Identify Detection Engine in Secure Endpoint Console

Contents

Introduction

Prerequisites

- Requirements
- Components Used

Problem

Solution

Introduction

This document describes how to identify the engine responsible for a specific detection in the Secure Endpoint console.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco Secure Endpoint console

Components Used

The information in this document is based on these software versions:

- Secure Endpoint Console v5.4.2025030619

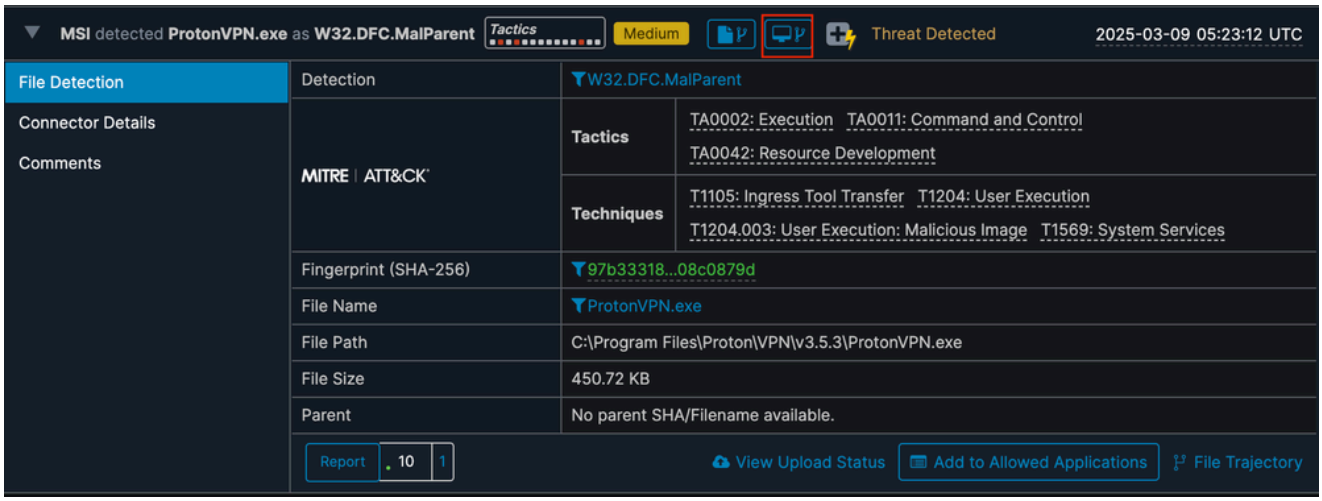
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Problem

Identifying the correct engine responsible for a specific detection is one of the initial steps in understanding the nature of the event and effectively triaging it.

Solution

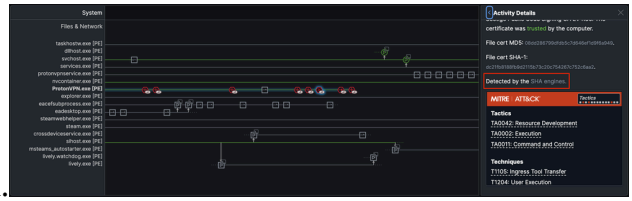
1. Navigate to the **Events** page in your AMP console to find the event you wish to investigate further.
2. Click the highlighted icon to open **Device Trajectory**.



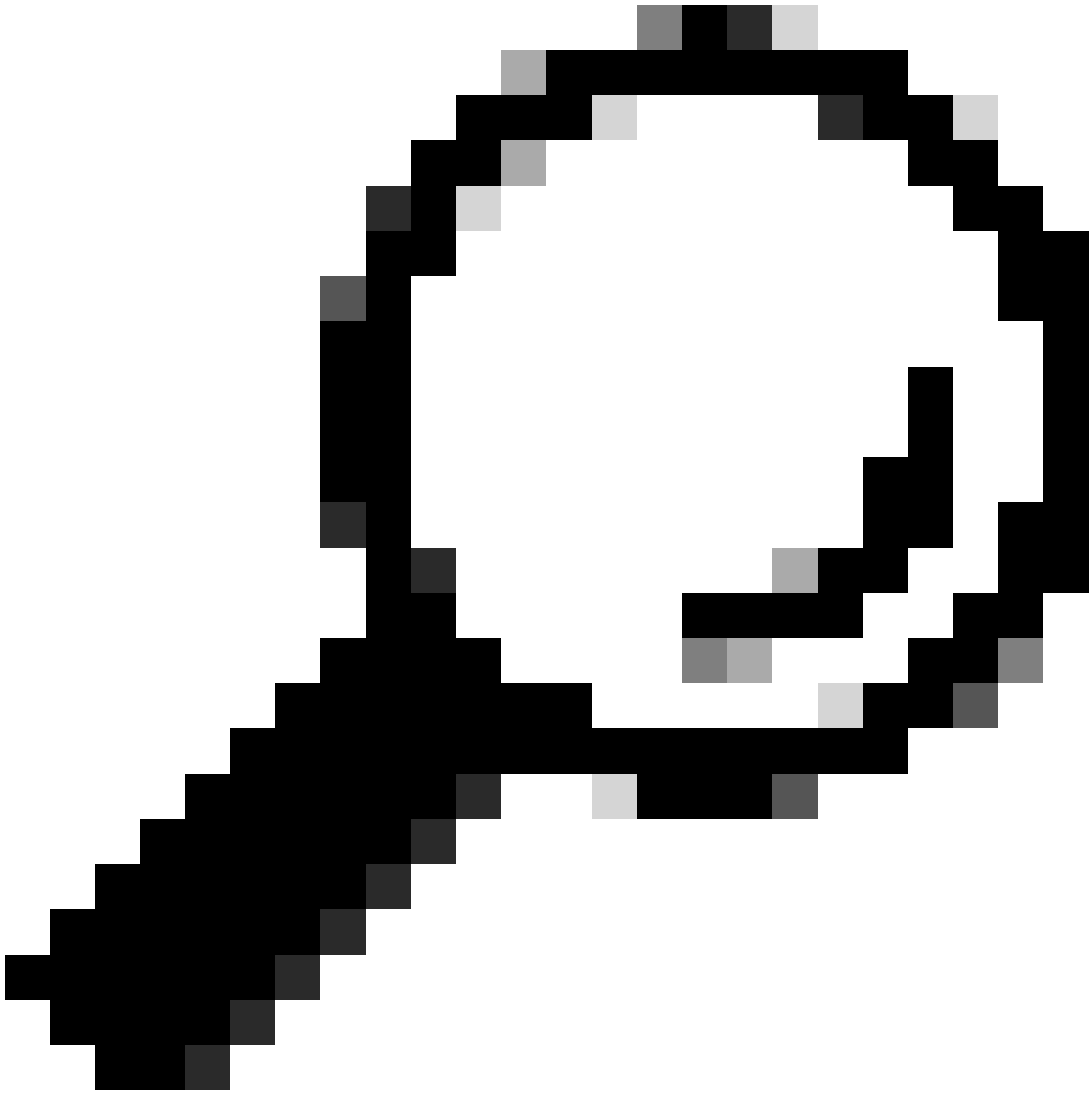
Device Trajectory Icon

3. You can view the event details to the right under **Activity Details**. 

Event Details in Device Trajectory

4. Scroll to the bottom to locate the **Detected by** section. 

Detected By Section



Tip: Understanding this information is essential for assessing the nature of the threat and swiftly determining the appropriate exclusion to configure. Additionally, providing these details when submitting a case to TAC for False Positive investigations can help expedite the process.

If you are unable to view the Detected By section or for any further assistance, contact TAC.