Cisco Secure Endpointでの高度なカスタム検出リストの作成

内容

概要

このドキュメントでは、Cisco Secure Endpointで高度なカスタム検出(ACD)を作成する手順について説明します。

背景説明

TALOS Intelligenceは、Microsoft Patch Tuesday Vulnerability Disclosureに対応するBLOGを2020年1月14日に公開しました。

1月15日更新：Microsoft ECC Code Signing Certificate Authority(https://blog.talosintelligence.com/2020/01/microsoft-patch-tuesday-jan-2020.html)としてマスカレードする証明書をスプーフィングすることで、CVE-2020-0601の不正利用を検出するために使用できるAMPのACDシグニチャを追加しました。

ACDで使用されるTALOS BLOG内のファイルの署名：

- Win.Exploit.CVE_2020_0601:1:*:06072A8648CE3D020106*06072A8648CE3D020 130
- https://alln-extcloud-storage.cisco.com/blogs/1/2020/01/CVE-2020-0601.txt

前提条件

要件

このドキュメントに特有の要件はありません。

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 Cloud Portal

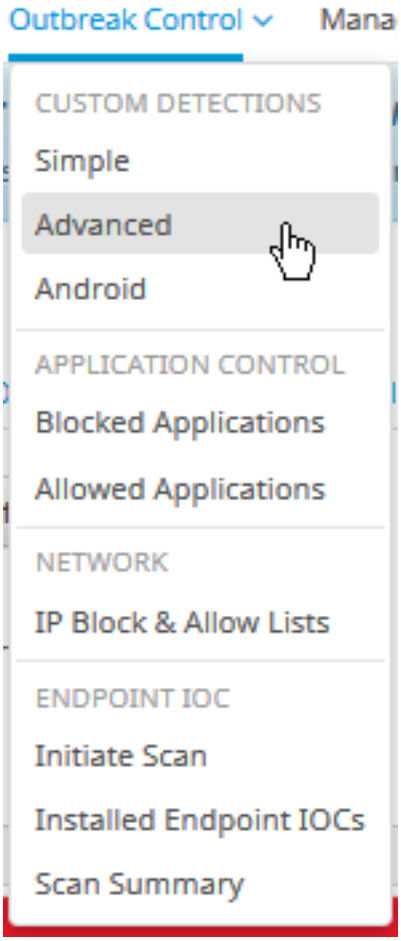
- ACD
- TALOSブログ

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たものです。 使用するすべてのデバイスは、クリアな（デフォルト）構成で開始されます。ネットワークが稼働中の場合は、コマンドの潜在的な影響を理解していることを確認してください。

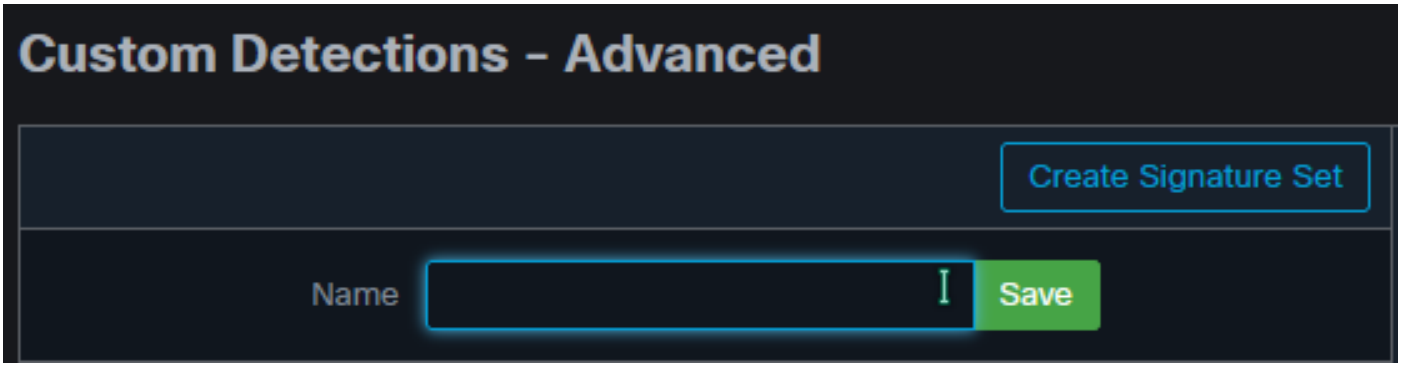
高度なカスタム検出リストの作成

次に、一致させるACDを作成します。

ステップ1：図に示すように、**[Secure Endpoint Portal] > [Outbreak Control] > [Advanced Custom Detection]**に移動します。

