Cisco Secure Endpoint Connectorの除外の設定と管理

内容

はじめに

このドキュメントでは、Cisco Secure Endpointコンソールのさまざまなエンジンの除外を作成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。

- セキュアエンドポイントコンソールで除外リストを変更してポリシーに適用する
- Windows CSIDL規則

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco Secure Endpointコンソール5.4.20211013
- Secure Endpointユーザガイドの改訂2021年10月15日

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。

セキュアなエンドポイントワークフロー

高レベルの操作では、Cisco Secure Endpointは、コネクタのメインコンポーネントを介してファイルのセキュアハッシュアルゴリズム(SHA)を次の順序で処理します。

- 除外
- 四重機関
- アプリケーション制御（許可リスト/ブロックリスト）
- SHAエンジン
- 不正利用の防止(Exprev)/悪意のあるアクティビティの保護(MAP)/システムプロセスの保護/ネットワークエンジン（デバイスフローの関連付け）

注：除外または許可/ブロックリストの作成は、ファイルを検出したエンジンによって異なります。

Cisco Maintainedの除外

Cisco-Maintained除外は、Secure Endpoint Connectorとアンチウイルス、セキュリティ製品、またはその他のソフトウェアとの互換性を高めるために、シスコが作成および維持します。

これらの除外セットには、適切な動作を保証するためのさまざまなタイプの除外が含まれています。

これらの除外に対して実行された変更は、『Cisco Secure Endpoint Consoleに関するCiscoで管理される除外リストの変更』で追跡できます。

カスタム除外

セキュアエンドポイントエンジン

Tetra & SHAエンジンによるファイルスキャン（CPU使用率/ファイル検出）:

これらのタイプの除外は、ファイルの検出/検疫を回避したり、Secure Endpointの高CPU使用率を軽減したりするために使用します。

Secure Endpointコンソールのイベントは、次の図のように表示されます。

注：除外にはCSIDLを使用できます。CSIDLの詳細については、このMicrosoftのドキュメントを参照してください。

パスの除外

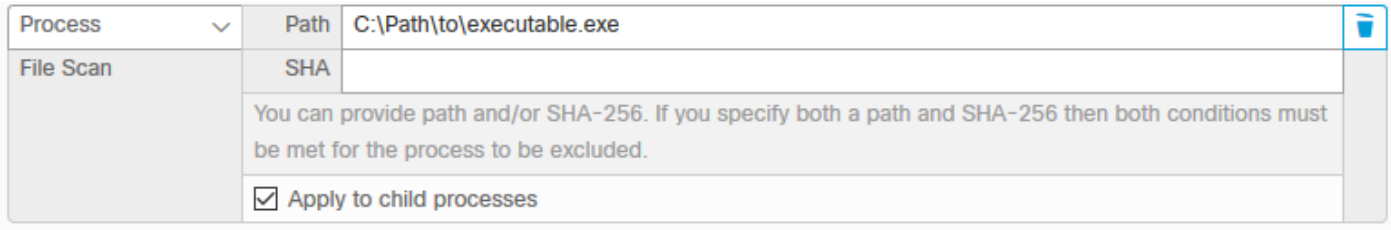
ワイルドカードの除外

注:[すべてのドライブ文字に適用]オプションは、システムに接続されているドライブ[A ~ Z]にも除外を適用するために使用されます。

ファイル拡張子の除外

注意：このタイプの除外は、パスの場所に関係なく、ファイル拡張子を持つすべてのファイルをスキャンから除外するため、注意して使用してください。

プロセス：ファイルスキャンの除外

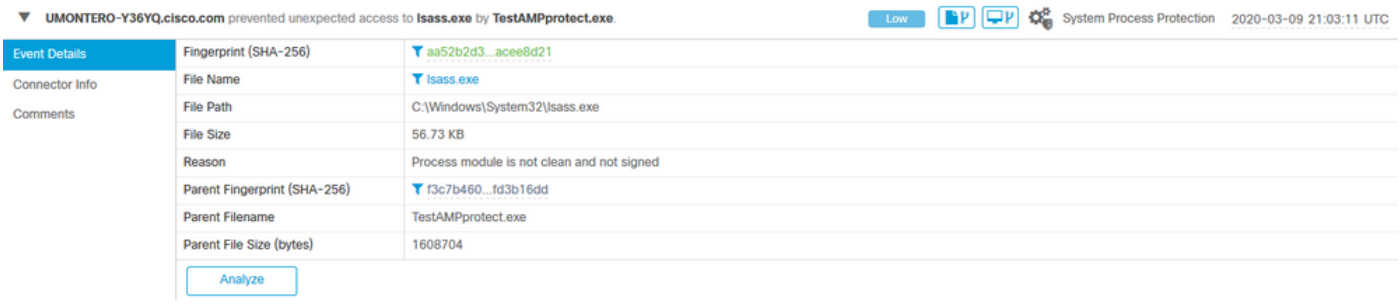


システムプロセス保護(SPP)

