Identifier le moteur de détection dans Secure Endpoint Console

Table des matières

Introduction

Ce document décrit comment identifier le moteur responsable d'une détection spécifique dans la console Secure Endpoint.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Console Cisco Secure Endpoint

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de logiciel suivantes :

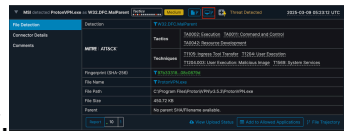
- Console de terminal sécurisé v5.4.2025030619

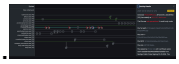
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Problème

L'identification du moteur approprié responsable d'une détection spécifique est l'une des étapes initiales permettant de comprendre la nature de l'événement et de le trier efficacement.

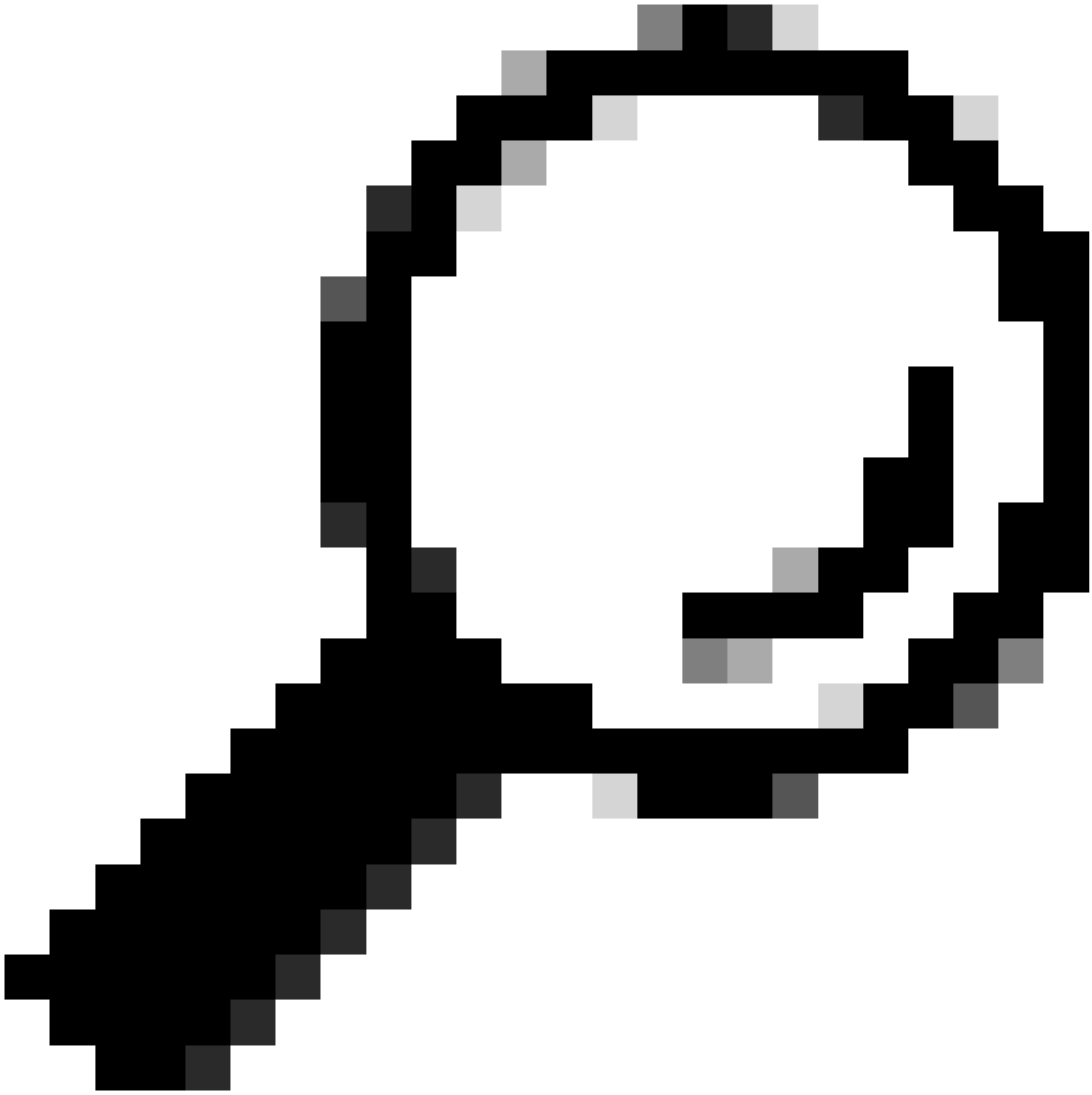
Solution

1. Accédez à la page Événements de votre console AMP pour rechercher l'événement que vous souhaitez approfondir.
2. Cliquez sur l'icône mise en surbrillance pour ouvrir Device Trajectory. 

   Icône Trajectoire du périphérique
3. Vous pouvez afficher les détails de l'événement à droite sous Détails de l'activité. 

   Détails des événements dans la trajectoire du périphérique
4. Faites défiler jusqu'en bas pour localiser la section Détecté par. 

   Détecté par section



Conseil : La compréhension de ces informations est essentielle pour évaluer la nature de la menace et déterminer rapidement l'exclusion appropriée à configurer. En outre, le fait de fournir ces détails lors de la soumission d'un dossier au TAC pour des investigations de faux positifs peut contribuer à accélérer le processus.

Si vous ne parvenez pas à afficher la section Détecté par ou si vous avez besoin d'aide, contactez le TAC.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.