セキュアエンドポイントコンソールでの検出エンジンの識別

内容

はじめに

このドキュメントでは、セキュアエンドポイントコンソールで特定の検出を実行するエンジンを特定する方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Cisco Secure Endpointコンソール

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアのバージョンに基づいています。

- セキュアエンドポイントコンソールv5.4.2025030619

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

問題

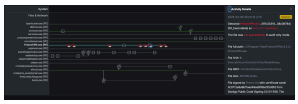
特定の検出の原因となる正しいエンジンを特定することは、イベントの性質を理解し、イベントを効果的にトリガーするための最初のステップの1つです。

解決方法

1. AMPコンソールのイベントページに移動し、さらに調査するイベントを見つけます。
2. 強調表示されたアイコンをクリックして、デバイストラジェクトリを開きます。

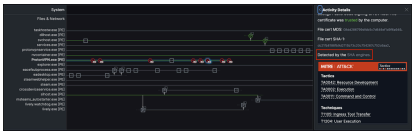
デバイストラジェクトリアイコン

3. 右側のアクティビティの詳細の下に、イベントの詳細が表示されます。

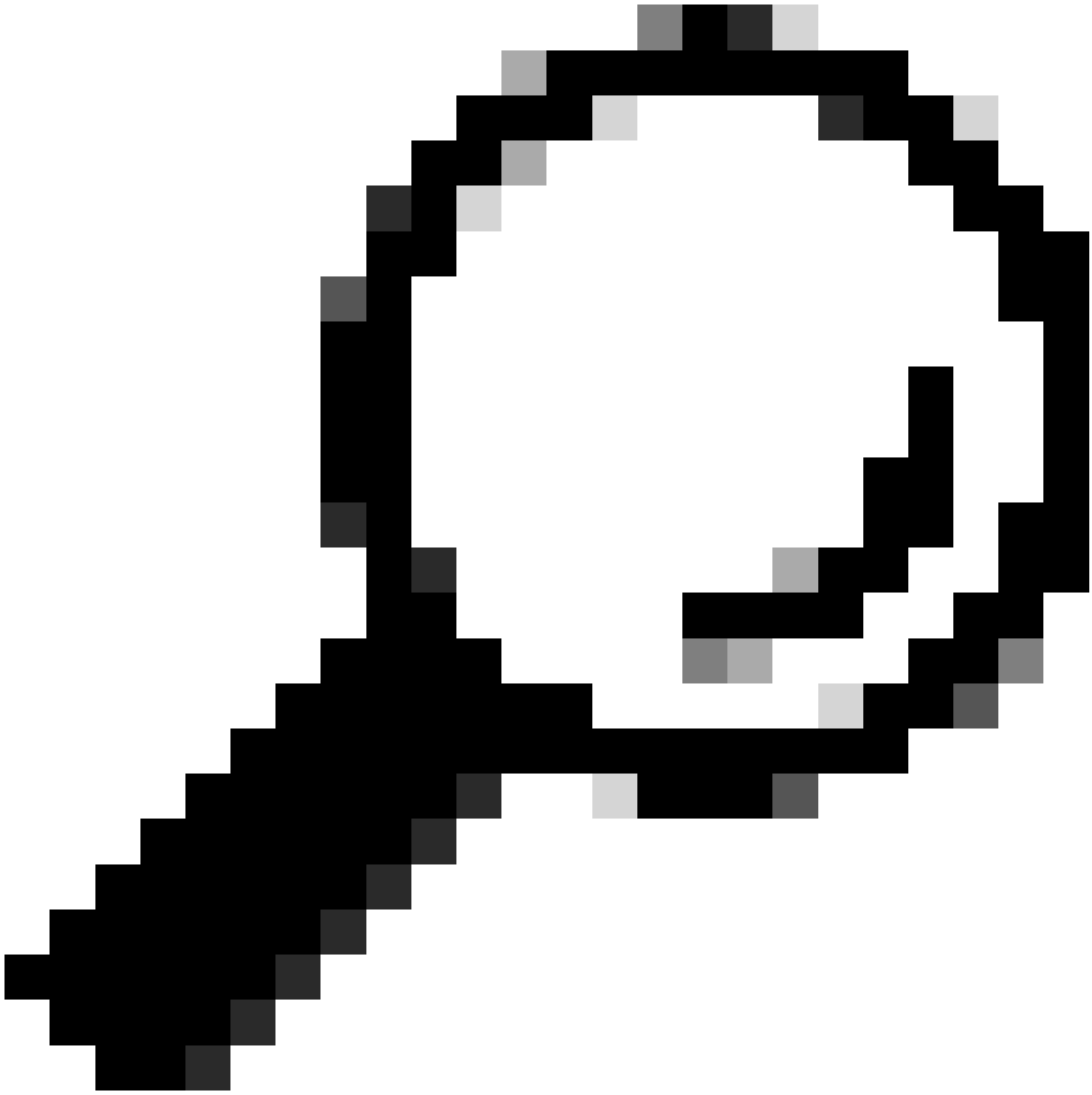


デバイストラジェクトリーのイベントの詳細

4. 一番下までスクロールしてDetected byセクションを探します。



セクションによって検出



ヒント：この情報を理解することは、脅威の性質を評価し、設定する適切な除外を迅速に判断するために不可欠です。さらに、誤検出調査のためにTACにケースを送信する際にこれらの詳細を提供すると、プロセスを迅速に進めることができます。

「Detected By」セクションを表示できない場合、またはさらにサポートが必要な場合は、TACにお問い合わせください。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。