AMP para o console dos valores-limite e o último filtro visto

Índice

Introdução

Este documento descreve a explicação do “último” erro considerado do filtro provido a CSCvh31177 na proteção avançada do malware (AMP) para valores-limite.

Contribuído por Caly Hess, engenheiro da Cisco.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Acesso a Cisco AMP para o painel dos valores-limite

Componentes Utilizados

A informação neste documento é baseada no software do thede:

- Cisco AMP para valores-limite para valores-limite consola a versão 5.4.20190917

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 rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Problema

O filtro para “último visto” da página dos computadores no console, conectores dos indicadores que foram vistos nas últimas 24 horas que aparece na lista.

Causa

A tração atual de “últimos” dados considerados é um trabalho singular cada 24 horas. Embora os dados que são refletidos na página dos computadores e na saída para a exportação ao CSV para “último considerado” são tempo real, o filtro próprio foge os dados batched desse trabalho singular. Isto foi executado para aumentar a velocidade dos

resultados, porque a análise em tempo real dos timestamps para grandes ambientes de empreendimento poderia conduzir aos intervalos e ao fechamento do base de dados.

Explicação de computadores “recentemente vistos” em um filtro do dia 7+

A máquina era autônoma pelos dias 7+ até depois o “último” trabalho considerado foi executado.

Exemplo do mundo real

- HostA.randomdomain.net teve um acidente infeliz com uma caneca de café completa e o cartão-matriz não fez um 10o completo da recuperação em agosto
- HostA.randomdomain.net está sentando-se agora no depósito do reparo até o 20 de setembro
- O 21 de setembro, os retornos de HostA.randomdomain.net à rede 4 horas depois que o “último” trabalho considerado foi executado mas 2 horas antes que o auditor fazem uma exportação ao CSV dos computadores não considerados para os últimos 30 dias
- HostA.randomdomain.net é alistado ainda do “último” trabalho visto como realizando-se sobre 30 dias não vistos. Apesar dele é agora inteiramente - funcional e café livres, o auditor trava-o agora em sua exportação “inativa”

Solução a curto prazo

O trabalho próprio não toma umas 24 horas completas para ser executado, mas pode tomar pelo menos 12. A fim aumentar a precisão do filtro, a reprogramação automática para o trabalho depois que precedente termina é em desenvolvimento, que é esperado cortar em qualquer lugar de 7-12 horas do tempo fora do indicador do grupo.

Solução a longo prazo

Um rework total do “último” mecanismo visto que se realiza mais perto do tempo real em que os dados são puxados. Esta solução exige a aplicação de uma estrutura do base de dados inteiramente nova que esteja atualmente durante o processo de desenvolvimento com a liberação proposta no próximo ano de calendário.