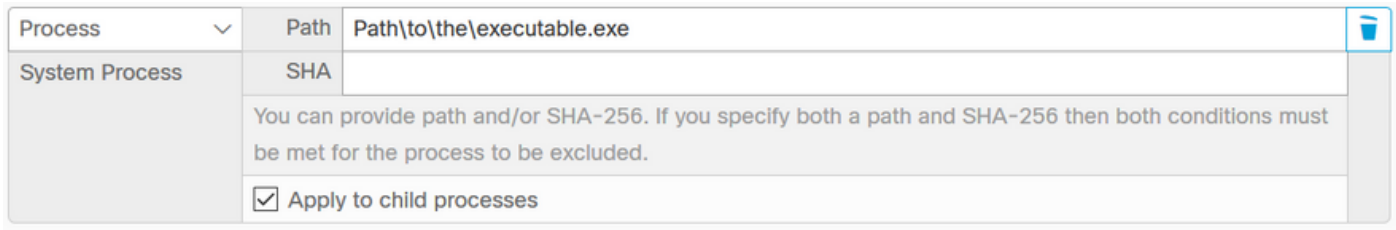
System Process Protection Engineは、コネクタバージョン6.0.5から入手でき、次のWindowsプロセスを保護します。

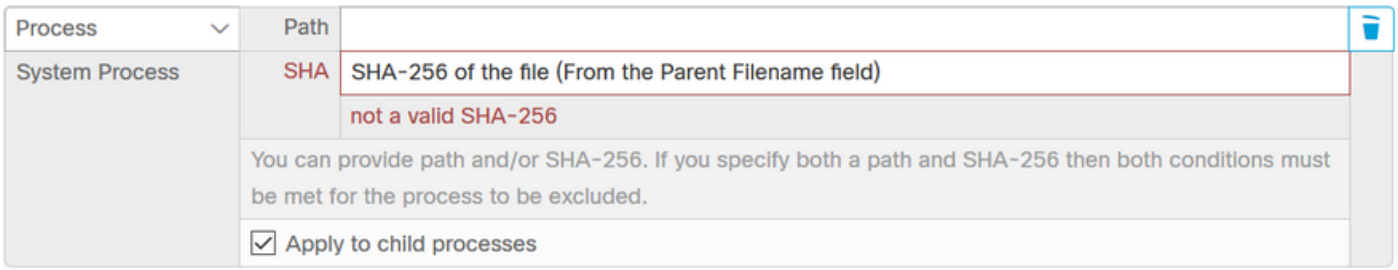
- セッションマネージャサブシステム(smss.exe)
- クライアント/サーバランタイムサブシステム(csrss.exe)
- ローカルセキュリティ機関サブシステム(lsass.exe)
- Windowsログオンアプリケーション(winlogon.exe)
- Windowsスタートアップアプリケーション(wininit.exe)

