Identificación del motor de detección en Secure Endpoint Console

Contenido

Introducción

Este documento describe cómo identificar el motor responsable de una detección específica en la consola de Secure Endpoint.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- consola de Cisco Secure Endpoint

Componentes Utilizados

La información que contiene este documento se basa en estas versiones de software:

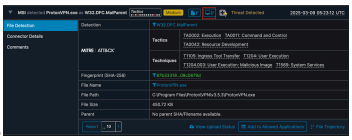
- Secure Endpoint Console v5.4.2025030619

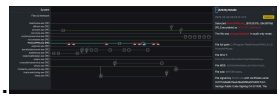
La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

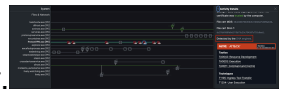
Problema

Identificar el motor correcto responsable de una detección específica es uno de los pasos iniciales para comprender la naturaleza del evento y probarlo de forma eficaz.

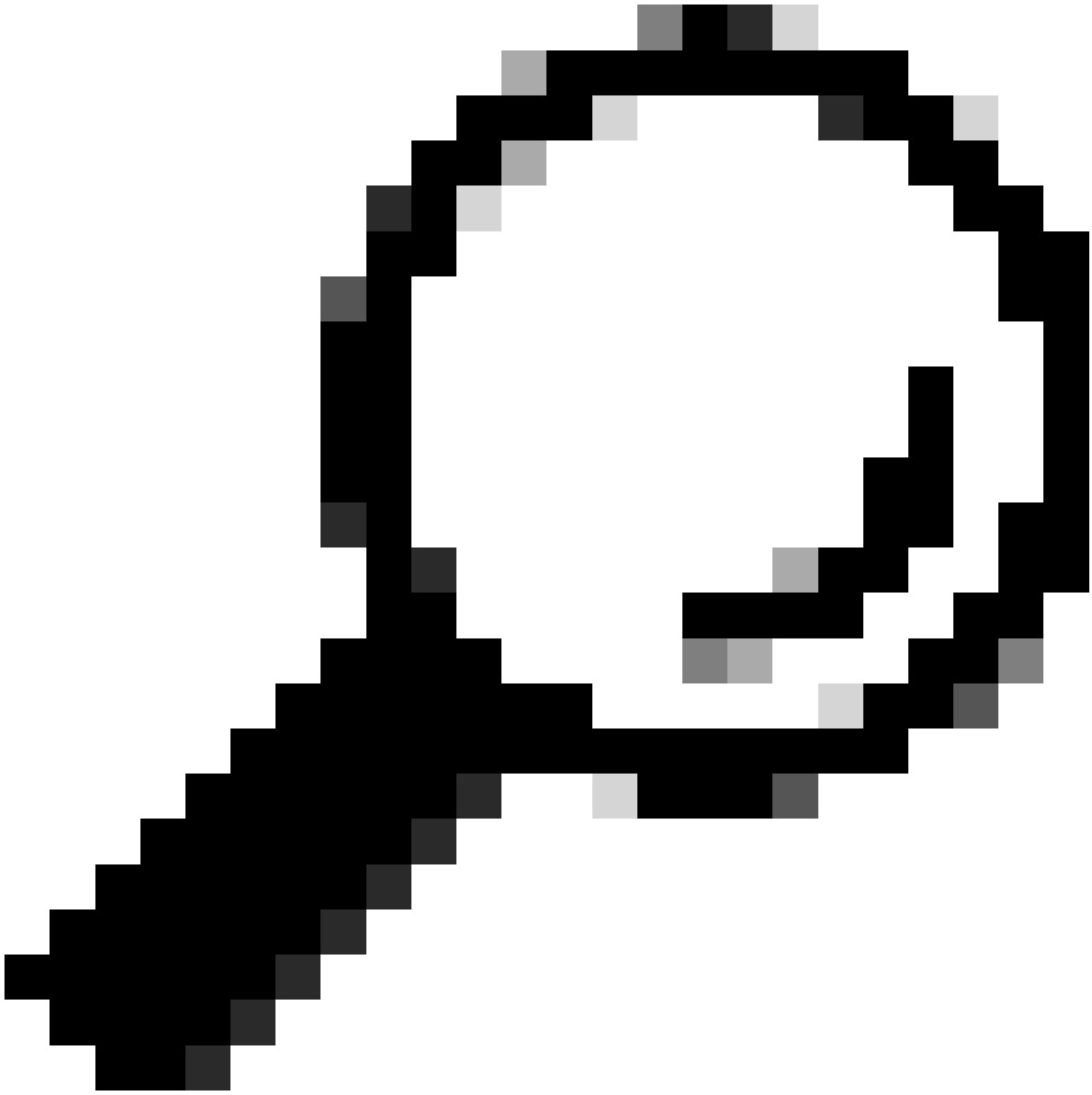
Solución

1. Vaya a la página Events (Eventos) de la consola de AMP para buscar el evento que desea investigar más a fondo.
2. Haga clic en el icono resaltado para abrir Trayectoria del dispositivo. 

   Icono de trayectoria del dispositivo
3. Puede ver los detalles del evento a la derecha en Detalles de la actividad. 

   Detalles del evento en la trayectoria del dispositivo
4. Desplácese hasta la parte inferior para localizar la sección Detectado por. 

   Detectado por sección



Consejo: Comprender esta información es esencial para evaluar la naturaleza de la amenaza y determinar rápidamente la exclusión adecuada que se debe configurar. Además, proporcionar estos detalles al enviar un caso al TAC para investigaciones de falsos positivos puede ayudar a acelerar el proceso.

Si no puede ver la sección Detectado por o necesita más ayuda, póngase en contacto con el TAC.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).