**Resumen de la actividad**

En esta actividad, analizarás un artefacto utilizando VirusTotal, así como la recopilación de detalles sobre los indicadores de compromiso asociados, utilizando la Pirámide del dolor.

Anteriormente, se te presentó el concepto de la Pirámide del dolor, la cual se emplea para comprender los distintos tipos de **indicadores de compromiso** (**IoC**). Recuerda, un IoC es una evidencia observable que sugiere signos de un posible incidente de seguridad. La Pirámide del dolor explica la relación entre los IoC y el nivel de dificultad que experimentan los agentes de amenaza cuando los IoC son bloqueados por los equipos de seguridad.

**VirusTotal** es una de las múltiples herramientas que utilizan los analistas de seguridad para identificar y responder a incidentes de seguridad. Se trata de un servicio que permite a cualquier persona analizar archivos, dominios, URLs y direcciones IP sospechosas en busca de contenido malicioso. A través de crowdsourcing, VirusTotal recopila e informa sobre inteligencia de amenazas proveniente de la comunidad global de ciberseguridad. Esto ayuda a los analistas de seguridad a determinar qué IoC han sido reportados como maliciosos. Como analista de seguridad, puedes aprovechar la inteligencia de amenazas compartida para profundizar en el conocimiento sobre las amenazas y contribuir a mejorar las capacidades de detección.

***Nota importante****: Los datos subidos a VirusTotal se compartirán públicamente con toda su comunidad. Ten cuidado con lo que envías y asegúrate de no subir información personal.*

**Escenario**

Revisa el siguiente escenario. Luego, completa las instrucciones paso a paso.

Eres analista de nivel uno del centro de operaciones de seguridad (SOC) en una empresa de servicios financieros. Recibiste una alerta sobre la descarga de un archivo sospechoso en la computadora de un empleado.

Decides investigarla y descubres que el empleado recibió un correo electrónico que contenía un archivo adjunto, con una hoja de cálculo protegida por contraseña. Esta contraseña se proporcionó en el correo electrónico. El empleado descargó el archivo e introdujo la contraseña para abrirlo. Al abrir el archivo, se ejecutó una carga maliciosa en su computadora.

Recuperas el archivo malicioso y creas un hash SHA256. Puede que recuerdes de un curso anterior que una **función hash** es un algoritmo que produce un código que no se puede descifrar. El hashing es un método criptográfico utilizado para identificar de forma exclusiva el malware, actuando como huella dactilar única del archivo.

Ahora, que tienes el hash del archivo, usarás VirusTotal para descubrir otros IoC asociados al archivo.

***Nota***: *Utiliza el diario de gestión de incidentes que iniciaste en* [*una actividad anterior*](https://www.coursera.org/learn/haz-sonar-la-alarma-deteccion-y-respuesta/exam/ghRgc/actividad-documenta-un-evento-en-un-diario-de-gestion-de-incidentes) *para tomar notas y hacer un seguimiento de tus hallazgos.*

***Nota****: Puede que recuerdes haber creado hashes SHA256 en la* [*actividad de lab sobre valores hash*](https://www.coursera.org/learn/haz-sonar-la-alarma-deteccion-y-respuesta/ungradedLti/TEDBX/actividad-analiza-tu-primer-paquete) *de un curso anterior.*

**Instrucciones paso a paso**

Sigue las instrucciones para completar la actividad. Luego, dirígete al siguiente elemento del curso para comparar tu trabajo con un ejemplo terminado.

**Paso 1: Accede a la plantilla**

Para utilizar la plantilla de este elemento del curso, haz clic en el enlace de abajo y selecciona “Usar plantilla”.

Enlace a la plantilla: [Pirámide del dolor](https://docs.google.com/presentation/d/1thqW6AhQk1kZbBFqILaZyDoWZbXu3A52Y9-9OOwFVEQ/template/preview?usp=sharing&resourcekey=0-owOdAXKrV-nSNmAO3I2Ulw)

O BIEN

Si no tienes una cuenta de Google, puedes descargar la plantilla directamente desde el siguiente archivo adjunto.

[Activity Investigate a suspicious file hash\_Pyramid-of-Pain](https://d3c33hcgiwev3.cloudfront.net/lY4fgicKTOiuLCqSRsdWPw_f619e56cd2ad460091bc5028fe2cbff1_Activity-Investigate-a-suspicious-file-hash_Pyramid-of-Pain.pptx?Expires=1708732800&Signature=RcBTX35EZ0~yJB~GEkhfJ9q~1zw0oU7OrbB5Rbd9H1wao4Nu5Ox~lmooP58zyEstwxgYQNm0XSdbnzi6bzVLkaj3~YpUDkA3jRDm7zoYU4jEte10PX55ZiQdImRpo0I-X3y2VgDa6JADk~mwAzes60BJl9qZIN0M7ufV4uuSK1k_&Key-Pair-Id=APKAJLTNE6QMUY6HBC5A" \t "_blank)

