Advanced Malware Protection （AMP）偽検出、発生および事件応答を操作する場合

目次

概要

Advanced Malware Protection （AMP）テクノロジーのための脅威 知性を改善し、拡張するように常に努力しますが AMP ソリューションがアラートを誘発しなかったし、またはアラートを間違って誘発しなかったら、環境にそれ以上の影響を防ぐいくつかの処置をとることができます。この資料はそれらのやるべきことでガイドラインを提供したものです。

説明

即座の行動

AMP ソリューションは脅威からネットワークを保護しなかったことを信じたら、次の処置をすぐにとって下さい:

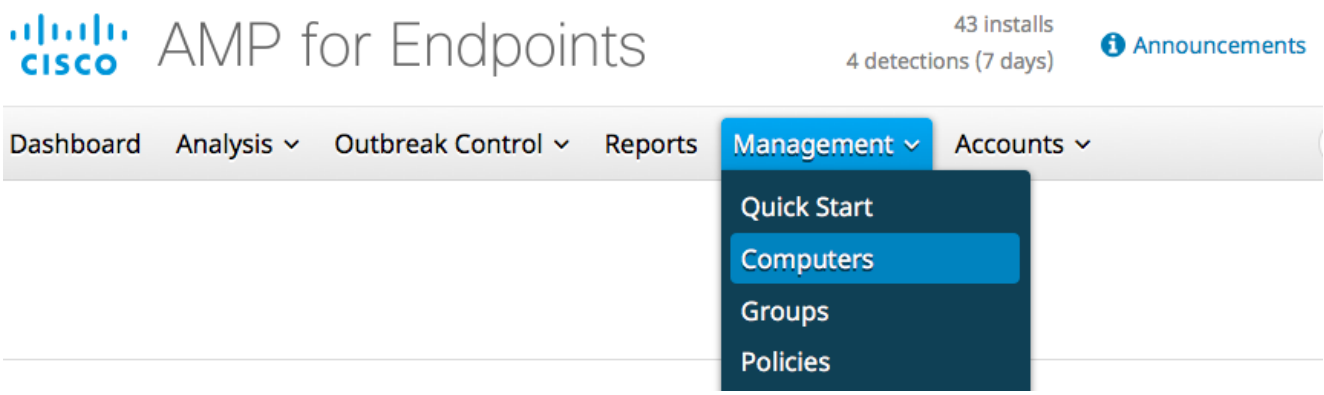
1. ネットワークの他からの疑わしい マシンを隔離して下さい。 これはマシンを消すか、またはネットワークから物理的に切り離すことを含む可能性があります。
2. マシンが感染するかもしれませんときに疑わしい マシンで感染、のような、時間ユーザー操作、先祖などについての重要な情報を書いて下さい

   警告： 一掃しませんでしたり、またはマシンをイメージ変更しないで下さい。 それは法廷調査かトラブルシューティング プロセスの間におこるソフトウェアかファイルを見つける可能性を除去します。

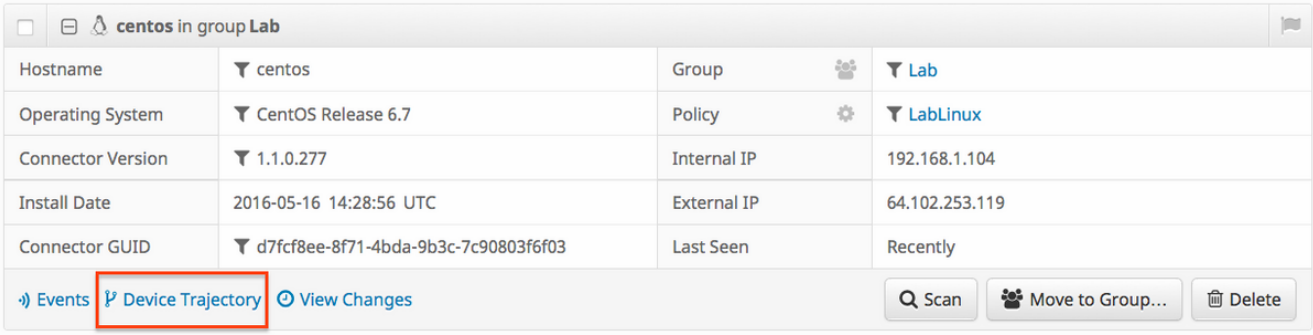
分析

1. あなた自身の調査を始めるのに**デバイス トラジェクトリ** 機能を使用して下さい。 デバイス トラジェクトリは 9，000,000 のほとんどの最近のファイル イベントをおよそ保存することができます。 AMP for Endpoints デバイス トラジェクトリはファイルを見つけ出すために非常に役立ちますまたはそれが感染に導いたプロセス。

   ダッシュボードでは、**管理 > コンピュータ**への移動。



疑わしい マシンを探し、そのマシンのためのレコードを拡張して下さい。 **トラジェクトリ** オプションを『Device』 をクリック して下さい。



2. 疑わしいファイルを見つけるか、またはハッシュする場合、カスタム検出リストにそれを追加して下さい。 AMP for Endpoints はファイルを扱うか、または悪意のあるようにハッシュするのにカスタム検出リストを使用できます。 これはそれ以上の影響を防ぐために応急カバレッジを提供する大きい方法です。

Cisco による分析

1. 動的解析のために疑わしいサンプルを入れて下さい。 ダッシュボードで**分析 > ファイル分析**から手動でそれらを入れることができます。 AMP for Endpoints は脅威 グリッドからのファイルの動作のレポートを生成する動的解析機能性が含まれています。 調査チームによる追加分析が必要となればこれにまた Cisco へファイルを提供することの利点があります。

2. ネットワークの *false positive* か *偽負*検出を疑う場合、AMP 製品のためのカスタム黒いリストまたは白リスト機能性を利用することを助言します。 Cisco Technical Assistance Center （ TAC ）に連絡するとき、分析に次の情報を提供して下さい:ファイルの SHA256 ハッシュ。ファイルのコピーもし可能なら。どこにのような来た、そしてなぜから環境にある必要があるかファイルについての情報。false positive または偽負であるとこれがなぜ信じるか説明して下さい。
3. 脅威を軽減するか、またはアクションプランを作成し、アクティブな発生を軽減するために感染させたマシンを研究し、高度ツールか機能を利用していることを専門にする環境のトリアージを行っていればアシスタンスを必要とする場合 Ciscoセキュリティ事件応答サービス （ CSIRS ）チームを実行する必要があります。
   注: Cisco Technical Assistance Center （ TAC ）は約束のこの型を支援に与えません。 CSIRS によってで説明されているプロシージャに従って下さい。 これは組織に Cisco からの事件応答サービスのための保持板がなければ $60,000 で開始する支払済サービスです。 実行されて彼らがサービスについての追加情報を提供し、事件のためのケースをオープンすれば。 彼らがプロセスで追加指導を提供できるようにまた Cisco Account Manager によっ

て追うことを推奨します。

関連記事

- Windows FireAMP
- FireAMP