次の図に、SPPイベントを示します。



SPP除外

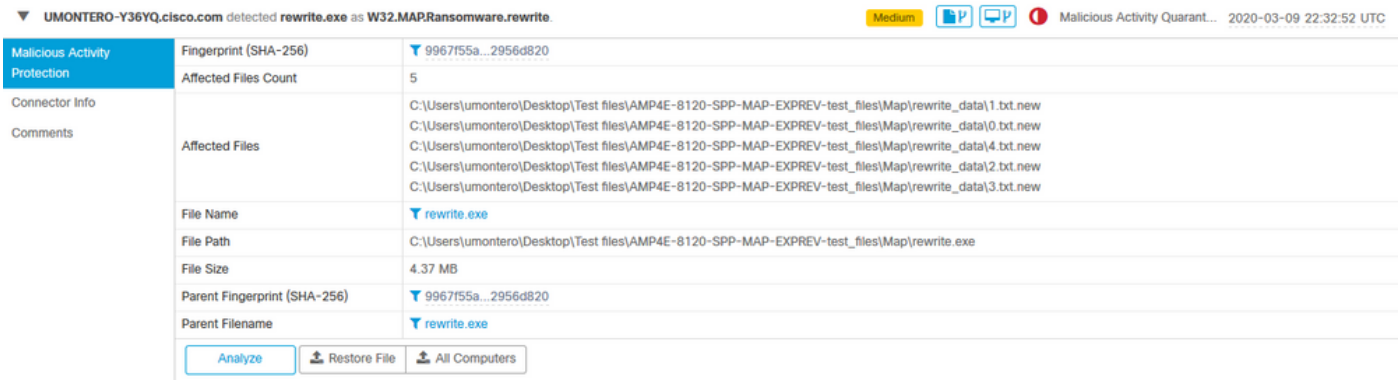




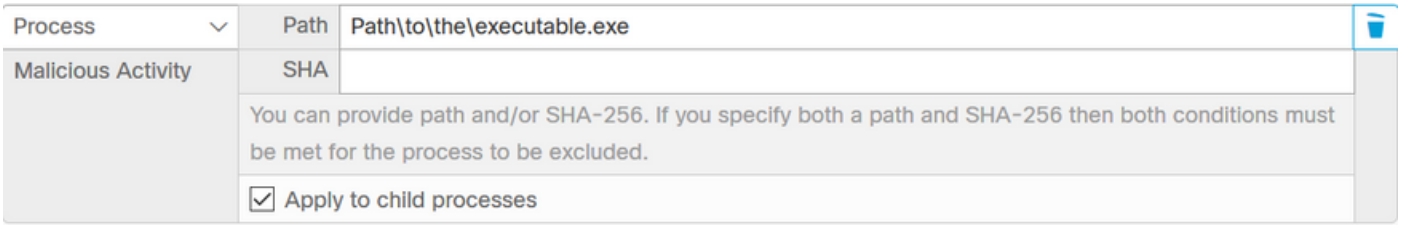
悪意のあるアクティビティの保護(MAP)

Malicious Activity Protection(MAP)エンジンは、エンドポイントをランサムウェア攻撃から保護します。悪意のあるアクションやプロセスが実行されたときに特定し、データを暗号化から保護します。

MAPイベントを次の図に示します。



MAP除外

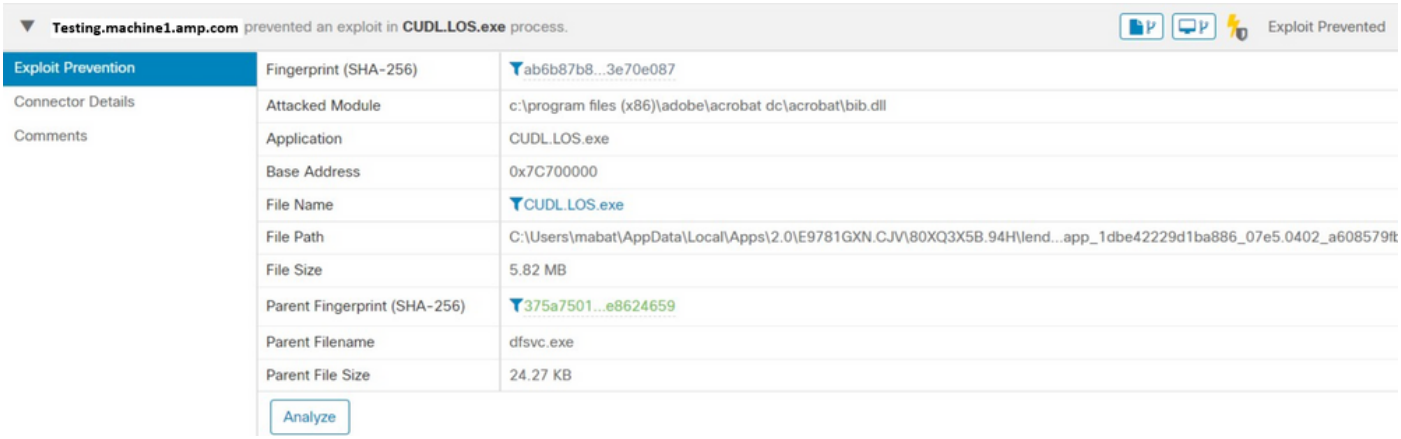


⚠ 注意：このタイプの除外は慎重に使用し、検出が悪意のあるものでないことを確認した後に使用してください。

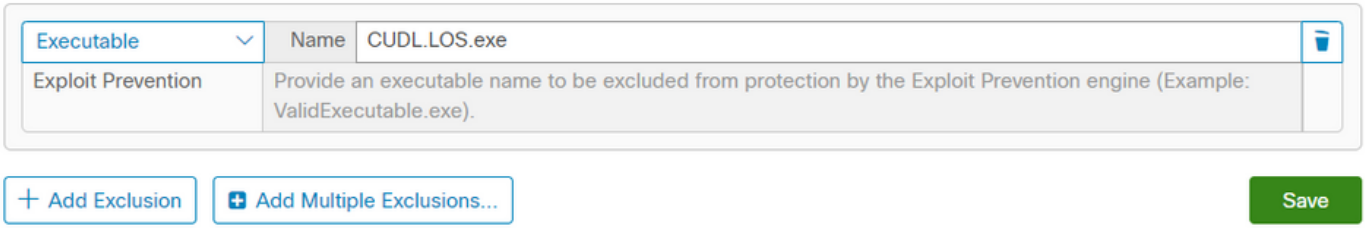
不正利用の防止(Exprev)

