先进的恶意软件保护(安培)错误检测、爆发和事件响应的使用

目录

简介

我们总是努力改进和扩展我们先进的恶意软件保护(安培)技术的威胁智力，然而，如果您的安培解决方案没有触发戒备也没有不正确触发戒备，您能采取一些行动防止任何另外影响到您的环境。本文在那些操作项提供一个指南。

说明

即时动作

如果相信您的安培解决方案没有保护您的网络免受威胁，请立即采取以下行动：

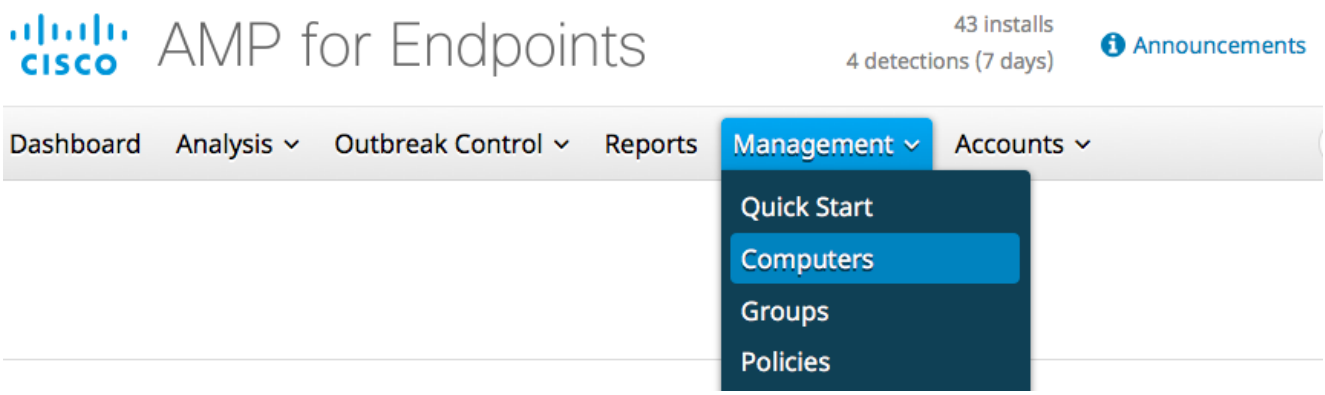
1. 查出从网络的其余的可疑机器。这能包括关闭机器或者物理断开它从网络。
2. 写下关于传染，例如，时候，当机器也许被传染，用户活动在可疑机器等等的重要信息。

   警告： 请勿消除也请勿再镜像机器。它在法庭调查或故障排除流程中排除查找触犯的软件或文件的机会。

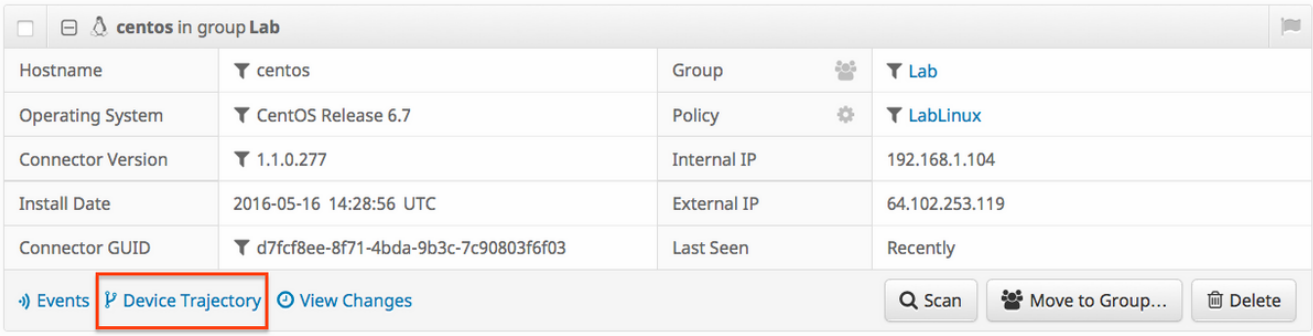
分析

1. 请使用**设备弹道**功能开始您自己的调查。设备弹道能够近似存储9百万个多数最近文件事件。终点设备弹道的安培为搜寻文件是非常有用的或那导致传染的进程。

   在显示板，请连接到**Management>计算机**。



查找可疑机器并且扩展该机器的记录。点击**设备弹道**选项。



2. 如果查找任何可疑文件或切细，请添加它到您的自定义检测列表。终端的安培能使用一张自定义检测列表对待文件或切细如有恶意。这是一个巨大方式提供临时的覆盖防止进一步影响。

分析用Cisco

1. 为动态分析提交所有可疑示例。 您能从**分析>文件分析**手工提交他们在显示板。终端的安培包括生成文件工作情况报告从威胁网格的动态分析功能。在需要情况下，这也有提供文件的好处给Cisco由我们的研究小组的另外的分析。

2. 如果怀疑在您的网络的任何*错误肯定*或*假攻击*检测，我们建议您利用您的安培产品的自定义黑色列表或白色列表功能。当您与Cisco技术支持中心(TAC)联系时，为分析请提供以下信息：文件的SHA256无用数据。文件的若可能复制。关于文件的信息例如来自的地方，并且为什么需要在环境里。解释您为什么认为此是错误肯定或假攻击。
3. 如果需要援助缓和威胁或执行专门化创建行动方案，研究受感染的机器和利用先进的工具或功能缓和活动爆发您的环境的会审，您将需要从事Cisco安全事件响应服务(CSIRS)小组。
Note:Cisco技术支持中心(TAC)不提供援助此种订婚。CSIRS小组可以通过呼叫此电话号码enagaged ：+1-844-831-7715.除非您的组织有事件响应服务的定位器从Cisco，这是开始在$60,000的一项有偿的服务。一旦从事他们将提供关于他们的服务的其他信息并且开您的事件的一个Case。我们也推荐进一步进行您的Cisco Account管理器，以便他们在进程能提供另外的指导。

相关条款

- WindowsFireAMP
- FireAMP