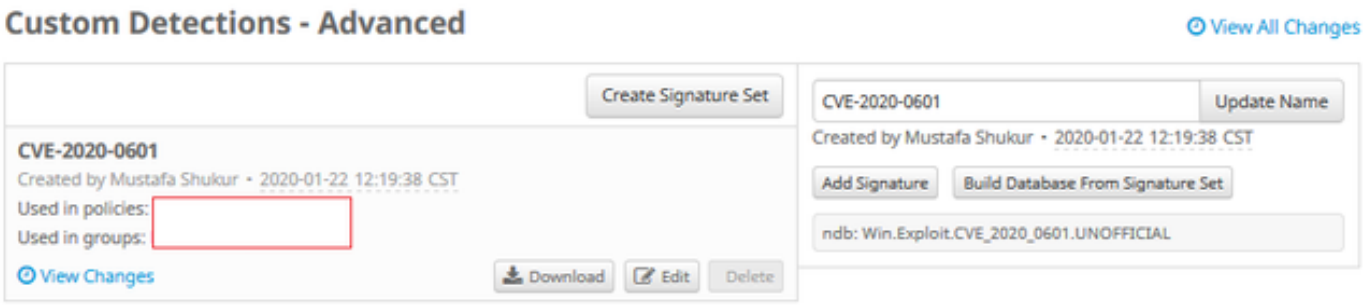


ステップ2：図に示すように、シグニチャセット**CVE-2020-0601の名前**で開始します。



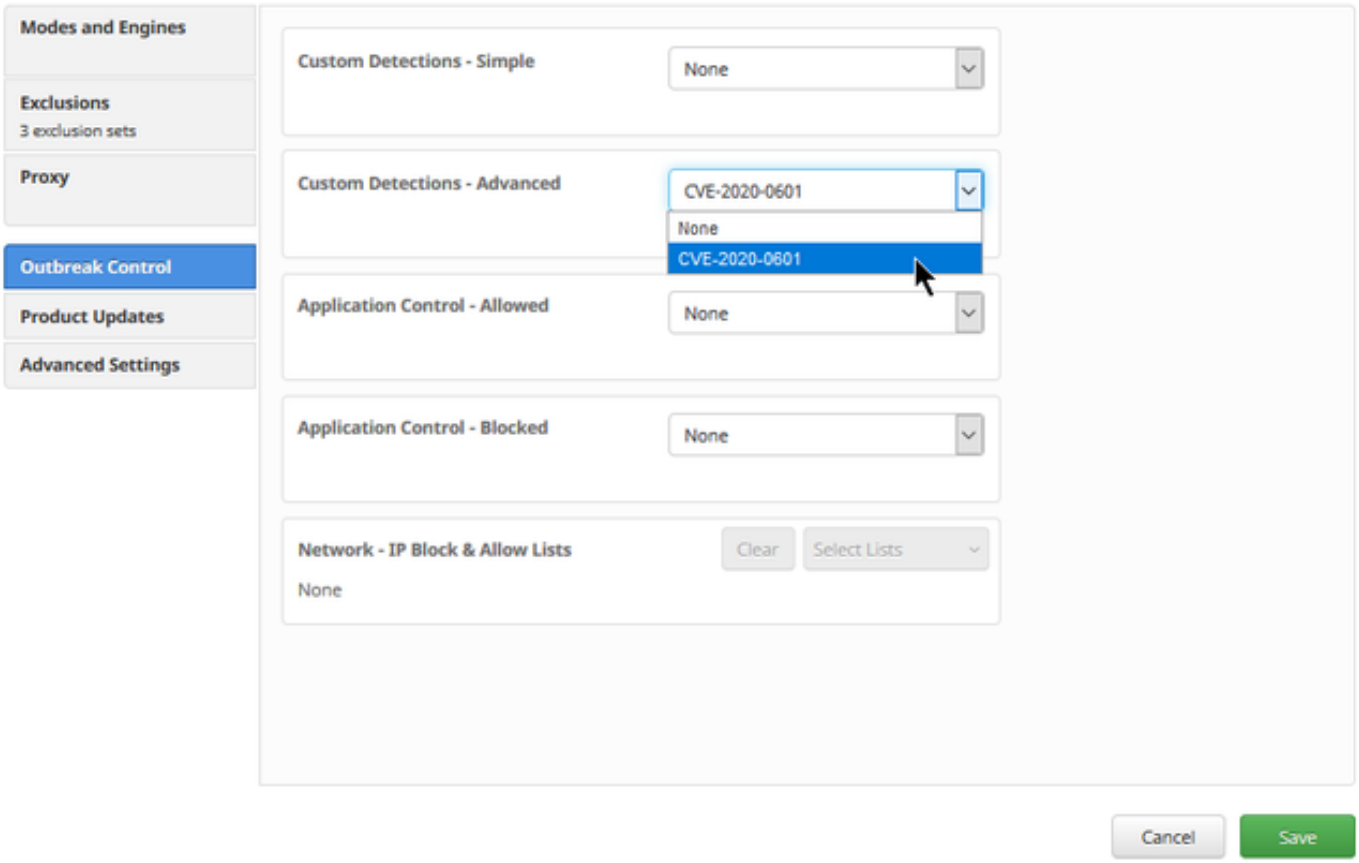
ステップ3：次に、その新しいシグニチャ・セットを編集し、[Add Signature]**を選択します。**

