Trabalhando com detecções falsas, manifestações, e resposta ao incidente avançadas da proteção do malware (AMP)

Índice

Introdução

Nós esforçamo-nos sempre para melhorar e expandir a inteligência de ameaça para nossa tecnologia avançada da proteção do malware (AMP), contudo se sua solução AMP não provocou um alerta nem provocou um alerta erroneamente, você pode tomar algumas ações para impedir todo o impacto mais adicional a seu ambiente. Este documento fornece uma diretriz naqueles itens de ação.

Descrição

Ações imediatas

Se você acredita que sua solução AMP não protegeu sua rede de uma ameaça, tome as seguintes ações imediatamente:

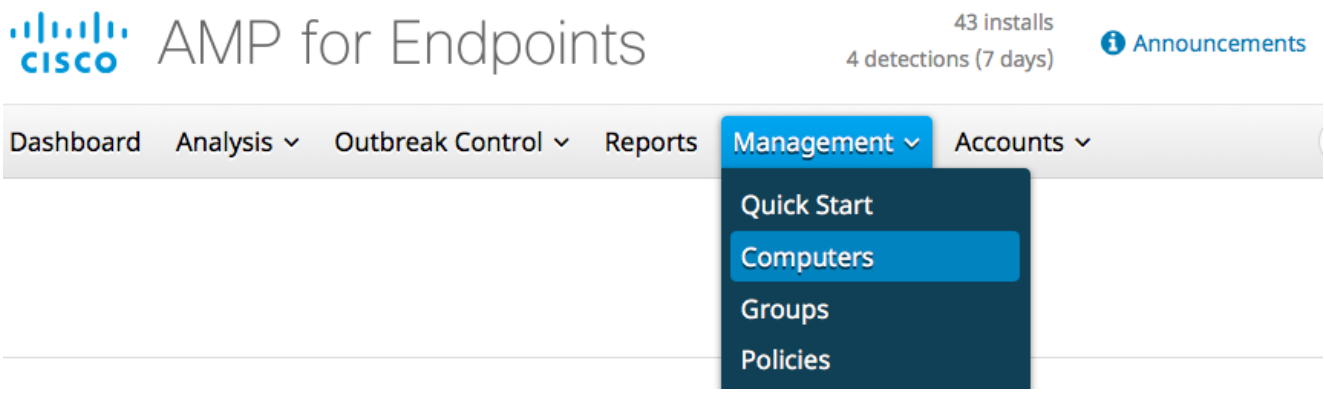
1. Isole as máquinas suspeitos do resto da rede. Isto podia incluir desligar a máquina, ou o desligamento dela da rede fisicamente.
2. Redija para baixo a informação importante sobre a infecção, como, o tempo quando a máquina pôde ser contaminada, as atividades do usuário nas máquinas suspeitos, etc.

aviso: Não limpe para fora ou nova imagem a máquina. Elimina as possibilidades de encontrar o software ou os arquivos de ofensa durante a investigação ou o processo de Troubleshooting judicial.

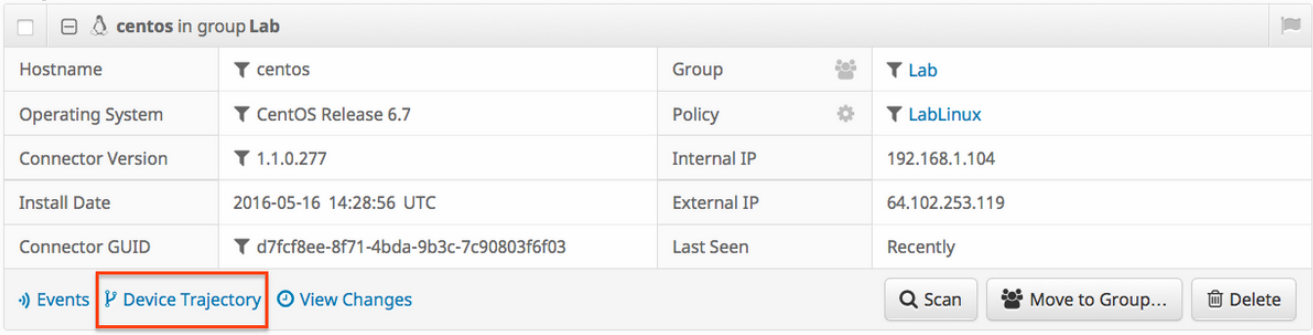
Análise

1. Use a característica da **trajetória do dispositivo** para começar sua própria investigação. A trajetória do dispositivo é capaz de armazenar aproximadamente o 9 milhão a maioria de eventos do arquivo recente. O AMP para a trajetória do dispositivo dos valores-limite é muito útil para seguir para baixo arquivos ou processos que isso conduziu a uma infecção.

No painel, navegue ao **Gerenciamento > aos computadores**.



Encontre a máquina suspeito e expanda o registro para essa máquina. Clique sobre a opção da **trajetória do dispositivo**.



2. Se você encontra alguma arquivo ou mistura suspeito, adicionar-la a suas lista feitas sob encomenda da detecção. O AMP para valores-limite pode usar uma lista feita sob encomenda da detecção para tratar um arquivo ou uma mistura como maliciosa. Esta é uma grande maneira de fornecer a cobertura transitória para impedir um impacto mais adicional.

Análise por Cisco

1. Submeta todas as amostras suspeitos para a análise dinâmica. Você pode manualmente submetê-los da **análise > da análise do arquivo no** painel. O AMP para valores-limite inclui a funcionalidade da análise dinâmica que gerencie um relatório do comportamento do arquivo da grade da ameaça. Isto igualmente tem o benefício de fornecer o arquivo a Cisco caso a análise adicional por nossa equipe de investigação for exigida.

2. Se você suspeita quaisquer detecções do *falso positivo* ou do *falso negativo em* sua rede, nós recomendamos que você leverage a funcionalidade preta feita sob encomenda da lista ou da lista do branco para seu Produtos AMP. Quando você contactar o centro de assistência técnica da Cisco (TAC), forneça a informação seguinte para a análise:A mistura SHA256 do arquivo.Uma cópia do arquivo se possível.Informação sobre o arquivo tal como de onde veio e de porque precisa de estar no ambiente.Explique porque você acredita este para ser um falso positivo ou um falso negativo.
3. Se você precisa o auxílio que abranda uma ameaça ou que executa a triagem de seu ambiente, você precisará de contratar a equipe dos serviços da resposta ao incidente do Cisco Security (CSIRS) que se especializa em criar planos de ação, em pesquisar máquinas infectadas, e em leveraging ferramentas ou características avançadas para abrandar uma manifestação ativa.

Note: O centro de assistência técnica da Cisco (TAC) não fornece o auxílio este tipo de acoplamento.A equipe CSIRS pode ser enagaged chamando este número de telefone: +1-844-831-7715. Este é um serviço pago que começa em $60,000 a menos que sua organização tiver um retentor para serviços da resposta ao incidente de Cisco. Uma vez que contratado fornecerão a informação adicional sobre seus serviços e abrirão um argumento para seu incidente. Nós igualmente recomendamos continuar com seu Cisco Account Manager de modo que possam fornecer a orientação adicional no processo.

Artigos relacionados

- Coleção de dados de diagnóstico de um conector de FireAMP que é executado em Windows
- Tipos de arquivo que são feitos a varredura pelo conector de FireAMP