[Externa]: Trabajar con protección frente a malware avanzado (AMP), detección de errores, brotes y respuesta ante incidentes

Contenido

Introducción

Siempre nos esforzamos por mejorar y ampliar la inteligencia de amenazas de nuestra tecnología de protección frente a malware avanzado (AMP). Sin embargo, si su solución de AMP no activa una alerta o la activa por error, puede tomar algunas medidas para evitar cualquier impacto adicional en su entorno. Este documento proporciona una directriz sobre esos elementos de acción.

Descripción

Acciones inmediatas

Si cree que su solución de AMP no protegía su red de una amenaza, lleve a cabo las siguientes acciones inmediatamente:

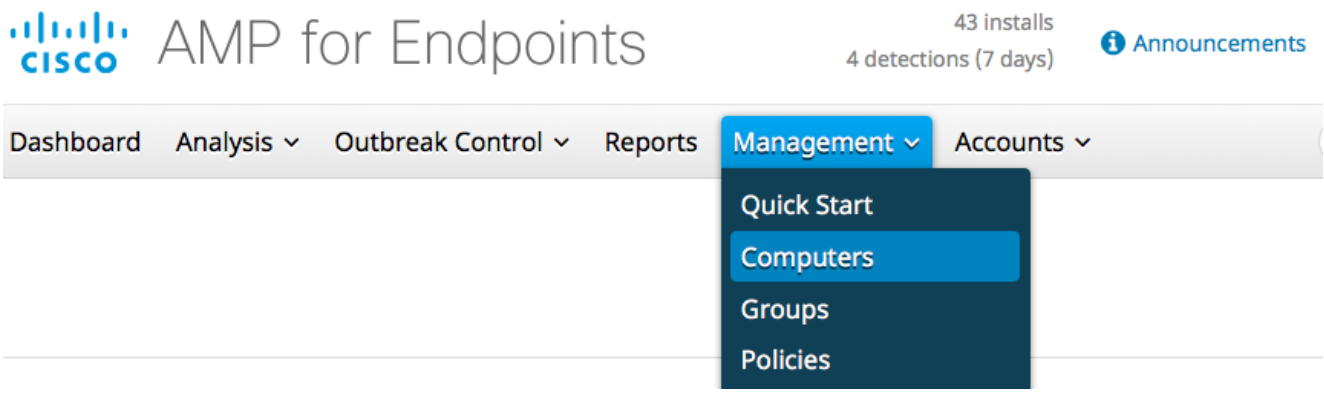
1. Aísle las máquinas sospechosas del resto de la red. Esto podría incluir apagar la máquina o desconectarla físicamente de la red.
2. Anote la información importante sobre la infección, como el momento en que la máquina puede estar infectada, las actividades del usuario en las máquinas sospechosas, etc.

Advertencia: No elimine ni vuelva a crear imágenes de la máquina. Elimina las posibilidades de encontrar el software o los archivos infractores durante la investigación forense o el proceso de resolución de problemas.

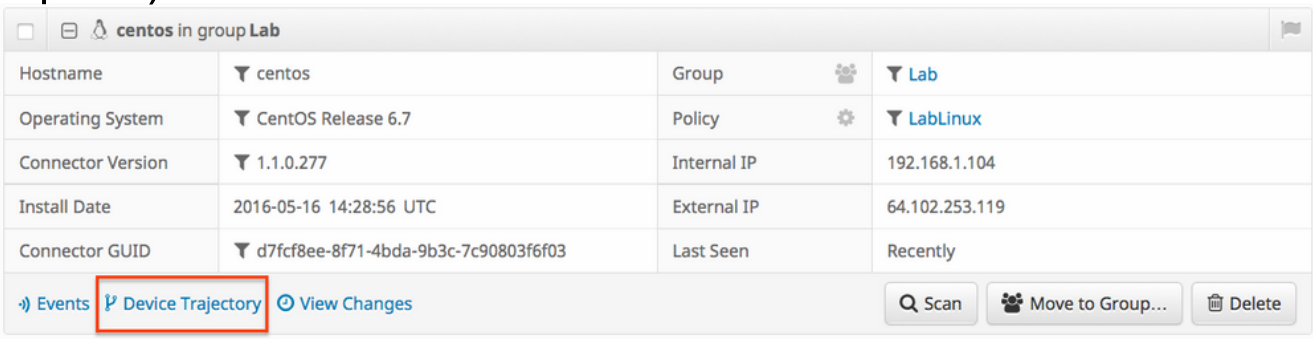
Análisis

1. Utilice la función **Trayectoria del dispositivo** para iniciar su propia investigación. La trayectoria de dispositivos es capaz de almacenar aproximadamente los 9 millones de eventos de archivos más recientes. La trayectoria de los dispositivos de AMP para terminales es muy útil para rastrear los archivos o procesos que condujeron a una infección.

En el panel, vaya a **Administración > Equipos**.



Encuentre la máquina sospechosa y expanda el registro para esa máquina. Haga clic en la opción **Device Trajectory (Trayectoria del dispositivo)**.



2. Si encuentra algún archivo sospechoso o hash, agréguelo a las listas de detección personalizadas. AMP para terminales puede utilizar una lista de detección personalizada para tratar un archivo o hash como malicioso. Se trata de una forma excelente de proporcionar una cobertura integral para evitar nuevos efectos.

Análisis de Cisco

1. Envíe las muestras sospechosas para su análisis dinámico. Puede enviarlos manualmente desde **Análisis > Análisis de archivos** en el panel. AMP para terminales incluye la funcionalidad de análisis dinámico que genera un informe del comportamiento del archivo desde Threat Grid. Esto también tiene la ventaja de proporcionar el archivo a Cisco en caso de que se requiera un análisis adicional por parte de nuestro equipo de investigación.

2. Si sospecha que se han detectado *falsos positivos* o *falsos negativos* en su red, le recomendamos que utilice la funcionalidad de lista blanca o lista negra personalizada para sus productos AMP. Cuando se ponga en contacto con el Cisco Technical Assistance Center (TAC), proporcione la siguiente información para su análisis:El hash SHA256 del archivo.Una copia del archivo si es posible.Información sobre el archivo como de dónde procede y por qué debe estar en el medio ambiente.Explique por qué cree que esto es falso positivo o falso negativo.
3. Si necesita ayuda para mitigar una amenaza o realizar una evaluación de su entorno, deberá ponerse en contacto con el equipo de respuesta ante incidentes de Cisco Talos (CTIR), que se especializa en la creación de planes de acción, la investigación de máquinas infectadas y el aprovechamiento de herramientas o funciones avanzadas para mitigar un brote activo.

Nota: El centro de asistencia técnica Cisco Technical Assistance Center (TAC) no proporciona asistencia con este tipo de compromiso.Se puede ponerse en contacto con el CTIR aquí. Se trata de un servicio de pago que comienza por 60 000 $ a menos que su organización disponga de un anticipo para los servicios de respuesta ante incidentes de Cisco. Una vez contactados, proporcionarán información adicional sobre sus servicios y abrirán un caso para su incidente. También le recomendamos que realice un seguimiento con su Cisco Account Manager para que puedan proporcionar orientación adicional sobre el proceso.

Artículos relacionados

- Recopilación de datos de diagnóstico de un conector de FireAMP que se ejecuta en Windows
- Tipos de archivo escaneados por el conector de FireAMP