Win.Exploit.CVE_2020_0601:1:*:06072A8648CE3D020106*06072A8648CE3D02 0130。

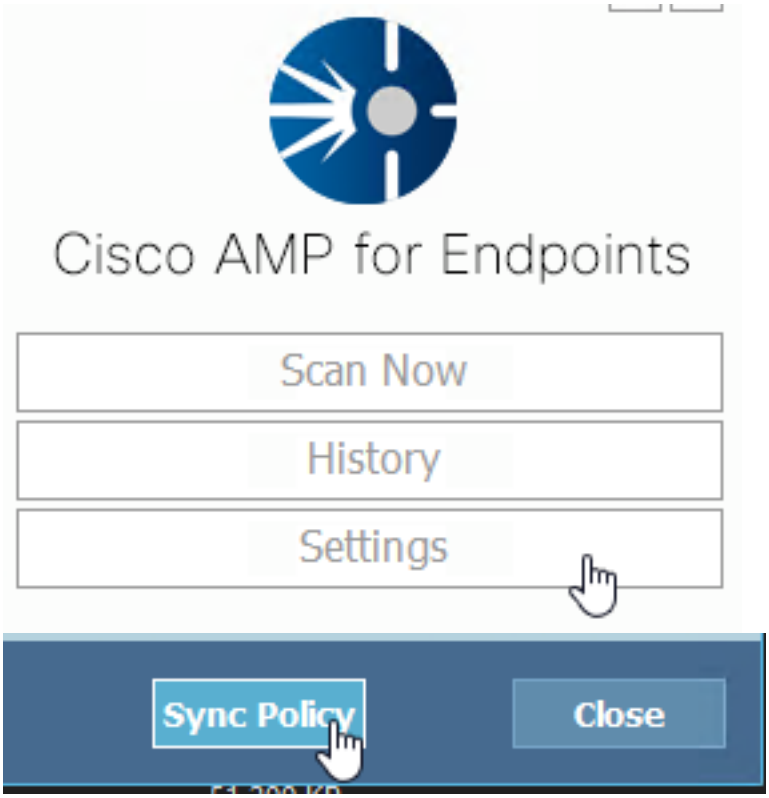


ステップ4:[Build Database From **Signature Set]を選択**して、データベースを作成します。

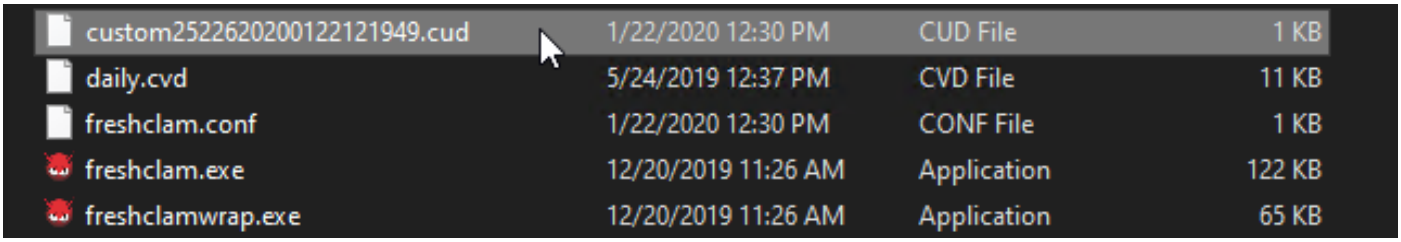
ステップ5：新しいシグニチャセットをポリシーに適用し、図に示すように、[Edit] > [Outbreak Control] > [Custom Detections] > [Advanced] をクリックします。



ステップ6：図に示すように、コネクタUIでポリシーと同期を保存します。



ステップ7：ディレクトリ**C:\Program Files\Cisco\AMP\ClamAVを検索**し、その日に作成された新しいSignatureフォルダを探します（図を参照）。



関連情報

- テストに使用されるビルドはWindows 10 1909で、MSKBごとの脆弱性の影響を受けません。https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0601
- https://support.microsoft.com/en-us/help/4534273/windows-10-update-kb4534273
- 適用対象：Windows 10、バージョン1809、Windows Serverバージョン1809、Windows Server 2019、すべてのバージョン
- **テクニカル サポートとドキュメント – Cisco Systems**