**Analiza los indicadores de compromiso con herramientas de investigación**

Hasta ahora, has aprendido sobre los diferentes tipos de métodos de detección que se pueden utilizar para detectar incidentes de seguridad. Esta lectura explora cómo se pueden utilizar las herramientas de investigación durante las investigaciones para analizar **indicadores de compromiso (IoC)** sospechosos y crear contexto en torno a las alertas. Recuerda que un IoC es evidencia observable que sugiere indicios de un posible incidente de seguridad.

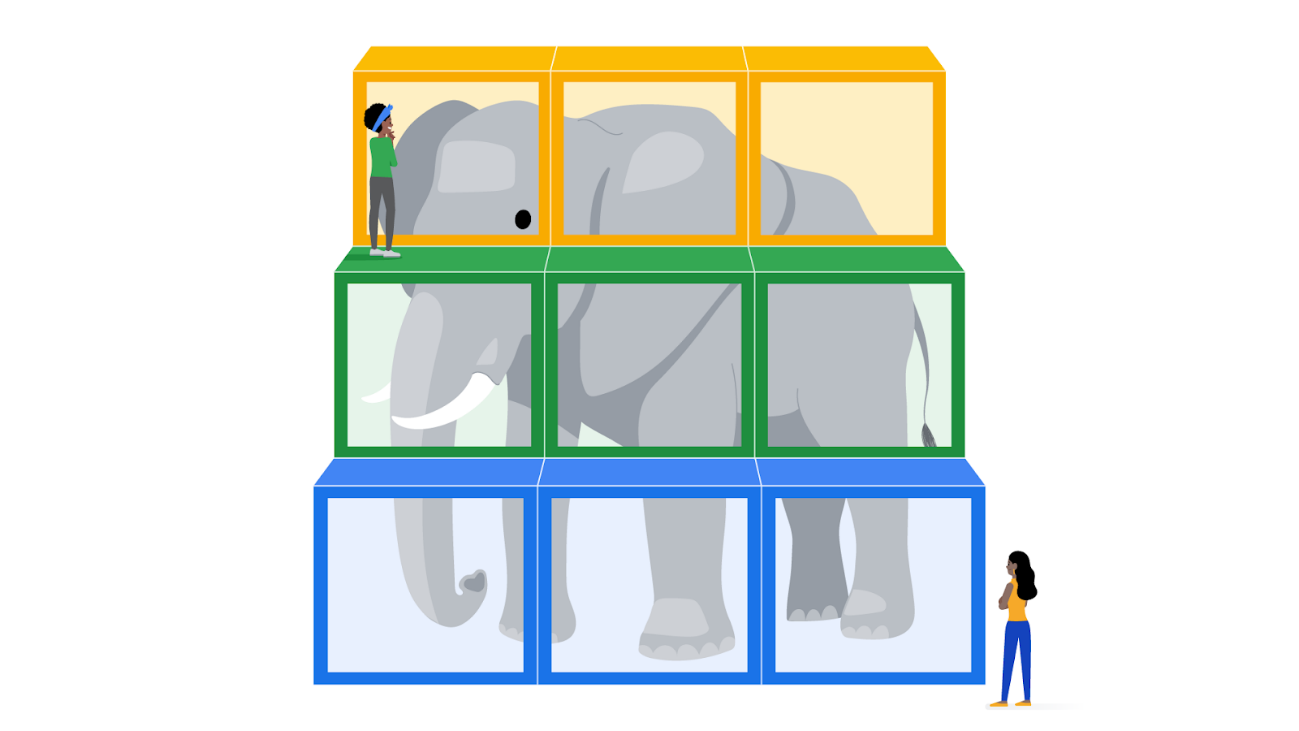
**Agregar contexto a las investigaciones**

Anteriormente, has aprendido sobre la pirámide del dolor, que describe la relación entre los indicadores de compromiso y el nivel de dificultad que experimentan los agentes de amenaza cuando los indicadores de compromiso son bloqueados por los equipos de seguridad. También aprendiste sobre diferentes tipos de IoC pero, como sabes, no todos los IoC son iguales. Los agentes de amenaza pueden lograr evadir la detección y continuar comprometiendo los sistemas aunque su actividad relacionada con los IoC esté bloqueada o limitada.

Por ejemplo, identificar y bloquear una sola dirección IP asociada con una actividad maliciosa no proporciona una visión amplia de un ataque, ni impide que un agente de amenaza continúe su actividad. Centrarse en una sola parte de la evidencia es como fijarse en una sola parte de un cuadro: se pierde el panorama general.



