

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

内容

[概要](#)

[背景説明](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[高度なカスタム検出リストの作成](#)

[関連情報](#)

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

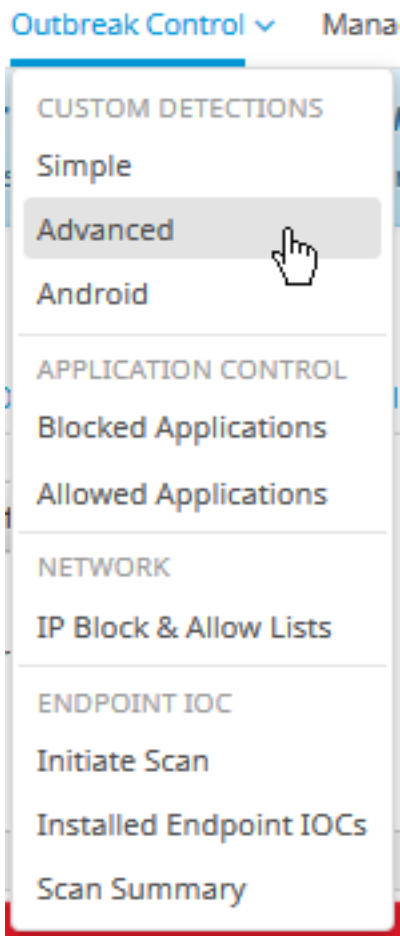
- ACD
- TALOSブログ

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。

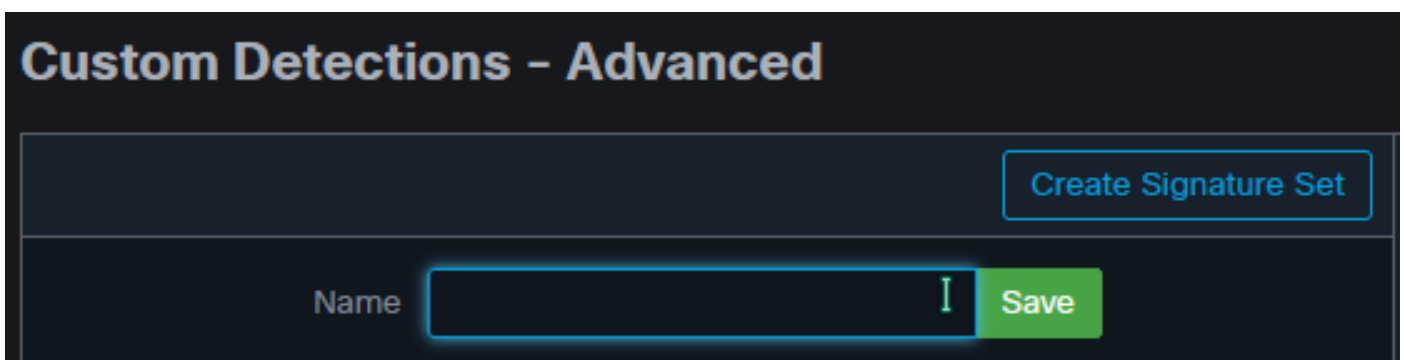
高度なカスタム検出リストの作成

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。

Custom Detections - Advanced

[View All Changes](#)

[Create Signature Set](#)

CVE-2020-0601 [Update Name](#)

Created by Mustafa Shukur · 2020-01-22 12:19:38 CST

Used in policies:

Used in groups:

[View Changes](#) [Download](#) [Edit](#) [Delete](#)

[Add Signature](#) [Build Database From Signature Set](#)

ndb: Win.Exploit.CVE_2020_0601.UNOFFICIAL

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。

Modes and Engines

Exclusions
3 exclusion sets

Proxy

Outbreak Control

Product Updates

Advanced Settings

Custom Detections - Simple

Custom Detections - Advanced

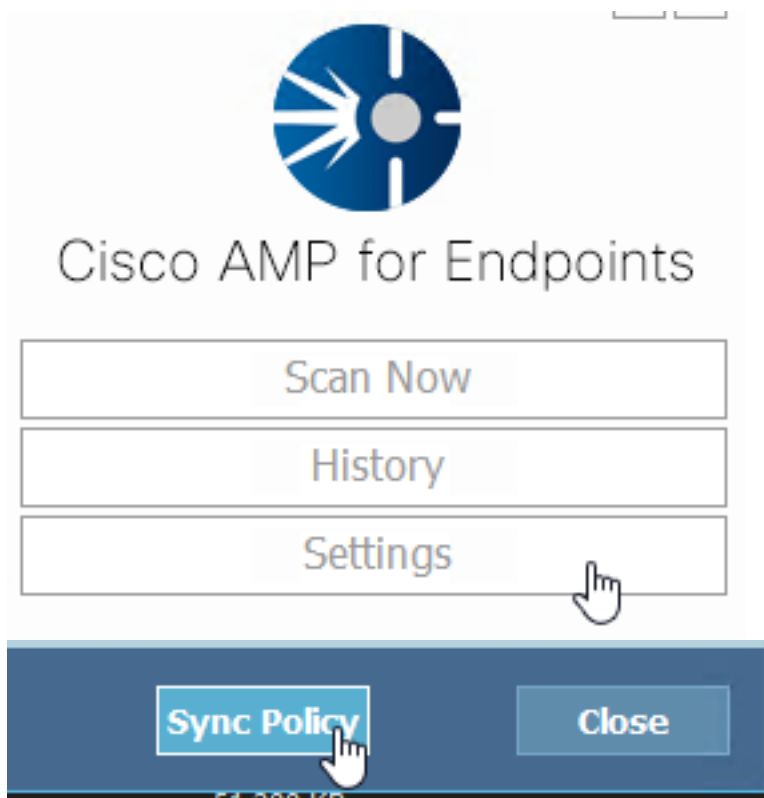
Application Control - Allowed

Application Control - Blocked

Network - IP Block & Allow Lists

None

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) 。

0.101.4.71	1/22/2020 12:30 PM	File folder	
custom2522620200122121949.cud	1/22/2020 12:30 PM	CUD File	1 KB
daily.cvd	5/24/2019 12:37 PM	CVD File	11 KB
freshclam.conf	1/22/2020 12:30 PM	CONF File	1 KB
freshclam.exe	12/20/2019 11:26 AM	Application	122 KB
freshclamwrap.exe	12/20/2019 11:26 AM	Application	65 KB

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](#)