目次

概要

高度 Malware 保護 (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。 AMP 製品がリアルタイムのアラートを引き起こさなかった場合、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

即時の処置

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:

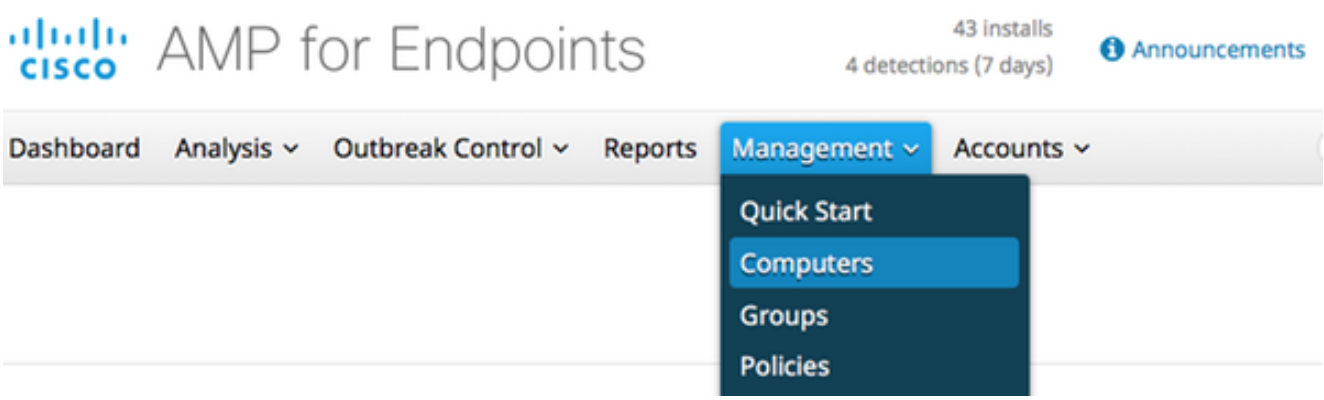
1. ネットワークの他からの疑わしい マシンを隔離して下さい。 これはマシンを消すか、またはネットワークから物理的に切り離すことを含む可能性があります。
2. マシンが感染するかもしれませんときに疑わしい マシンで感染、のような、時間ユーザー操作、先祖などについての重要な情報を書いて下さい

   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

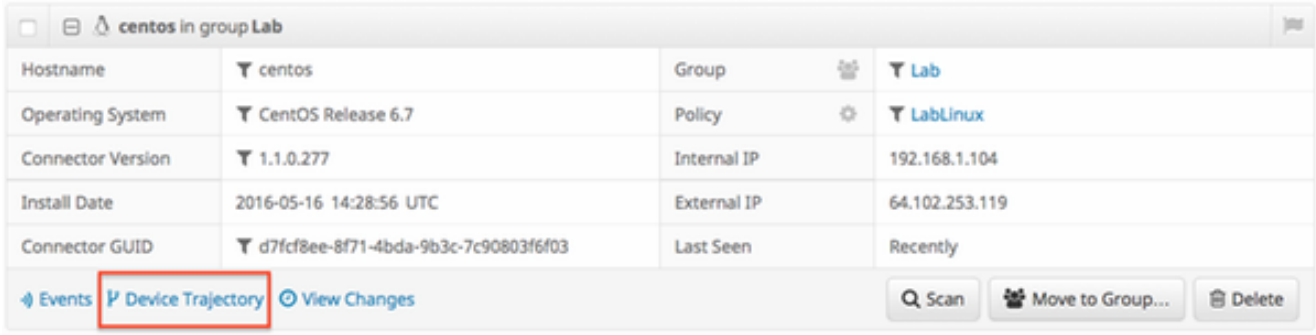
1. あなた自身の調査を始めるのに**デバイス トラジェクトリ** 機能を使用して下さい。 デバイス トラジェクトリは 9 , 000,000 のほとんどの最近のファイル イベントをおよそ保存することができます。 エンドポイント デバイス トラジェクトリのための AMP はファイルを見つけ出すために非常に役立ちますまたはそれが感染に導いたプロセス。

   ダッシュボードでは、**管理 > コンピュータ**へのナビゲート。



?

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。 エンドポイントのための AMP 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力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。 エンドポイントのための AMP 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* または *偽陰性* 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 または偽陰性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の作成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 緊急状態応答チーム（ 感染したマシンを研究し、発生を解決するのに高度ツールか機能を活用 する CSIRT 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。 CSIRT チームはこの電話番号を呼出すことによって enagaged できます: +1-844-831-7715。 それらはサービスについてのその他の情報を提供し、事件のためのケースをオープ

ンします。 それらがプロセスで追加指導を提供できるように Cisco Account Manager によって追って下さい。

関連記事

- Windows FireAMP
- FireAMP