Trabajando con las detecciones falsas de la protección de Malware (AMP), los brotes, y la respuesta avanzados del incidente

Contenido

Introducción

Nos esforzamos siempre mejorar y ampliar la inteligencia de amenaza para nuestra tecnología avanzada de la protección de Malware (AMP), sin embargo si su solución AMP no accionó una alerta ni accionó una alerta erróneamente, usted puede tomar algunas medidas para prevenir cualquier impacto más otro a su entorno. Este documento proporciona una directriz sobre esos elementos de acción.

Descripción

Acciones inmediatas

Si usted cree que su solución AMP no protegió su red contra una amenaza, tome medidas siguientes inmediatamente:

1. Aísle las máquinas sospechosas del resto de la red. Esto podía incluir apagar la máquina, o la desconexión de ella de la red físicamente.
2. Anote la información importante sobre la infección, por ejemplo, el tiempo cuando la máquina pudo ser infectada, las actividades del usuario en las máquinas sospechosas, el etc.

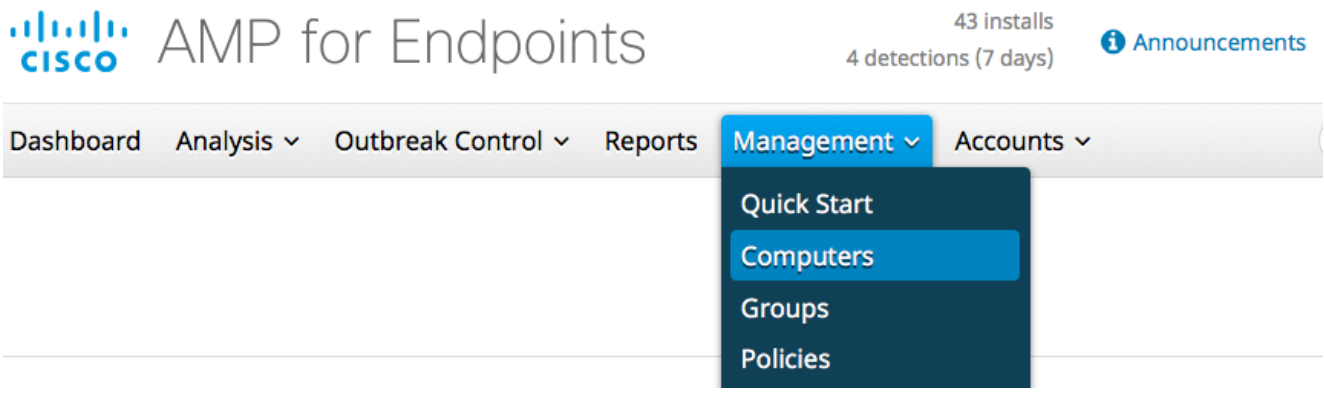
   Advertencia: No limpie hacia fuera o nueva imagen la máquina. Elimina las ocasiones de encontrar el software o los archivos que ofenden durante la investigación o el proceso de Troubleshooting forense.

Análisis

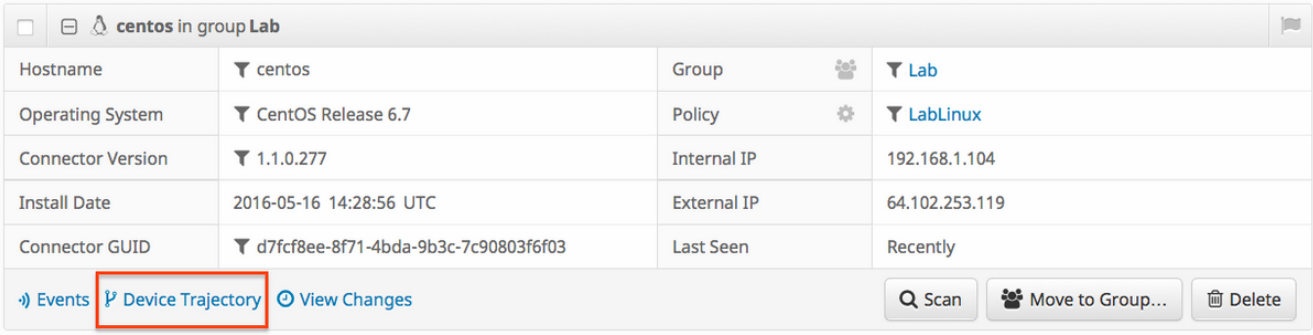
1. Utilice la característica de la **trayectoria del dispositivo** para comenzar su propia investigación. La trayectoria del dispositivo es capaz de salvar aproximadamente 9 millones de la mayoría de eventos del archivo reciente. El AMP para la trayectoria del dispositivo de los puntos finales es muy útil para rastrear los archivos o los procesos que eso llevó a una

infección.

En el panel, navegue a la **Administración > a las Computadoras**.



Encuentre la máquina sospechosa y amplíe el expediente para esa máquina. Haga clic en la opción de la **trayectoria del dispositivo**.



2. Si usted encuentra algún archivo o hash sospechoso, agreguelo a sus listas de encargo de la detección. El AMP para los puntos finales puede utilizar una lista de encargo de la detección para tratar un archivo o un hash como malévolo. Esto es una gran manera de proporcionar la cobertura transitoria para prevenir el impacto adicional.

Análisis por Cisco

1. Someta cualquier muestra sospechosa para la análisis dinámico. Usted puede someterla manualmente del **análisis > del análisis del archivo** en el panel. El AMP para los puntos finales incluye las funciones de la análisis dinámico que generan un informe del comportamiento del archivo de la rejilla de la amenaza. Esto también tiene la ventaja de proporcionar al archivo a Cisco en caso que el análisis adicional de nuestro equipo de investigación se requiera.

2. Si usted sospecha cualesquiera detecciones del *falso positivo* o de la *negativa falsa* en su red, aconsejamos que usted leverage las funciones negras de encargo de la lista o de la lista del blanco para sus Productos AMP. Cuando usted entra en contacto el Centro de Asistencia Técnica de Cisco (TAC), proporcione la siguiente información para el análisis:El hash SHA256 del archivo.Una copia del archivo si es posible.Información sobre el archivo tal como de donde vino y de porqué necesita estar en el entorno.Explique porqué usted cree esto para ser un falso positivo o una negativa falsa.
3. Si usted necesita la ayuda que atenúa una amenaza o que realiza la clasificación de su entorno, usted necesitará contratar al equipo de los servicios de la respuesta del incidente

del Cisco Security (CSIRS) que se especialice en crear los planes de acción, la investigación de los equipos infectados, y leveraging las herramientas o las características avanzadas para atenuar un brote activo.
Note: El Centro de Asistencia Técnica de Cisco (TAC) no proporciona la ayuda con este tipo de compromiso.El equipo CSIRS puede enagaged llamando este número de teléfono: +1-844-831-7715. Esto es un servicio pagado que comienza en $60,000 a menos que su organización tenga un criado para los servicios de la respuesta del incidente de Cisco. Una vez que están enganchados proporcionan la información adicional sobre sus servicios y abren un caso para su incidente. También recomendamos el seguir con su Cisco Account Manager de modo que puedan proporcionar la dirección adicional en el proceso.

Artículos relacionados

- Colección de datos diagnósticos de un conector de FireAMP que se ejecuta en Windows
- Tipos de archivo que son analizados por el conector de FireAMP