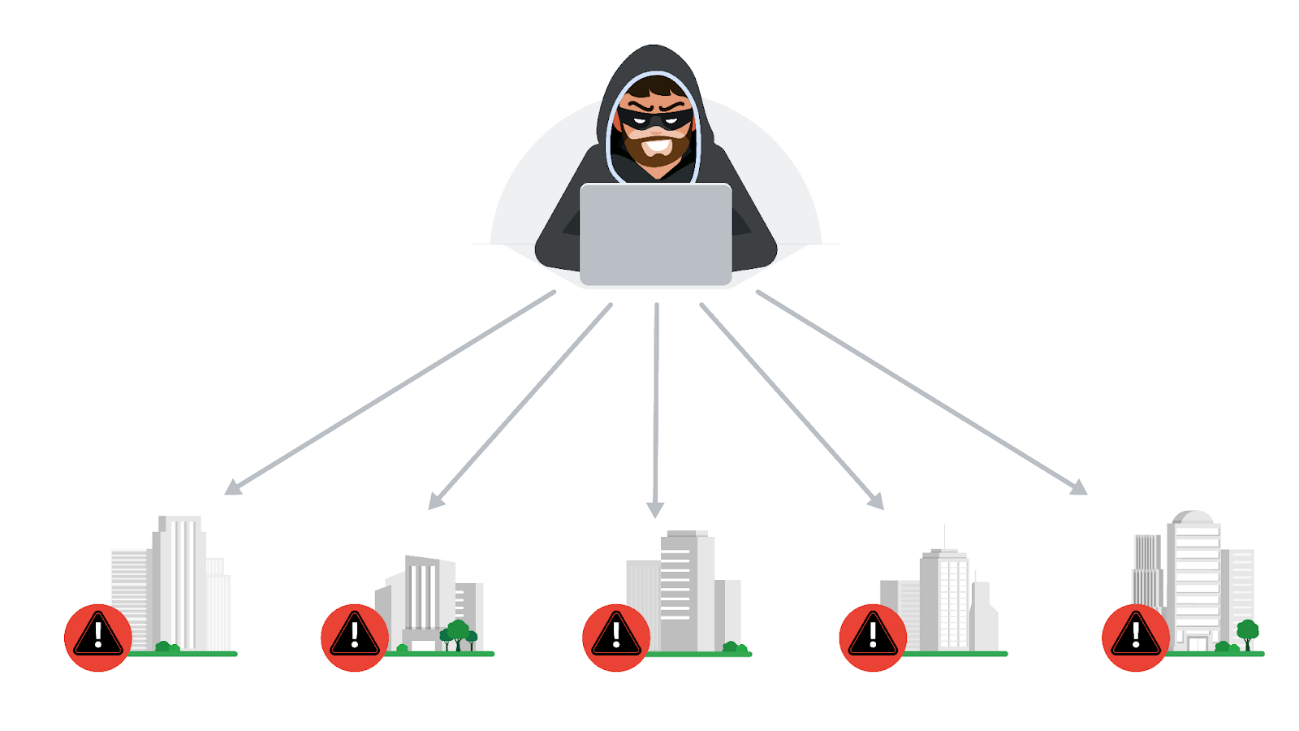
Los analistas de seguridad necesitan expandir el uso de los IoC para poder agregar contexto a las alertas. **La inteligencia sobre amenazas** es la información basada en evidencia que proporciona contexto sobre amenazas existentes o emergentes. Al acceder a información adicional relacionada con los IoC, los analistas de seguridad pueden ampliar su punto de vista para observar el panorama general y construir una narrativa que ayude a informar sus acciones de respuesta.



Al agregar contexto a un IoC, por ejemplo, mediante la identificación de otros artefactos relacionados con la dirección IP sospechosa, como comunicaciones de red dudosas o procesos inusuales, los equipos de seguridad pueden  tener una imagen más concreta de un incidente. Este contexto puede ayudar a los equipos de seguridad a detectar incidentes de seguridad más rápido y adoptar un enfoque más informado en su respuesta.

