在安全终端控制台中识别检测引擎

目录

简介

本文档介绍如何在安全终端控制台中识别负责特定检测的引擎。

先决条件

要求

Cisco 建议您了解以下主题：

- 思科安全终端控制台

使用的组件

本文档中的信息基于以下软件版本：

- 安全终端控制台v5.4.2025030619

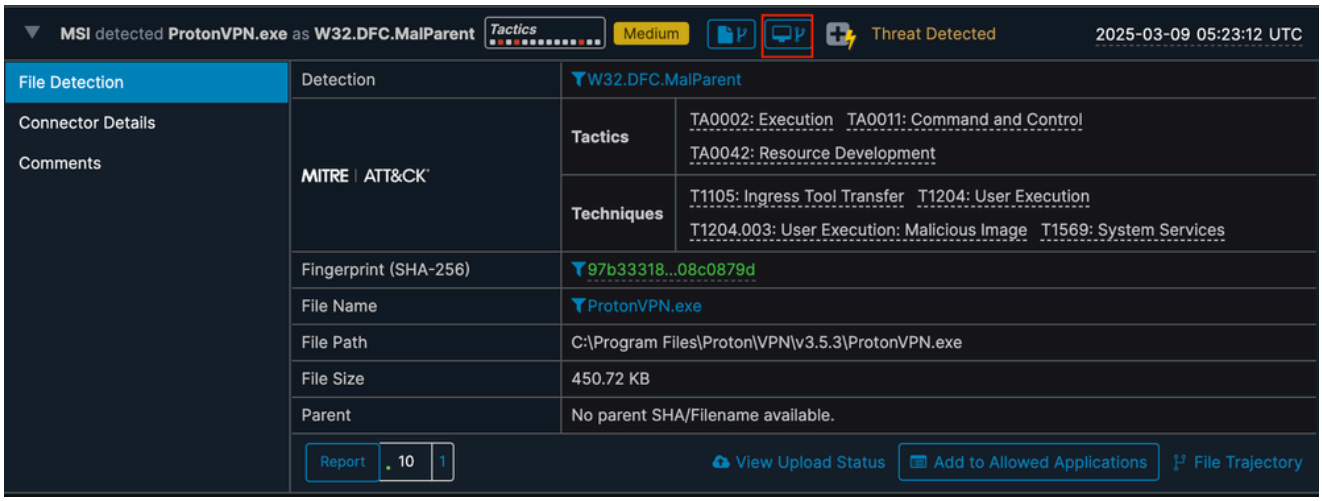
本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