[PPTX File](https://d3c33hcgiwev3.cloudfront.net/lY4fgicKTOiuLCqSRsdWPw_f619e56cd2ad460091bc5028fe2cbff1_Activity-Investigate-a-suspicious-file-hash_Pyramid-of-Pain.pptx?Expires=1708732800&Signature=RcBTX35EZ0~yJB~GEkhfJ9q~1zw0oU7OrbB5Rbd9H1wao4Nu5Ox~lmooP58zyEstwxgYQNm0XSdbnzi6bzVLkaj3~YpUDkA3jRDm7zoYU4jEte10PX55ZiQdImRpo0I-X3y2VgDa6JADk~mwAzes60BJl9qZIN0M7ufV4uuSK1k_&Key-Pair-Id=APKAJLTNE6QMUY6HBC5A" \t "_blank)

**Paso 2: Revisa los datos de la alerta**

La siguiente información contiene datos sobre la alerta que te ayudarán a completar esta actividad. Estos incluyen un hash de archivo y una línea de tiempo del evento. Guarda estos detalles como referencia para los pasos que aparecen a continuación.

**Hash de archivo SHA256:** 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b

He aquí una línea de tiempo de los acontecimientos que llevaron a esta alerta:

* **1:11 p.m.:** Un empleado recibe un correo electrónico que contiene un archivo adjunto.
* **1:13 p.m.:** El empleado descarga y abre el archivo.
* **1:15 p.m.:** Se crean varios archivos ejecutables no autorizados en la computadora del empleado.
* **1:20 p.m.:** Un sistema de detección de intrusos detecta los archivos ejecutables y envía una alerta al SOC.

Paso 3: Introduce el hash del archivo en VirusTotal

Dirígete al [sitio web de VirusTotal](https://www.virustotal.com/). Haz clic en **SEARCH (BUSCAR)**, ingresa el hash del archivo SHA256 en el cuadro de búsqueda y presiona Intro. El hash de archivo SHA256 aparece en el Paso 2 de esta actividad.

***Nota****: Para completar esta actividad, te enfocarás en evaluar los resultados de VirusTotal. Sin embargo, ninguna herramienta puede detectar todos los tipos de actividad maliciosa. Los analistas de seguridad suelen utilizar una combinación de otras herramientas para evaluar cuidadosamente los resultados de un análisis antes de tomar una decisión sobre el archivo.*

Paso 4: Analiza el informe de VirusTotal

Una vez que hayas recuperado el informe de VirusTotal sobre el hash del archivo, tómate un tiempo para examinar los detalles. Puedes empezar explorando las siguientes pestañas:

1. **Detección:** Esta pestaña proporciona una lista de proveedores de seguridad externos y sus veredictos sobre un artefacto. Los veredictos de detección incluyen categorías como malicioso, sospechoso e inseguro, entre otros. Presta atención cuántos proveedores de seguridad han reportado este hash como malicioso y cuántos no lo han hecho.
2. **Datos**: Esta pestaña ofrece información adicional obtenida a través de un análisis estático del IoC. Observa los hashes adicionales asociados a este malware, como MD5, SHA-1 y otros.
3. **Relaciones**: Aquí encontrarás información sobre las conexiones de red que este malware ha establecido con URL, nombres de dominio y direcciones IP. La columna **Detecciones** indica cuántos proveedores han señalado la URL o la dirección IP como maliciosa.
4. **Comportamiento**: Esta sección proporciona datos relacionados con la actividad observada y los patrones de comportamientos observados de un artefacto después de ejecutarlo en un entorno controlado, como un entorno sandbox. Un entorno sandbox es un entorno aislado que permite que un archivo sea ejecutado y observado por analistas e investigadores. Aquí se presentan detalles sobre las acciones específicas que el archivo lleva a cabo al ejecutarse en este entorno, como operaciones en el registro y sistema de archivos, procesos, y más. Observa los diferentes tipos de tácticas y técnicas empleadas por este malware y los archivos que creó.

***Consejo profesional****: Los informes del entorno sandbox son útiles para comprender el comportamiento de un archivo, pero pueden contener información que no es relevante para su análisis. De forma predeterminada, VirusTotal muestra todos los informes de sandbox en la pestaña Comportamiento. Puedes seleccionar informes individuales para verlos. Esto es útil porque puedes ver las similitudes y diferencias entre los informes para que sea más fácil identificar qué comportamientos es probable que estén asociados con el archivo.*

Paso 5: Determina si el archivo es malicioso

Revisa el informe de VirusTotal para determinar si el archivo es malicioso. Te será útil revisar las siguientes secciones antes de arribar a una conclusión:

* El **ratio** **de proveedores** es el widget métrico que aparece en la parte superior del informe. Este número representa la cantidad total de proveedores de seguridad que han marcado el archivo como malicioso. Un archivo con un número elevado de marcas tiene más probabilidades de ser malicioso.
* El **puntaje** **de la comunidad** se basa en los aportes colectivos de la comunidad de VirusTotal. Este puntaje se encuentra debajo del ratio de proveedores y se puede visualizar colocando el cursor sobre la **X** roja. Un archivo con un puntaje de comunidad negativo tiene más probabilidades de ser malicioso.
* En la pestaña **Detección**, la sección **Análisis de proveedores de seguridad** proporciona una lista de detecciones de este archivo realizadas por proveedores de seguridad, como herramientas antivirus. Los proveedores que *no han* identificado el archivo como malicioso están señalados con una marca de verificación. Los proveedores que *han* marcado el archivo como malicioso están marcados con un signo de exclamación. Los archivos señalados como maliciosos también pueden incluir el nombre del malware detectado y otros datos adicionales sobre el archivo. Esta sección proporciona información sobre la posible malicia de un archivo.