**El poder del "crowdsourcing" (externalización abierta de tareas)**

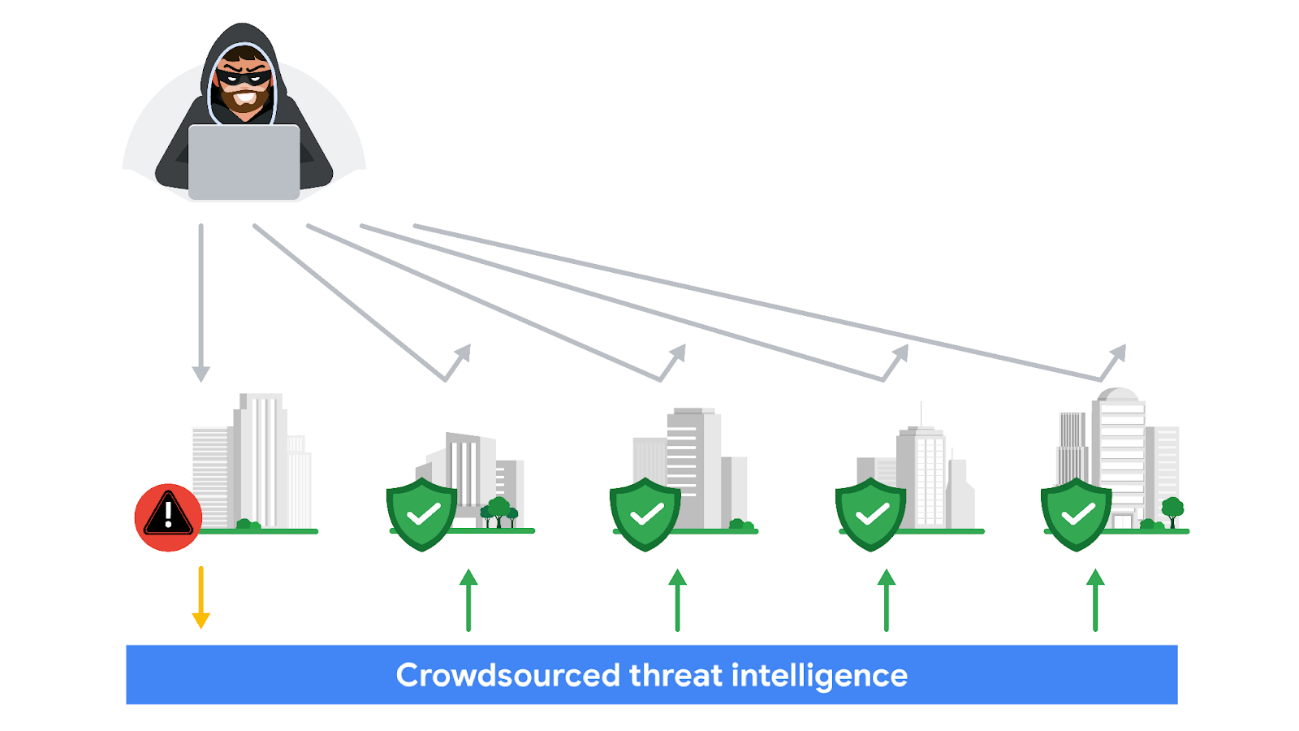
El **crowdsourcing**, también denominado colaboración colectiva, es la práctica de recopilar información utilizando los aportes y la colaboración del público. Las plataformas de inteligencia sobre amenazas lo utilizan para reunir información de la comunidad global de ciberseguridad. Tradicionalmente, la respuesta a incidentes de una organización se realizaba de forma aislada; un equipo de seguridad recibía y analizaba una alerta, y luego procedía a remediarla, sin haber contemplado perspectivas adicionales acerca de cómo abordarla. De esta manera, sin el crowdsourcing, los atacantes podían llevar a cabo los mismos ataques contra distintas organizaciones.



Gracias al crowdsourcing, en cambio, las organizaciones aprovechan los conocimientos de millones de otros profesionales de la ciberseguridad, incluidos, entre otros, los vendedores de productos de ciberseguridad, organismos públicos y proveedores de servicios en la nube. Esta práctica permite a personas y organizaciones de la comunidad de la ciberseguridad mundial compartir y acceder abiertamente a una colección de datos de inteligencia sobre amenazas, lo cual ayuda a mejorar continuamente las tecnologías y metodologías de detección.