问题

确定负责特定检测的正确引擎是了解事件性质并有效对其进行分类的初始步骤之一。

解决方案

1. 导航到AMP控制台中的Events页面，以查找要进一步调查的事件。
2. 单击突出显示的图标打开Device Trajectory。

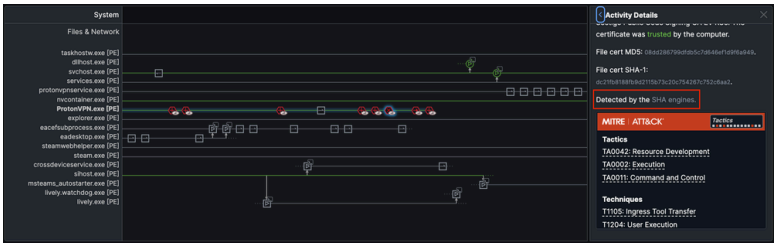


设备轨迹图标

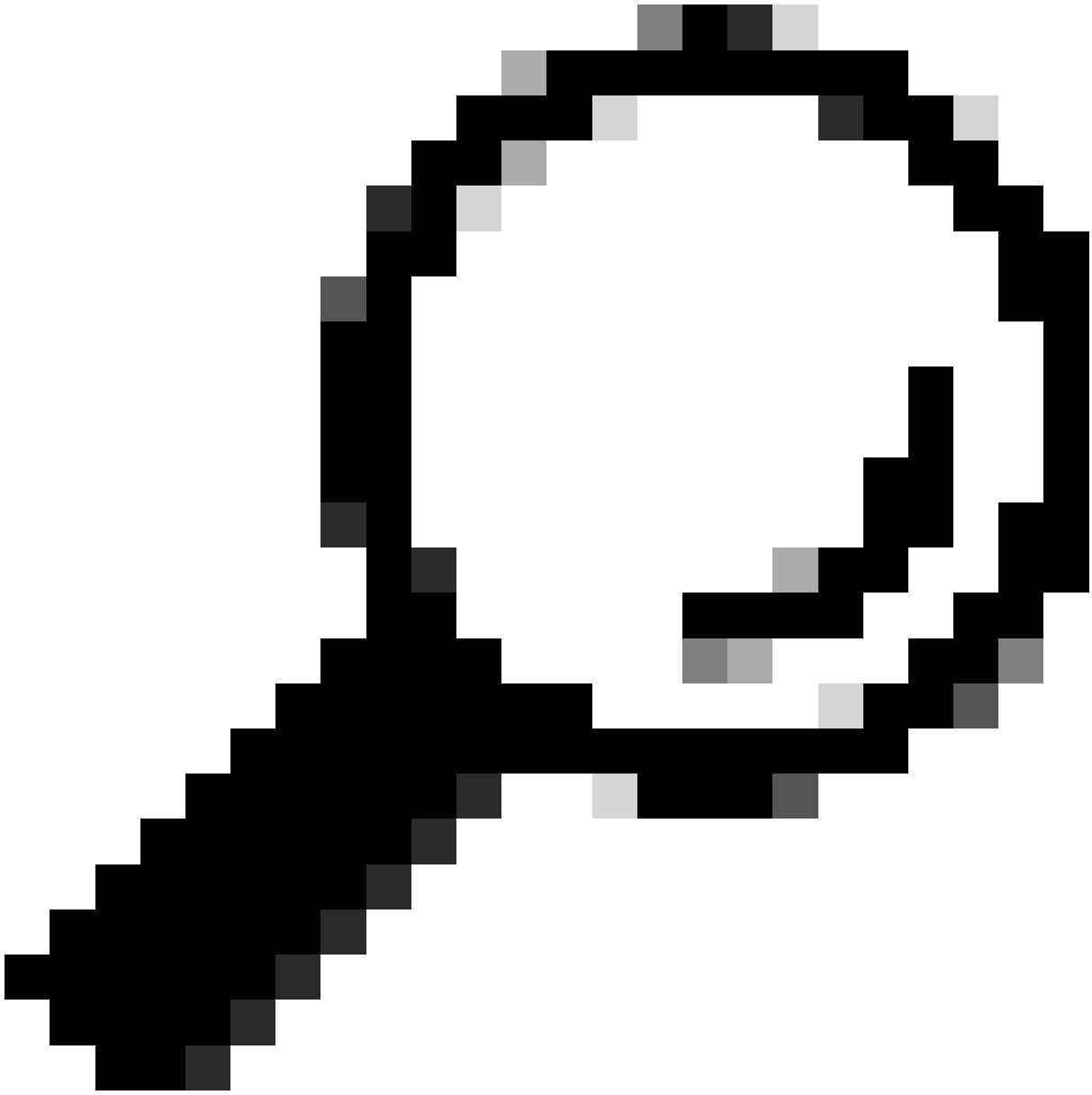
3. 您可以在右侧的Activity Details下查看事件详细信息。

设备轨迹中的事件详细信息

4. 滚动到底部，找到“Detected by”部分。



按部分检测



提示：了解此信息对于评估威胁的性质以及快速确定要配置的适当排除项至关重要。此外，向TAC提交支持误报调查的案例时，提供这些详细信息有助于加快流程。

如果您无法查看“检测者”(Detected By)部分或寻求任何进一步帮助，请联系TAC。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。