在安全終端控制檯中識別檢測引擎

目錄

簡介

本文檔介紹如何識別負責安全終端控制檯中的特定檢測的引擎。

必要條件

需求

思科建議您瞭解以下主題：

- 思科安全終端主控台

採用元件

本檔案中的資訊是根據以下軟體版本：

- 安全終端控制檯5.4.2025030619

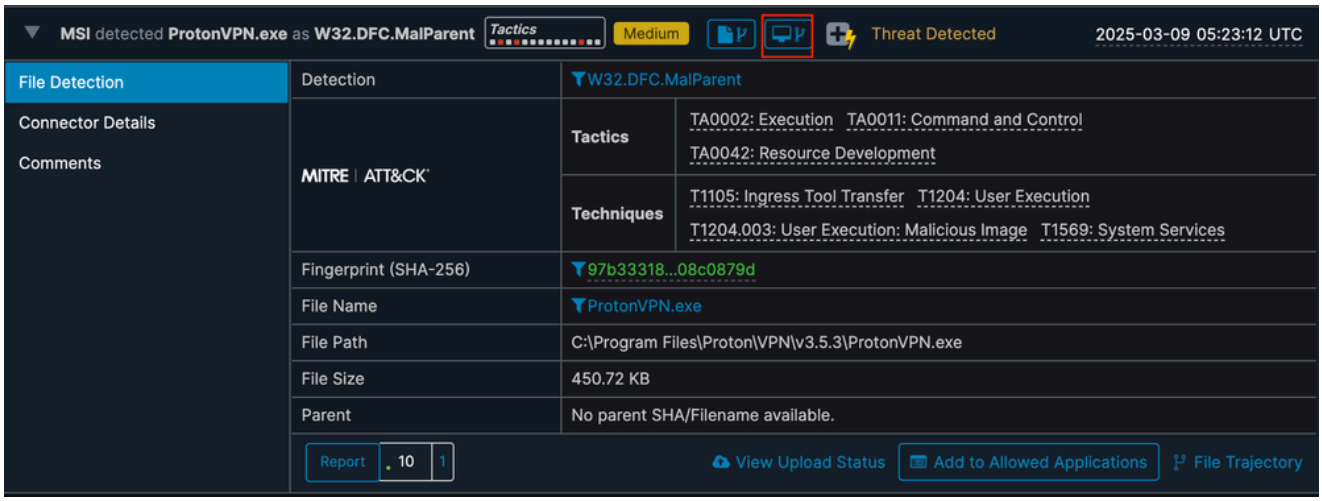
本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

問題

確定負責特定檢測的正確引擎是瞭解事件性質並對其進行有效分類的最初步驟之一。

解決方案

1. 導航到AMP控制檯中的Events頁面，查詢要進一步調查的事件。
2. 按一下突出顯示的圖示以開啟Device Trajectory。



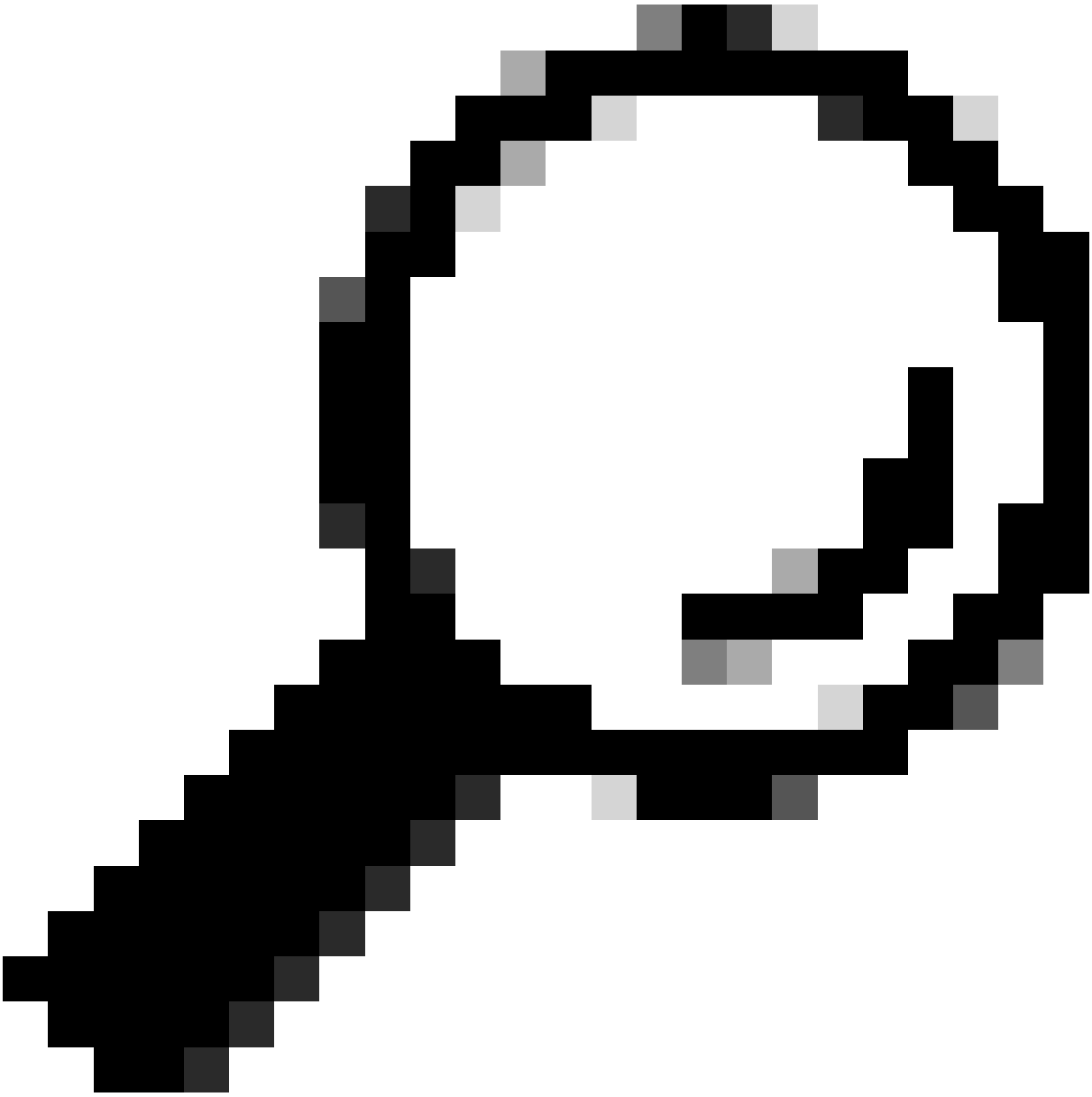
裝置軌跡圖示

3. 您可以檢視Activity Details下的右側事件詳細資訊。

裝置軌跡中的事件詳細資訊

4. 滾動到底部，找到「Detected by(檢測者)」部分。

按節檢測



提示：瞭解此資訊對於評估威脅的性質以及快速確定要配置的適當排除項至關重要。此外，將案件提交至TAC進行誤報調查時提供這些詳細資訊，有助於加快程式。

如果您無法檢視「檢測者」部分或任何進一步幫助，請聯絡TAC。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。