この不正利用の防止エンジンは、マルウェアが通常使用するメモリインジェクション攻撃や、パッチが適用されていないソフトウェアに対するその他のゼロデイ攻撃からエンドポイントを保護します
を参照してください。保護されたプロセスに対する攻撃を検出すると、ブロックされてイベントが生成されますが、隔離は行われません。

Exprevイベントを次の図に示します。



除外の表示

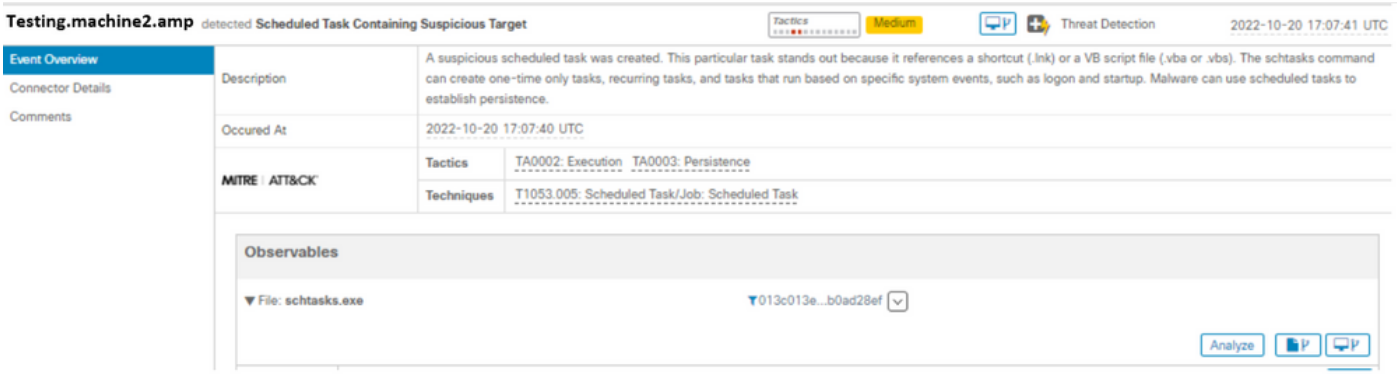


⚠ 注意：影響を受けるモジュールまたはアプリケーションのアクティビティを信頼する場合は、この除外を使用してください。

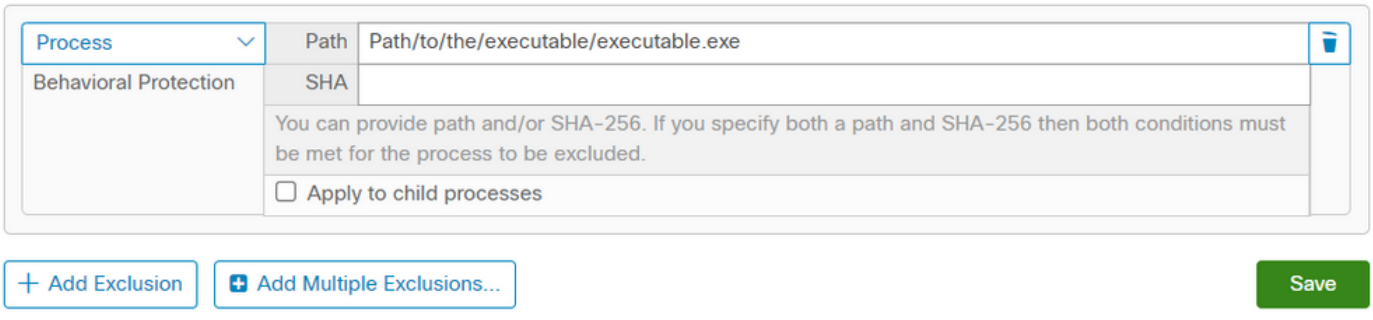
行動保護(BP)

動作保護エンジンは、脅威の動作を検出して停止する機能を強化します。また、「国外に住む」攻撃を検出する機能を強化し、
シグニチャアップデートを通じて、脅威状況の変化に迅速に対応できます。

BPイベントを次の図に示します。



血圧除外



関連情報

- ポリシー設定の詳細については、ユーザガイドを参照してください
- Cisco Secure Endpoint Connectorでの除外の作成に関するビデオ
- テクニカル サポートとドキュメント - Cisco Systems

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。