Entre los ejemplos de organizaciones de intercambio de información, se encuentran los Centros de Intercambio y Análisis de Información (ISAC), que se centran en recopilar inteligencia sobre amenazas dirigidas a sectores específicos y compartirla con empresas que operan en esos sectores concretos, como pueden ser los de energía o los de salud. Por su parte, la **inteligencia de fuentes abiertas (OSINT)** es la recopilación y análisis de información procedente de fuentes de acceso público para generar inteligencia utilizable. La OSINT también se puede utilizar como método para recopilar información relacionada con agentes de amenaza, amenazas, vulnerabilidades y más.

Estos datos de inteligencia sobre amenazas se utilizan para mejorar los métodos y técnicas de detección de productos de seguridad, como las herramientas de detección o el software antivirus. Por ejemplo, los atacantes suelen realizar los mismos ataques contra múltiples objetivos, con la esperanza de que uno de ellos sea exitoso. Si una organización detecta un ataque y publica inmediatamente los detalles del incidente, como archivos maliciosos, direcciones IP o URL, en herramientas como VirusTotal, esta inteligencia sobre amenazas puede ayudar a otras organizaciones a defenderse contra el mismo ataque.



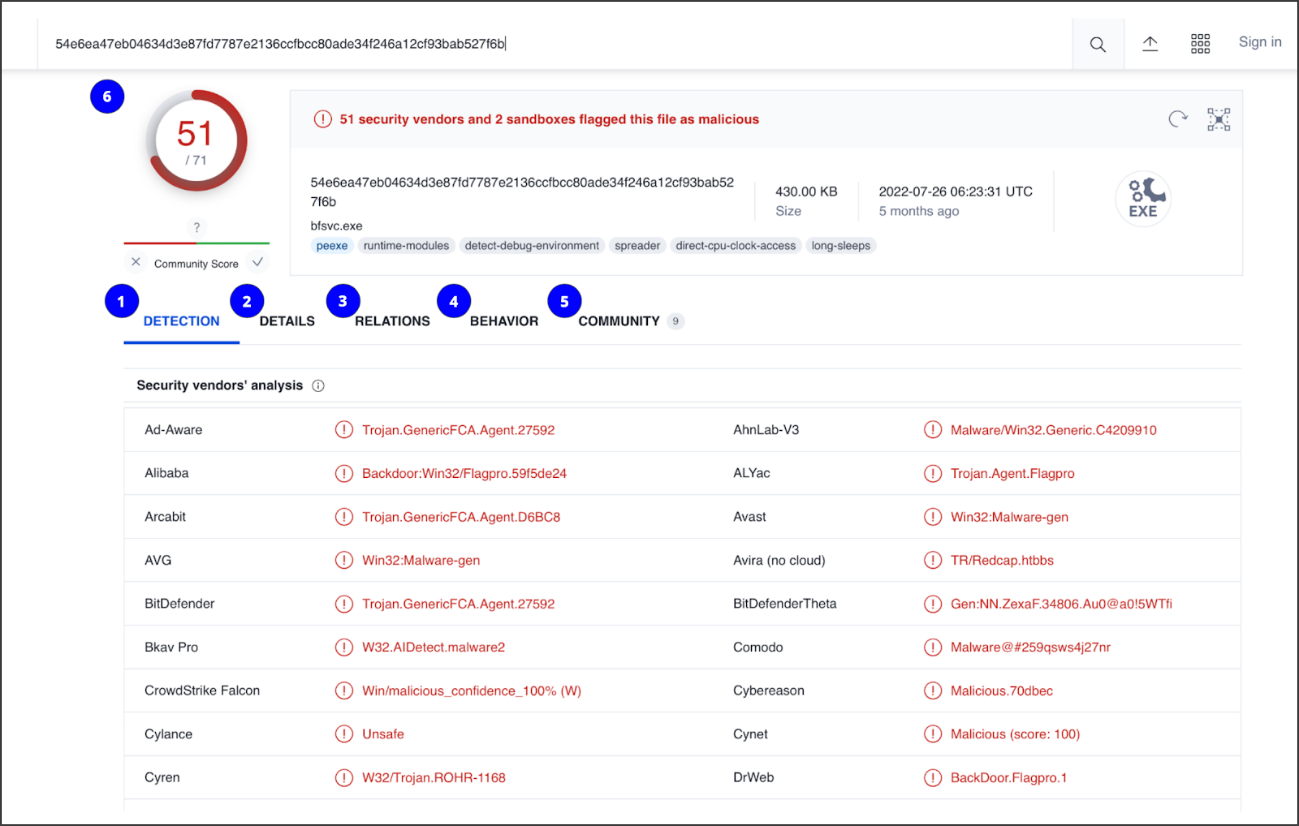
**VirusTotal**

[**VirusTotal**](https://www.virustotal.com/gui/home) es un servicio que permite a cualquier persona analizar archivos, dominios, URL y direcciones IP sospechosos en busca de contenido malicioso. VirusTotal también ofrece servicios y herramientas adicionales para uso empresarial. Esta lectura se centra en el sitio web de VirusTotal, que está disponible para uso gratuito y no comercial.

