**Evaluación del ejemplo**



Compara el ejemplo con tu actividad completada. Revisa tu trabajo utilizando cada uno de los criterios del modelo. ¿Qué hiciste bien? ¿En qué aspectos podrías mejorar? Las respuestas a estas preguntas te servirán como guía a medida que avances en el curso.

***Nota:*** *El ejemplo representa una de las muchas formas posibles de realizar esta actividad. Es probable que el tuyo difiera según los IoC que hayas identificado y catalogado. Lo importante es que tu actividad capture algunos detalles de la investigación del hash del archivo, incluidos los IoC relacionados y la verificación del archivo como malicioso.*



**Paso 1**: El ejemplo proporciona un resumen claro y breve del hash del archivo al utilizar la información que se encuentra en la pestaña **Detection (Detección)**. La **puntuación de la comunidad (Community Score)** y el **análisis de los proveedores de seguridad** enumerados en el informe de VirusTotal proporcionan información sobre el archivo. Más de cincuenta proveedores de seguridad han marcado este archivo como malicioso. Además, varios proveedores han categorizado el archivo como malware Flagpro, un software malicioso que varios agentes de amenazas avanzadas utilizan.

**Paso 2**: El ejemplo también identifica tres tipos diferentes de IoC mediante el uso del informe VirusTotal. La información que se encuentra en las pestañas **Relations (Relaciones)** y **Details (Detalles)** te permitirá encontrar IoC adicionales que están relacionados con el archivo, como un nombre de dominio, una dirección IP y un valor hash.

* **Nombres de dominio**: org.misecure.com se informa como un dominio malicioso contactado en la pestaña Relations (Relaciones) en el informe de VirusTotal.
* **Dirección IP**: 207.148.109.242 aparece como una de las muchas direcciones IP en la pestaña Relations (Relaciones) del informe de VirusTotal.
* **Valor de hash:** 287d612e29b71c90aa54947313810a25 es un hash MD5 que aparece en la pestaña Details (Detalles) del informe de VirusTotal.

**Conclusiones clave**

En esta actividad, determinaste que un archivo era malicioso utilizando la información de un informe de VirusTotal. También identificaste indicadores de compromiso adicionales que están asociados con este archivo. Como analista de seguridad, utilizarás herramientas de investigación como VirusTotal para acceder a la inteligencia sobre amenazas de la comunidad de ciberseguridad mundial. Esto podrá ayudarte a agregar contexto a las investigaciones y aprender más sobre las amenazas al momento de investigar un posible incidente de seguridad.