerta. As assinaturas componentes do meta, à revelia, não têm nenhuma ação associada com ela; isto é intencional porque combinam frequentemente no tráfego comum. As assinaturas componentes do meta têm uma avaliação de risco da base do padrão de 15. A fim excluir a captação destes fósforos da assinatura em uma ultrapassagem da ação do evento, Cisco recomenda que você não usa uma avaliação de risco mais baixo de 25 quando você cria uma ultrapassagem da ação do evento; isto é, a avaliação de risco não deve estar abaixo de 25-100.

Verifique a utilização IPS

Comandos

> Nota: Use a ferramenta de consulta de comandos (clientes registrados somente) a fim obter mais informação nos comandos usados nesta seção

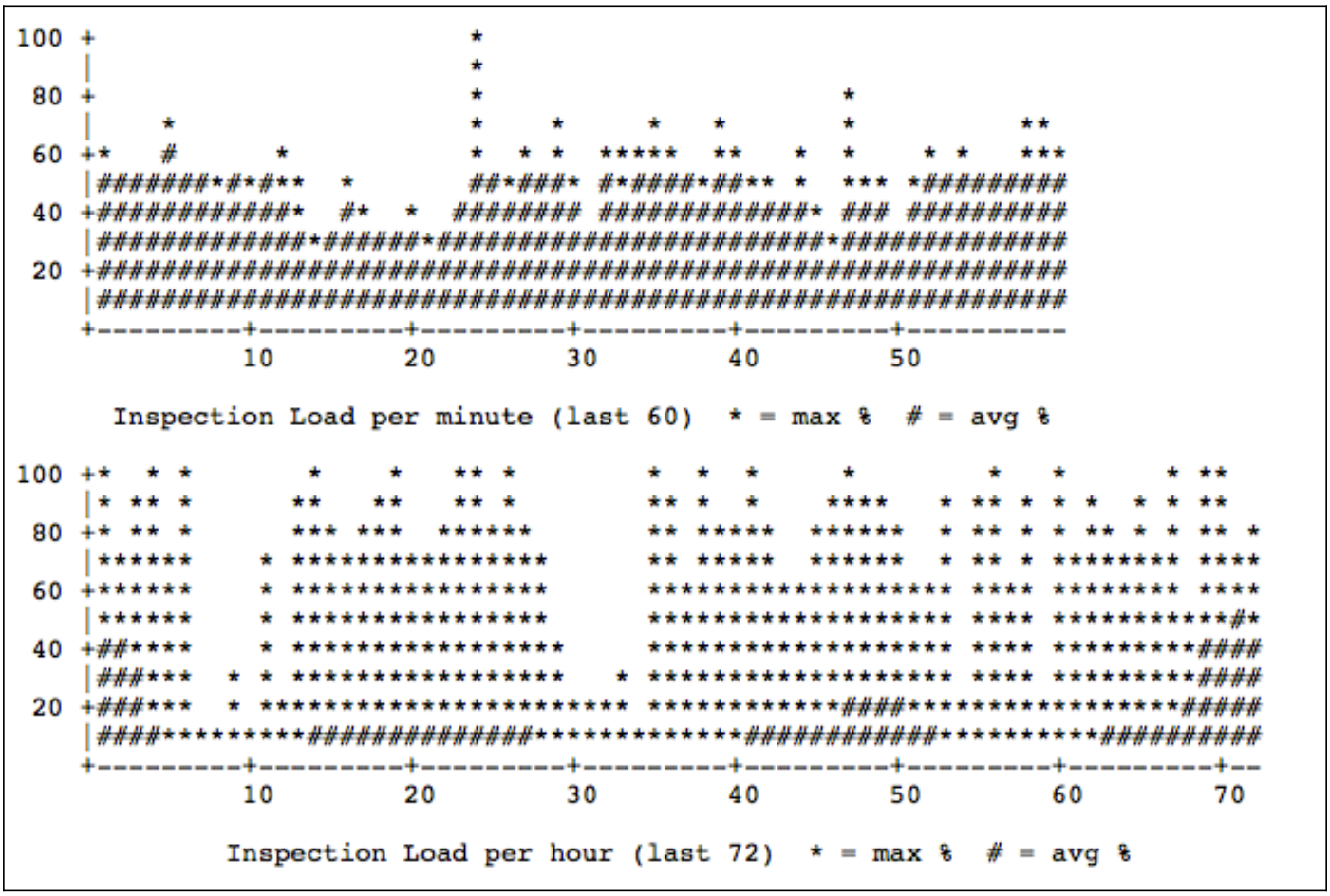
Incorpore o comando do virtual-**sensor das estatísticas da mostra no** CLI a fim procurar a porcentagem da carga da inspeção:

```
sensor# show statistics virtual-sensor | inc Load
Processing Load Percentage = 100
```

Em versões 7.0(8)E4 e 7.1(6)E4 IPS, o comando da inspeção-**carga da mostra** foi adicionado:

```
sensor#  show inspection-load history
sensor 10:17:57 UTC Mon Apr 05 2013
```

Esta é saídas de exemplo desse comando:



Muito uma porcentagem da carga elevada (90% ou mais alto) pôde indicar que há uns eventos excessivos provocados pela ação do evento cancela. Refira entra a ordem para confirmar mais esta possibilidade.

Logs

O indicador principal da ação excessiva do evento cancela é loja rápida do evento que envolve, como visto neste arquivo de main.log do exemplo:

```
25Jan2010 05:13:08.326 19.897 sensorApp[18316] IdsEventStore/W errWarning -
the event store wrapped around [IdsEventStore::writeEvent(), index = 19530]
25Jan2010 05:32:05.751 85.031 sensorApp[18316] IdsEventStore/W errWarning -
the event store wrapped around [IdsEventStore::writeEvent(), index = 19529]
25Jan2010 05:50:45.442 4.989 sensorApp[18316] IdsEventStore/W errWarning -
the event store wrapped around [IdsEventStore::writeEvent(), index = 19530]
25Jan2010 06:08:59.281 70.143 sensorApp[18316] IdsEventStore/W errWarning -
the event store wrapped around [IdsEventStore::writeEvent(), index = 19529]
25Jan2010 06:25:40.923 34.562 sensorApp[18316] IdsEventStore/W errWarning -
the event store wrapped around [IdsEventStore::writeEvent(), index = 19531]
```

Geralmente, o envolvimento da loja do evento que ocorre mais frequentemente de uma vez uma hora pode indicar um problema. Em algumas encenações, o envolvimento é tão excessivo que

pode ocorrer muitas vezes dentro de um minuto. Há muitas variáveis, tais como a capacidade de desempenho geral da plataforma, de considerar.

Troubleshooting

Determine que tipo de evento, de tráfego, ou de ação está causando o problema da ultrapassagem da ação do evento. É um alerta do produto, registro IP, assinatura do normalizador, ou de componente do meta assinatura?

- Se é uma assinatura “tagarela” e você determina a assinatura cria falsos positivos para eventos, escreva um filtro da ação do evento (CES).
- Para o IP que registra, Cisco recomenda-o evita EAFs ou usa EAFs com cuidado e com uma compreensão completa dos riscos.
- As assinaturas do normalizador e as assinaturas componentes do meta não devem ter uma ação alerta à exceção dos scenarios de Troubleshooting provisórios.

Informações Relacionadas

- Configurar a ação do evento cancela
- Manuais de configuração IPS
- Suporte Técnico e Documentação - Cisco Systems