[外部] – 高度なマルウェア防御(AMP)による誤検出、アウトブレイク、インシデント対応

内容

概要

Advanced Malware Protection(AMP)テクノロジーの脅威インテリジェンスの向上と拡張に努めておりますが、AMPソリューションがアラートをトリガーしなかったり、誤ってアラートをトリガーした場合は、環境への影響を防ぐために対策を講じることができます。このドキュメントでは、これらのアクション項目に関するガイドラインを示します。

説明

即時の処置

AMPソリューションがネットワークを脅威から保護していないと思われる場合は、すぐに次の措置を講じてください。

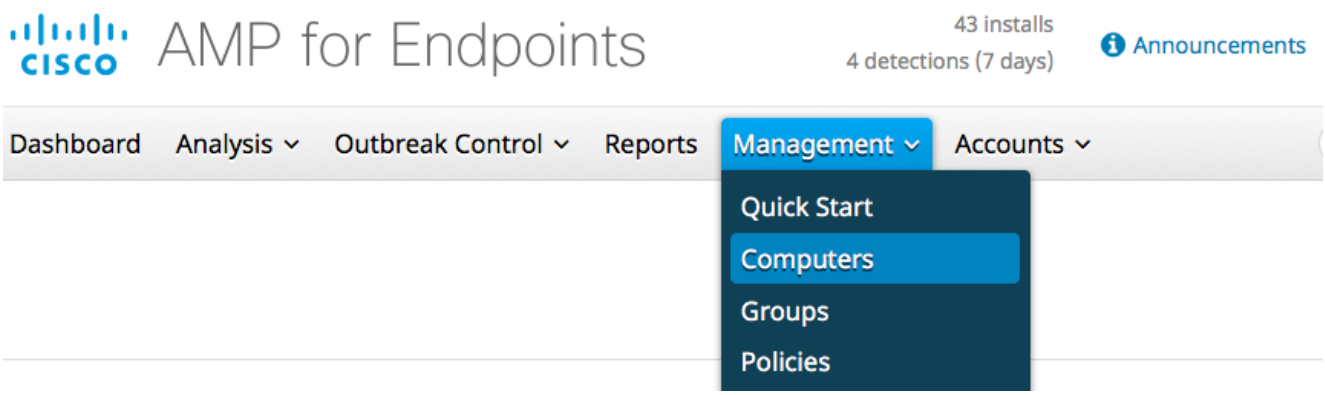
1. 疑わしいマシンをネットワークの残りの部分から隔離します。これには、マシンの電源を切るか、物理的にネットワークから切断することが含まれます。
2. 感染に関する重要な情報（マシンが感染している可能性がある時間、疑わしいマシンでのユーザアクティビティなど）を書き留めます。

   警告：マシンをワイプしたり再イメージ化したりしないでください。これにより、フォレンジック調査またはトラブルシューティングプロセスで問題のソフトウェアやファイルを見つける可能性がなくなります。

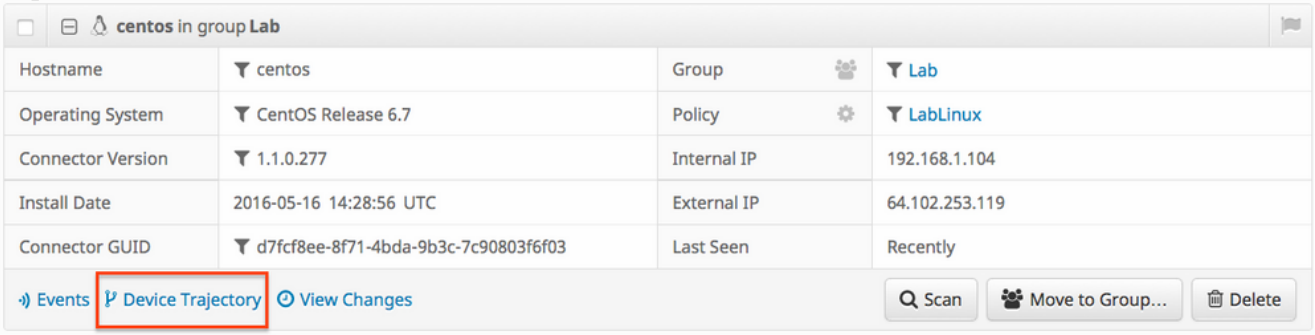
分析

1. デバイストラジ**ェクトリ**ジェクトリ機能を使用して、独自の調査を開始します。デバイストラジェクトリーは、最新の約900万件のファイルイベントを保存できます。エンドポイント用AMPデバイストラジェクトリは、感染の原因となったファイルやプロセスを追跡するのに非常に便利です。

   ダッシュボードで、[管理] > [コンピュータ]**に移動します。**



不審なマシンを見つけて、そのマシンのレコードを展開します。[デバイストラジェクトリー]**オプションを**クリックします。



2. 疑わしいファイルやハッシュが見つかった場合は、カスタム検出リストに追加します。AMP for Endpointは、カスタム検出リストを使用して、ファイルまたはハッシュを悪意のあるファイルとして扱うことができます。これは、さらなる影響を防ぐためにストップギャップカバレッジを提供する優れた方法です。

シスコによる分析

1. 疑わしいサンプルを動的分析のために発行します。ダッシュボードの「分析」>「ファイル分析」**から手動**で発行できます。エンドポイント用AMPには、脅威グリッドからファイルの動作のレポートを生成する動的分析機能が含まれます。また、調査チームによる追加の分析が必要な場合に、このファイルをシスコに提供する利点もあります。

2. ネットワーク内で誤検出*または誤検出が疑*わしい場合は、AMP製品にカスタムブラックリストまたはホワイトリストの機能を利用することをお勧めします。Cisco Technical Assistance Center(TAC)に連絡する際には、分析のために次の情報を提供してください。ファイルのSHA256ハッシュ。可能であれば、ファイルのコピー。ファイルの送信元や環境内にファイルが必要な理由など、ファイルに関する情報。なぜ、これが偽陽性または偽陰性であると考えるのかを説明します。
3. 脅威の軽減や環境のトリアージの実行を支援する必要がある場合は、アクションプランの作成、感染したマシンの調査、高度なツールや機能の活用を専門とするCisco Talos Incident Response(CTIR)チームと連携する必要があります。
注：Cisco Technical Assistance Center(TAC)は、このタイプの契約に関するサポートを提供しません。CTIRへは連絡できます。これは、シスコのインシデント対応サービスのリテーナを組織に持たない限り、60,000ドルから始まる有料サービスです。契約が結ばれたら、サービスに関する追加情報を提供し、インシデントのケースをオープンします。また、プロセスに関する追加のガイダンスを提供できるように、シスコのアカウントマネージャにフォローアップすることをお勧めします。

関連記事

- Windows FireAMP
- FireAMP