Revisa estas tres secciones para determinar si existe una evaluación consistente de la malicia potencial del archivo, como un ratio de proveedores elevado, un puntaje de la comunidad negativo y detecciones de malware en la sección de análisis de proveedores de seguridad.

En la primera diapositiva de tu **plantilla de Pirámide del dolor**, indica si este archivo es malicioso. A continuación, justifica tu respuesta basándote en tus conclusiones.

***Nota****: El ratio de proveedores se basa en las detecciones de los proveedores de seguridad y es posible que estos no siempre detecten archivos maliciosos. El puntaje de la comunidad se basa en las opiniones y puntos de vista de la comunidad de VirusTotal. Si las puntuaciones de un archivo son bajas, no significa necesariamente que el archivo sea seguro. Se recomienda utilizar múltiples fuentes de información al evaluar los archivos.*

Paso 6: Completa la plantilla con indicadores de compromiso adicionales

Después de explorar las secciones del informe de VirusTotal, descubrirás otros IoC asociados al archivo.

Identifica *tres* **indicadores de compromiso** (**IoC**) asociados a este hash de archivo utilizando las pestañas del informe de VirusTotal. Luego, ingresa los IoC en sus respectivas secciones en la plantilla Pirámide del dolor.

Los indicadores de compromiso son fuentes valiosas de información para los profesionales de la seguridad, ya que se utilizan para identificar actividades maliciosas. Puedes elegir identificar tres de los seis tipos de IoC que se encuentran en la Pirámide del dolor:

* **Valor hash:** Los hash convierten la información en un valor único que no se puede descifrar. Los hash se suelen utilizar como referencias únicas a los archivos involucrados en una intrusión. En esta actividad, utilizaste un hash SHA256 como artefacto para esta investigación. Busca otro hash que se use para identificar este malware e introdúcelo junto a la sección **Valores hash** en la plantilla Pirámide del dolor. Puedes utilizar la pestaña **Datos** para ayudarte a identificar otros hashes.
* **Dirección IP**: Busca una dirección IP con la que haya contactado este malware e introdúcela junto a la sección **Direcciones** **IP** en la plantilla Pirámide del dolor. Puedes localizar direcciones IP en la pestaña **Relaciones**, en la sección Direcciones IP contactadas, o en la pestaña **Comportamiento**, en la sección Tráfico IP.
* **Nombre de dominio:** Busca un nombre de dominio con el que haya contactado este malware e introdúcelo junto a la sección **Nombres de dominio** en la plantilla Pirámide del dolor. Puedes encontrar información sobre nombres de dominio en la pestaña Relaciones. Es posible que encuentres nombres de dominio benignos. Utiliza la columna **Detecciones** para identificar los nombres de dominio que se han notificado como maliciosos.
* **Artefacto de red/artefacto de host:** El malware puede crear artefactos relacionados con la red o con el host en un sistema infectado. Busca un archivo creado por este malware e introdúcelo junto a la sección **Artefactos de red/host** en la plantilla Pirámide del dolor. Puedes encontrar esta información en los informes de sandbox en la pestaña **Comportamiento** o en la pestaña Relaciones.
* **Herramientas:** Los atacantes pueden utilizar herramientas para lograr su objetivo. Intenta averiguar si este malware ha utilizado alguna herramienta. Luego, introdúcela junto a la sección **Herramientas** de la plantilla Pirámide del dolor.
* **Tácticas, técnicas y procedimientos (TTP):** Los TTP describen el comportamiento de un atacante. Usando los informes de sandbox de la pestaña Comportamiento, busca la lista de tácticas y técnicas utilizadas por este malware, según lo identificado por MITRE ATT&CK®, e introdúcela junto a la sección **TTP** en la plantilla Pirámide del dolor.

***Nota***: *Los informes de VirusTotal pueden contener dominios y direcciones IP legítimos que no se consideran maliciosos.*

***Consejo profesional***: *Para conocer más sobre una sección de VirusTotal, coloca el cursor por encima del ícono de información para ver qué incluye esa sección.*

**Qué incluir en tu respuesta**

Asegúrate de incluir los siguientes puntos en la plantilla de la actividad completada:

* Una explicación acerca de si el hash del archivo es malicioso.
* Tres tipos de indicadores de compromiso diferentes.