Esta herramienta se puede utilizar para analizar archivos, direcciones IP, dominios y URL sospechosos, a fin de detectar amenazas de ciberseguridad, como el software malicioso. Los usuarios pueden enviar y verificar artefactos como hashes de archivos o direcciones IP para obtener informes de VirusTotal. Estos proporcionan información adicional sobre si un IoC se considera malicioso o no, cómo ese IoC está conectado a, o relacionado con, otros IoC en el conjunto de datos y más.



Aquí se presenta un desglose del resumen de los informes:



1. **Detection (Detección):** La pestaña Detection proporciona una lista de proveedores de seguridad externos y sus veredictos de detección sobre un IoC. Por ejemplo, los proveedores pueden catalogar su veredicto de detección como malicioso, sospechoso, inseguro, entre otros.
2. **Details (Detalles)**: Esta pestaña proporciona información adicional extraída de un análisis estático del IoC. En esta pestaña se puede encontrar información sobre los distintos hashes, tipos de archivos, tamaños de archivo y encabezados, hora de creación y detalles sobre el primer y último envío.
3. **Relations (Relaciones)**: La pestaña Relations proporciona los IoC relacionados que están conectados de alguna manera a un artefacto, como las URL, dominios, y direcciones IP contactados y los archivos soltados si el artefacto es un ejecutable.
4. **Behavior (Comportamiento)**: La pestaña Behavior contiene información relacionada con la actividad y los comportamientos de un artefacto que se han observado después de ejecutarlo en un entorno controlado, como uno de pruebas (sandbox). Esta información incluye tácticas y técnicas detectadas, comunicaciones de red, acciones de sistemas de registro y archivos, procesos, entre otros.
5. **Community (Comunidad):** La pestaña Community es donde los miembros de la comunidad VirusTotal, como los profesionales de seguridad o los investigadores, pueden dejar comentarios e ideas sobre el IoC.
6. **Vendors’ ratio and community Score (Ratio de proveedores y puntuación de la comunidad)**: La puntuación que se muestra en la parte superior del informe es el ratio de proveedores, que indica cuántos proveedores de seguridad han marcado el IoC como malicioso. Debajo de esta puntuación también figura la de la comunidad, que se basa en los aportes de los usuarios de VirusTotal. Cuantas más detecciones tenga un archivo y mayor sea la puntuación de la comunidad, más probable es que sea malicioso.

**Nota**: Los datos subidos a VirusTotal se compartirán públicamente con toda la comunidad de VirusTotal. Es necesario tener cuidado al enviar información y asegurarse de no subir información personal.

**Otras herramientas**

Existen otras herramientas de investigación que se pueden utilizar para analizar los IoC, que también pueden compartir los datos con la comunidad.

**Jotti's malware scan**

[Jotti's malware scan](https://virusscan.jotti.org/) es un servicio gratuito que te permite analizar archivos sospechosos con varios programas antivirus. Hay algunas limitaciones en cuanto a la cantidad de archivos que se pueden enviar.

**Urlscan.io**

[Urlscan.io](https://urlscan.io/) es un servicio gratuito que escanea y analiza las URL y proporciona un informe detallado que resume la información de la URL.

**CAPE Sandbox**

[CAPE Sandbox](https://capesandbox.com/analysis/) es un servicio de código abierto utilizado para automatizar el análisis de archivos sospechosos. En un entorno aislado, se analizan archivos maliciosos como el malware, cuyo comportamiento se describe en un informe exhaustivo.

**MalwareBazaar**

[MalwareBazaar](https://bazaar.abuse.ch/browse/) es un repositorio gratuito para muestras de software malicioso. Estas muestras son una gran fuente de inteligencia sobre amenazas que se puede utilizar con fines de investigación.

**Conclusiones clave**

Como analista de seguridad, analizarás IoC. Es importante comprender cómo el hecho de agregar contexto a las investigaciones puede ayudar a mejorar las capacidades de detección y tomar decisiones informadas y efectivas.