

Identificar Mecanismo de Detecção no Console de Ponto de Extremidade Seguro

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Problema](#)

[Solução](#)

Introdução

Este documento descreve como identificar o mecanismo responsável por uma detecção específica no console do Secure Endpoint.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Console Cisco Secure Endpoint

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software:

- Secure Endpoint Console v5.4.2025030619

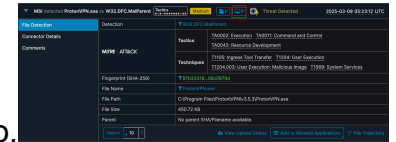
As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer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

Problema

Identificar o mecanismo correto responsável por uma detecção específica é uma das etapas iniciais para entender a natureza do evento e triá-lo efetivamente.

Solução

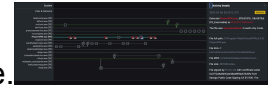
1. Navegue até a página Eventos no console do AMP para localizar o evento que deseja investigar mais.



2. Clique no ícone em destaque para abrir a Trajetória do dispositivo.

Ícone de trajetória do dispositivo

3. Você pode exibir os detalhes do evento à direita em Detalhes da atividade.

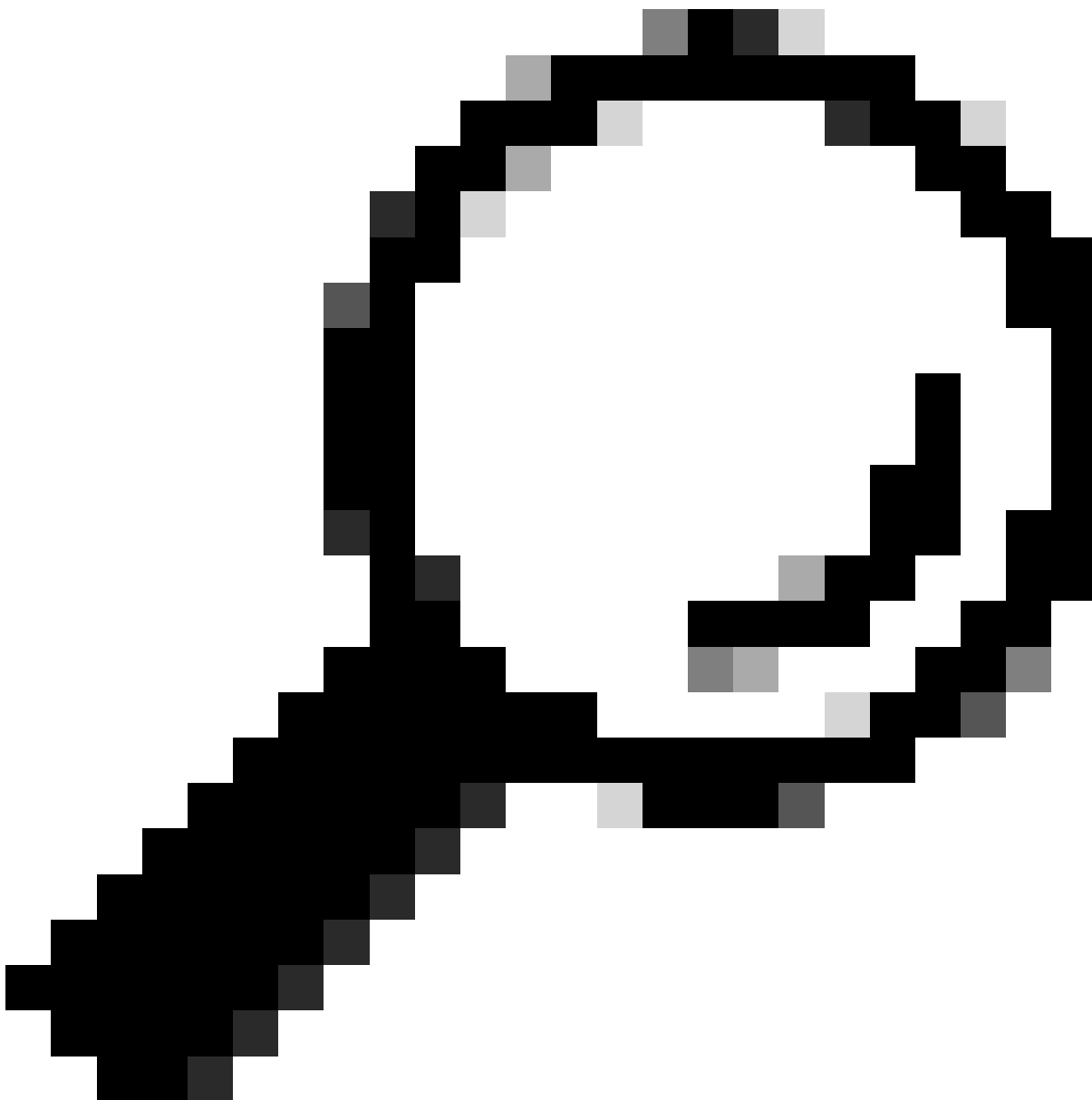


Detalhes do evento na trajetória do dispositivo

4. Role até a parte inferior para localizar a seção Detectado por.



Detectado pela Seção



Tip: Compreender essas informações é essencial para avaliar a natureza da ameaça e determinar rapidamente a exclusão apropriada a ser configurada. Além disso, fornecer esses detalhes ao enviar um caso ao TAC para investigações de falsos positivos pode ajudar a acelerar o processo.

Se você não conseguir visualizar a seção Detectado por ou para obter mais ajuda, entre em contato com o TAC.

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.