

# エンドポイント向け AMP または FireAMP で Endpoint Indication of Compromise ( IOC ) スキャンを実行する

## 目次

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[IOC 署名 ファイル](#)

[IOC 署名 ファイルのスキャンをして下さい](#)

[IOC 署名 ファイルを作成して下さい](#)

[IOC 署名 ファイルをアップロードして下さい](#)

[スキャンを始めて下さい](#)

## 概要

この資料に Mandiant IOC エディタで妥協 ( IOC ) 署名 ファイルの示す値を、Cisco FireAMP ダッシュボードにそれを作成する方法をおよびエンドポイント IOC スキャンをアップロードする方法を始める方法を記述されています。

## 前提条件

### 要件

Cisco はエンドポイント IOC スキャンをするように試みる前に自由なドライブ領域の少なくとも 1 ギガバイトがあることを推奨します。

### 使用するコンポーネント

この文書に記載されている情報は Cisco FireAMP Windows コネクタ バージョン 4.0.2 およびそれ以降で利用可能であるエンドポイント IOC スキャンナーに基づいています。

本書の情報は、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。このドキュメントで使用するすべてのデバイスは、初期 ( デフォルト ) 設定の状態から起動しています。稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

さい。

## 背景説明

エンドポイント IOC スキャナー機能は複数のコンピューターを渡る後妥協インジケータースキャンするために使用する強力なインシデントレスポンスツールです。

注: FireAMP が Mandiant 言語の IOCS をサポートするが、Mandiant IOC エディタソフトウェア自体は Cisco によって開発されませんし、サポートされません。Cisco サポートはユーザー定義サードパーティ IOCS を解決しません。

## IOC 署名 ファイル

IOC 署名 ファイルは妥協の既知脅威、攻撃者方法論、または他の証拠を識別する技術特性の説明のための拡張可能な XML スキーマです。

名前のようなファイルプロパティで、サイズおよびハッシュ誘発するために書かれている、またプロセス情報のような他の属性およびシステム性質で OpenIOC ベースのファイルからコンソールを通してエンドポイント IOCS を、サービスインポートおよび Microsoft Windows レジストリエントリを実行します。IOC 構文は事件レスポンスによって特定の成果物を見つけるためにまたは malware の系列のための洗練された、関連させた検出を作成するのにロジックに従うために使用することができます。

## IOC 署名 ファイルのスキャンをして下さい

IOC 署名 ファイルのスキャンをするために完了する必要がある 3 つのステップがあります:

1. IOC 署名 ファイルを作成して下さい。
2. IOC 署名 ファイルをアップロードして下さい。
3. スキャンを始めて下さい。

これらのステップは続くセクションで説明されます。

## IOC 署名 ファイルを作成して下さい

注: この例では test.txt と名付けられるテキストファイルのための IOC 署名 ファイルを構築するために、Mandiant IOC エディタは使用されます。

IOC 署名 ファイルを作成するためにこれらのステップを完了して下さい:

1. IOCe を開き、File > New > インジケータにナビゲートして下さい。これは IOC を構築し始めることができるようにブランクワークスペースを提供します。

注: 特定の何かのための IOC を作成するためにプロパティとバイナリ ロジックに従って下さい。はたらく最も簡単なベースがある最初のオペレータはまたはです。これは IOC の最初の機能がはたらくようにします従ってそれを変更するために必要となりません。スキャンでそれを正常に使用するために IOC 署名 ファイルに少なくとも 2 つのプロパティか条件があることが必要となります。

2. オペレータを追加するために項目ドロップダウン メニューをクリックして下さい。追加する必要がある最初のプロパティはファイル拡張子含んでいます。項目ツリーメニューのプロパティを見つけ、クリックして下さい。
3. プロパティを追加した後、設定ペインを開くために画面の右端の小さいアイコンをクリックして下さい。このペインの中では、ファイル拡張子を一致するためにコンテンツ フィールドを使用して下さい。たとえば、`test.txt` テキストファイルを一致するために `txt` を追加して下さい:
4. 今ロジック オペレータを追加して下さい。この例では、テスト テキストファイルを一致する。これを一致するために、およびオペレータを使用し、次のプロパティを追加して下さい。ファイル名を見つけ、項目ツリーメニューから選択して下さい。プロパティ ペインでは、見つけたいと思うファイルの名前を追加して下さい。たとえば、コンテンツ フィールドのテストを追加して下さい:
5. 追加のプロパティがこの簡単な IOC に必要ではないので、今ファイルを保存することができます。File > Save の順にクリックすれば、.ioc 拡張の署名 ファイルはシステムで保存されます:

## IOC 署名 ファイルをアップロードして下さい

スキャンを行うために、FireAMP ダッシュボードに IOC ファイルをアップロードして下さい。IOC 署名 ファイル、XML ファイルを、または複数の IOC ファイルが含まれている zip アーカイブを使用できます。ダッシュボードは IOC シグニチャが付いているファイルを復元し、解析します。不適切な構文がサポートされていないプロパティが使用される場合知らせられます。

ヒント : 5 メガバイトまでであるファイルをアップロードできます。

FireAMP ダッシュボードに IOC 署名 ファイルをアップロードするためにこれらのステップを完了して下さい:

1. FireAMP Cloud コンソールにログイン し、発生制御に > インストール済みエンド ポイント IOC ナビゲートして下さい。
2. 『Upload』 をクリック すれば、アップロード エンド ポイント IOCS ウィンドウは現われます:

IOC 署名 ファイルが正常にアップロードされた後、シグニチャはリストで現われます:

3. シグニチャの実際の XML データを表示するために『View』 をクリックして下さい:

## スキャンを始めて下さい

署名 ファイルをアップロードした後、完全なスキャンを行って下さい。最初のスキャンは 1-2 時間がかかる場合がある全体のコンピュータのためのメタデータのカタログを構築する必要があるため完全なスキャンである必要があります。システムが完全なスキャンによってカタログされた後フラッシュ スキャンを行うことができます。

**注:** 完全なスキャンは非常に CPU 中心です。Cisco は使用中の間、PC の完全なスキャンをしないことを推奨します。機能を常用するために計画する場合カタログを再製するために完全なスキャンを月に一度行うことができます。

IOC スキャンをするために使用できる 2 つの異った方法があります。最初の方式はイベントまたはダッシュボードからの即時スキャンを行うことです。PC が Cloud にハートビートを送信 するのは次に引き起こされます。

**注:** 完全なスキャンをすることこれが最初になら、スキャン オプションの前に再カタログを チェックするために必要となりません。

第 2 方式はダッシュボードの発生コントロール メニューからのスケジュールされたエンド ポイント IOC スキャンを作成することです。このオプションはオフピークの時間の間にスキャンを行うことを望むとき理想的であるかもしれませんが。特定のコンピューターの権限が Scheduled Tasks を作成し、ログオンをバッチ グループ ポリシー権限として許可するためにあるアカウントの信任状を提供して下さい。

エンド ポイント IOC スキャンをスケジュールするとき、この警告メッセージが現れます:

その PC がハートビートを送信 する時次に、そして信任状が有効なら、Windows タスク スケジューラでこれと同じようなジョブを見るはずです:

スキャンが始まる時、このメッセージが現れます:

**注:** GUI が非表示であるために設定される場合システム カタログ表記を見ません。

スキャンが完了するとき、エンド ポイント IOC スキャン検出要約を表示できます。この例は test.txt IOC 署名 ファイルのための一致を示したものです: