




Herramientas de inteligencia de código abierto (OSINT) para la prevención del fraude

Tabla de Contenidos

¿Qué es la inteligencia de código abierto (OSINT)?	2
¿Cómo funciona la OSINT?	3
¿Quién utiliza la OSINT?	4
¿Por qué es importante la OSINT?	4
Ventajas de la OSINT	5
Desventajas de la OSINT	5
¿Son legales las investigaciones de OSINT?	6
¿Qué son las herramientas OSINT?	6
¿Qué hace un investigador OSINT?	7
¿Cómo puede ayudar la OSINT en la detección y prevención del fraude?	8
OSINT: Captura de pruebas y toma de notas	13
¿Qué herramientas OSINT están disponibles para la detección y prevención del fraude?	13
Conclusión	15



Cuando uno se inicia en el mundo de la lucha contra el fraude, OSINT es uno de los primeros acrónimos que hay que aprender.

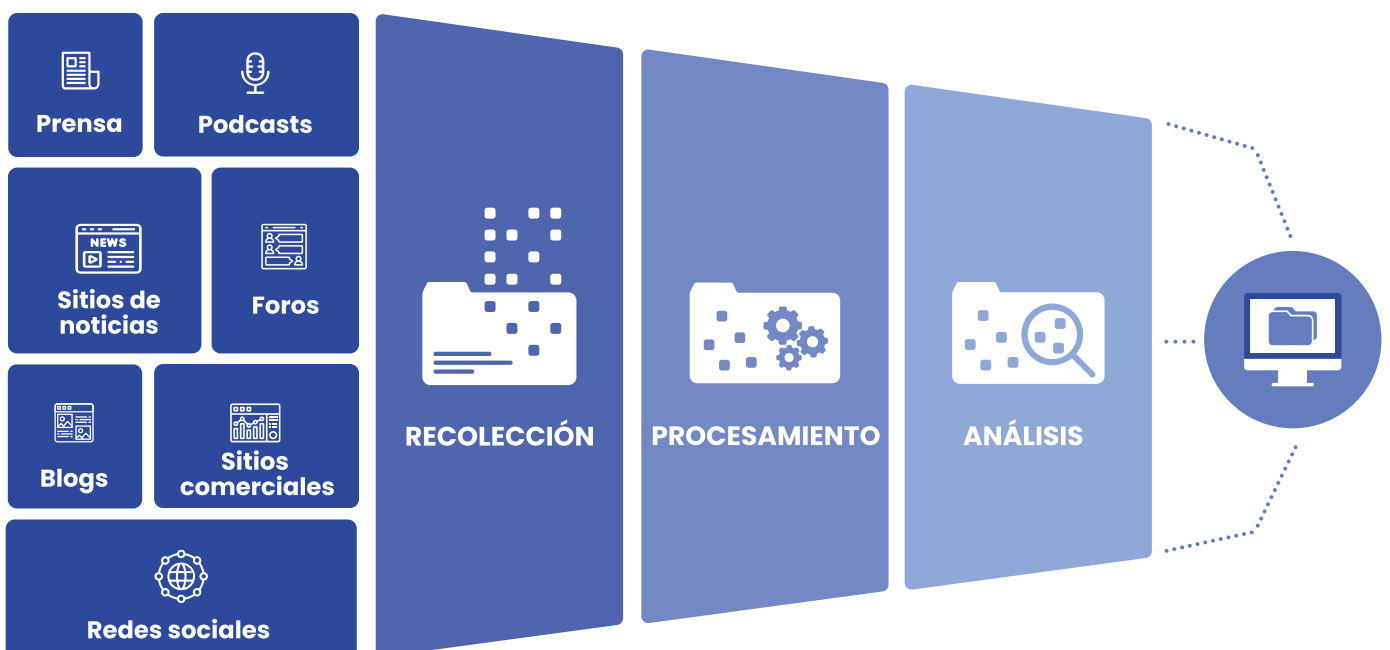
La abreviatura de "Open Source Intelligence" (inteligencia de código abierto) no solo abarca un campo, sino casi una forma de pensar. ¿Cómo utilizamos los datos disponibles públicamente para dar sentido a la situación en cuestión?

Esta guía pretende guiarte a través de los principios básicos de la OSINT, las herramientas de OSINT más comunes que se utilizan, así como consejos comprobados para ayudarte a luchar contra el fraude.

La OSINT se utiliza en una gran variedad de campos, desde la aplicación de la ley hasta la seguridad nacional e incluso la inteligencia empresarial cotidiana.

Hoy en día, la mayoría de las personas que han crecido con internet tienen algunas habilidades de "stalkeo", pero el marco de esta guía es el de la prevención y detección del fraude.

¿Qué es la inteligencia de código abierto (OSINT)?



La inteligencia de código abierto consiste en recopilar los datos disponibles públicamente en internet, las redes sociales y las fuentes tradicionales como la televisión, los periódicos y las revistas, con el fin de evaluar un caso o una situación.

La información adquirida puede abarcar desde textos hasta imágenes, videos y perfiles, que una vez reunidos deben ser procesados, evaluados y almacenados en función del objetivo final del analista.

Como afirma el sitio web de la CIA, “la información no tiene que ser secreta para ser valiosa”.

¿Cómo funciona la OSINT?

Las herramientas OSINT recopilan y agregan información de una serie de fuentes disponibles públicamente, y pueden ayudar a dar una visión más detallada de un usuario o empresa en particular.

La mayoría de las fuentes disponibles públicamente pueden ser utilizadas como OSINT, incluyendo:

| **blogs**

| **foros**

| **sitios de redes sociales**

| **medios de comunicación tradicionales (televisión, radio, publicaciones)**

| **documentos de investigación**

| **registros gubernamentales**

| **revistas académicas**

| **etc.**

En términos de detección y prevención de fraudes, la utilización de la OSINT implica la recopilación de información sobre un determinado cliente o caso para determinar quiénes son, sus intenciones o incluso lo que ha sucedido.

El escenario más común es verificar si el usuario y el titular de la tarjeta son o no la misma persona, pero la OSINT también entra en juego en casos de fraude más complejos en los que hay que analizar entidades (usuarios sospechosos, afiliados y similares).

Estas entidades se denominan comúnmente personas o puntos de interés (POI), un término acuñado originalmente por la CIA.

¿Quién utiliza la OSINT?

La OSINT es utilizada por una variedad de proveedores de soluciones para encontrar más información sobre personas o temas específicos en los que se necesita más inteligencia.

Se suele utilizar en los siguientes campos:

- | **aplicación de la ley**
- | **gestión de riesgos y fraude**
- | **recursos humanos**
- | **ciberseguridad**
- | **operaciones militares**

Desde las empresas que manejan sistemas de entrada y salida de dinero hasta las fuerzas del orden, la OSINT puede apoyar cualquier tipo de investigación.

¿Por qué es importante la OSINT?

Las razones por las que el uso de OSINT es importante están estrechamente relacionadas con el propósito de su uso. Algunos ejemplos pueden ser:

- 1 **identificar las filtraciones de datos;**
- 2 **la diligencia debida del cliente (CDD);**
- 3 **descubrir vulnerabilidades;**

4 respaldar los procesos de toma de decisiones;

5 mantenerse al día con las noticias.

Ventajas de la OSINT

La OSINT puede añadir una capa adicional de seguridad y mejorar tu conocimiento de los usuarios potenciales sin requerir ninguna intervención por su parte, por lo que no afecta al recorrido del usuario.

Esta capa adicional puede ayudar a mejorar tus procesos de toma de decisiones a un costo más económico, ya que muchas herramientas están disponibles de forma gratuita.

Hay muchas más herramientas por ahí, y hemos recogido algunas de ellas en nuestro post sobre las mejores herramientas para OSINT.

Además de esta validación adicional, otra de las principales ventajas de utilizar herramientas OSINT para el análisis de riesgos es que los datos pueden estar en tiempo real o actualizados con frecuencia, ya que la información pública se añade constantemente en línea.

Desventajas de la OSINT

Debido a la naturaleza de la OSINT y al hecho de que esencialmente estás accediendo a la biblioteca pública de internet, filtrar el ruido puede ser bastante agotador.

Sin herramientas especializadas, tu equipo puede pasar fácilmente mucho tiempo examinando miles de piezas de información sin ninguna dirección o propósito real.

No hay muchas herramientas directas que apoyen el análisis de esta información y, sin el apoyo de la inteligencia artificial, la OSINT requiere una gran cantidad de información humana para verificar la información recopilada.

No podemos dejar de insistir en que la OSINT tiene que ser validada. Las fuentes de información deben ser examinadas o, de lo contrario, se puede analizar fácilmente información falsa o sin utilidad.

¿Son legales las investigaciones de OSINT?

La OSINT se basa en datos producidos y disponibles públicamente que pueden ser recogidos y compartidos sin infringir las leyes o políticas, sin necesitar una orden judicial o sin participar en lo que comúnmente se consideraría prácticas sospechosas.

Son perfectamente legales en el contexto de las investigaciones de fraude, aunque la información recopilada y almacenada debe ser manejada de una manera que cumpla con las normas.

En los últimos años, ha cobrado notoriedad la práctica generalizada del “doxing”: desvelar a usuarios anónimos de internet mediante la combinación de información disponible públicamente. Esto puede ser ilegal, dependiendo de lo que se haga con esta información, así como de la legislación local.

¿Qué son las herramientas OSINT?

Las herramientas OSINT abarcan la metodología de adquisición de la información mencionada, es decir, el conocimiento de dónde buscar o qué herramientas utilizar para el trabajo.

Esta distinción es crucial, ya que aunque la mayoría de los sitios web y las plataformas de redes sociales tienen algún tipo de funcionalidad de búsqueda, tratan cierta información (como los correos electrónicos y los números de teléfono) como sensible, y hay que saber dónde buscar para que la búsqueda dé resultados.

A veces esto significa trabajar en contra del algoritmo: Google ordena los resultados de la búsqueda de una manera, pero el uso de operadores de búsqueda especiales permite filtrar el resultado para un determinado tipo de archivo, o solo en un determinado idioma o de dominios específicos.

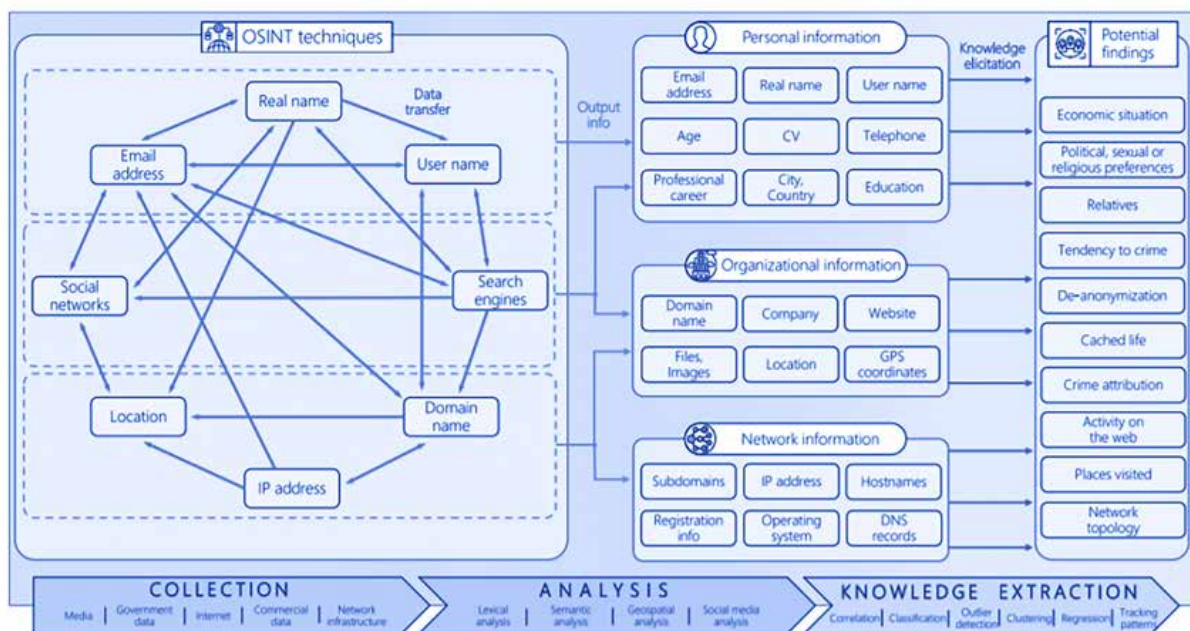
De hecho, es útil utilizar motores de búsqueda diferentes, como DuckDuckGo o Bing, para contrarrestar el sesgo del algoritmo.

Otras consultas requieren motores de búsqueda especializados (como las búsquedas de personas), y existen bases de datos específicas para cada caso (como la base de datos

de correos electrónicos filtrados de haveibeenpwned.com). Muchas de estas fuentes son gratuitas (aunque requieren mucho tiempo), mientras que el software especializado suele ser caro.

Las fuentes incluyen el marco OSINT, mientras que recomendamos Moz.com para dominar los operadores de búsqueda avanzada.

¿Qué hace un investigador OSINT?



Osint tech

Un investigador OSINT es responsable de reunir y analizar la información, así como de extraer conocimientos de sus hallazgos.

Aunque todo el mundo trabaja de forma diferente y cada organización tendrá diferentes protocolos sobre cómo se lleva a cabo exactamente una investigación, normalmente se siguen ciertos marcos.

Recoger información de fuentes abiertas: Siguiendo el mantra de “empieza con lo que sabes o con lo que tienes”, el investigador buscará en sus fuentes información como correos electrónicos, números de teléfono, nombres de usuario, nombres propios, direcciones, etc. para crear un archivo sobre el caso en cuestión.

Filtrado: Muchos de los hallazgos pueden resultar ser erróneos o irrelevantes para la investigación, y deben dejarse de lado para poder realizar las evaluaciones correctas. Trabajar con información errónea conducirá inevitablemente a tomar decisiones equivocadas en un caso.

Análisis de la información: Utilizando la lógica ascendente (o el razonamiento inductivo), el analista o investigador examina los datos y elabora una teoría basada en lo que ve, trabajando para obtener información procesable. Esto puede ir desde algo sencillo (llamar a las cosas por su nombre) hasta descubrir tramas y planes muy elaborados.

Obtención de información: En la fase final, el investigador puede hacer una recomendación sobre lo que hay que hacer con el caso en cuestión, y puede presentar su razonamiento con la información pertinente. Es una buena práctica involucrar a otro investigador en esta fase, para comprobar la posible parcialidad.

En resumen, ¡la inteligencia es análisis **más** información!

Acerca de la seguridad operativa

La seguridad operativa (OpSec) significa estar atento a los rastros que dejas mientras realizas tus actividades. En el contexto de la OSINT, esto significa que debes tener cuidado de no alertar al objetivo de tu investigación.

Dependiendo del sistema utilizado, pueden recibir notificaciones, o tu dirección IP puede aparecer en sus análisis, etc. La mejor práctica es investigar de la forma más anónima posible, utilizando máquinas virtuales si es necesario.

¿Cómo puede ayudar la OSINT en la detección y prevención del fraude?

La OSINT suele asociarse a las **revisiones manuales en la detección de fraudes**, cuando el conjunto de reglas del sistema de prevención de fraude no es suficiente para evaluar correctamente el caso.

Sigue una cierta lógica: El sistema no pudo hacer una evaluación correcta porque las puntuaciones de riesgo se calculan en función de los datos capturados para una acción determinada (o, más comúnmente, una transacción), y es necesario que un humano intervenga y reúna inteligencia adicional.

El otro caso de uso principal es **estar al día de lo que hacen los defraudadores**. Las herramientas OSINT pueden utilizarse para buscar en foros de estafadores o en la dark web para ver qué es lo que está de moda y para qué hay que prepararse.

Aunque la OSINT suele abarcar las 5 preguntas “W” (¿Quién, Qué, Cuándo, Dónde, Por qué y Cómo?), para un analista de fraude la pregunta más típica será “¿Eres realmente quien dices ser?”. La segunda consideración más común es “¿Es demasiado bueno para ser verdad?”. La tercera es: “¿Se ajusta esta persona realmente a nuestro perfil de usuario o cliente?”. Y así sucesivamente.

El problema es que los defraudadores -los mejores, al menos- son adversarios inteligentes y no solo se fijarán en las posibles lagunas de tu sistema, sino también en las tuyas.

Alguien que acaba de adquirir los datos de una tarjeta de crédito robada investigará a su víctima y tratará de hacer coincidir los detalles de la transacción con lo que tú puedas averiguar también sobre la persona, además de utilizar un apoderado que parezca plausible en una comprobación de la distancia de la dirección.

Del mismo modo, un afiliado sospechoso tratará de parecer legítimo, y no es raro que los delincuentes serios encubran sus operaciones con empresas de responsabilidad limitada.

Esto significa que, al recopilar información, hay que tener en cuenta una distinción. Cuando se trata de un fraude, el escenario más común **es que alguien se presente como otra persona**.

La información que se obtiene de los datos proporcionados podría coincidir con la de una persona existente, que podría ser víctima de un robo de identidad o que es una mula de dinero.

La otra mitad del rompecabezas es la información relacionada directamente con el usuario: los metadatos de su dispositivo, la dirección IP, el correo electrónico proporcionado y el número de teléfono.

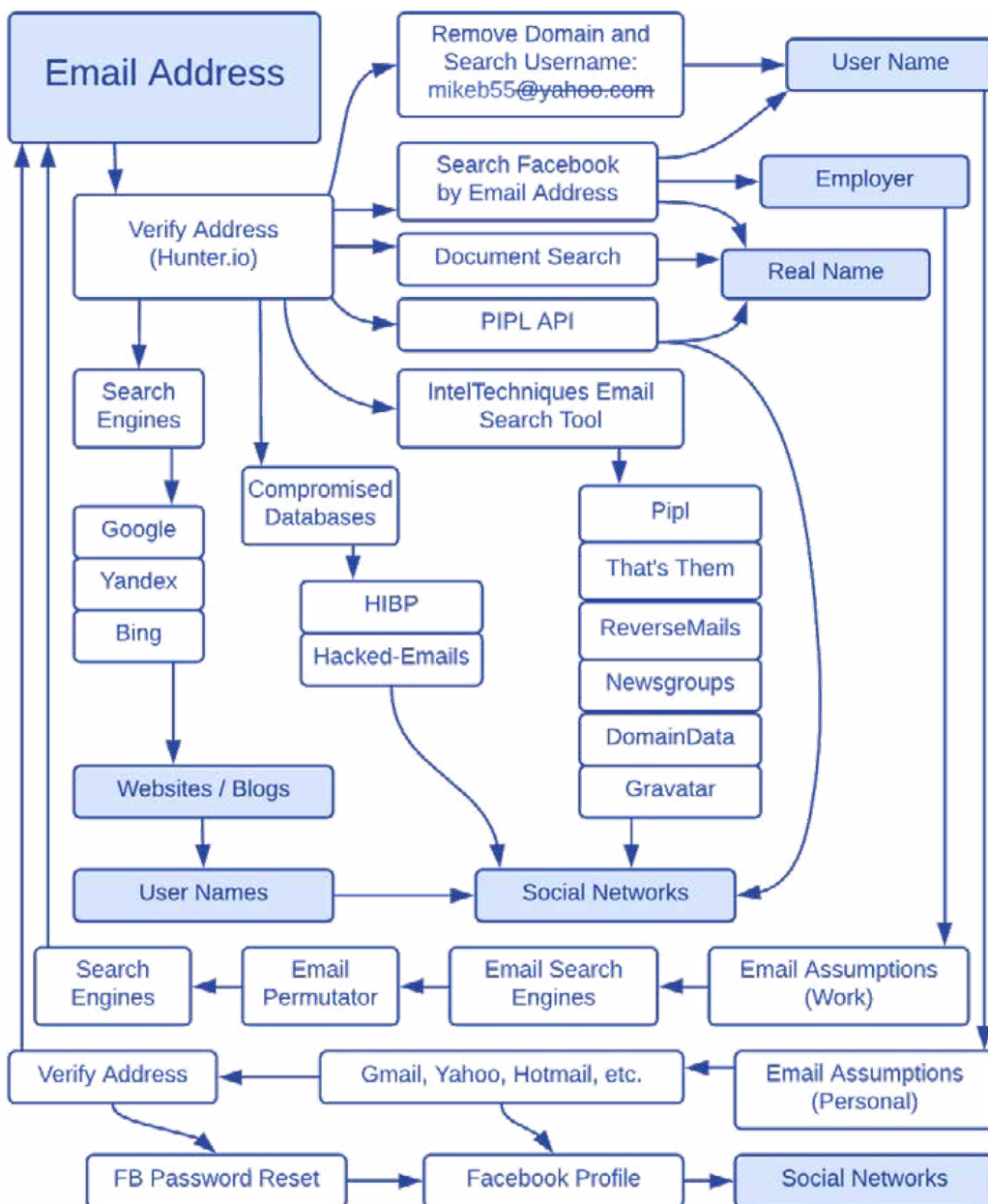
La pregunta que se intenta responder es si las dos mitades están vinculadas entre sí por algo que no sea la transacción o registro que se está viendo.

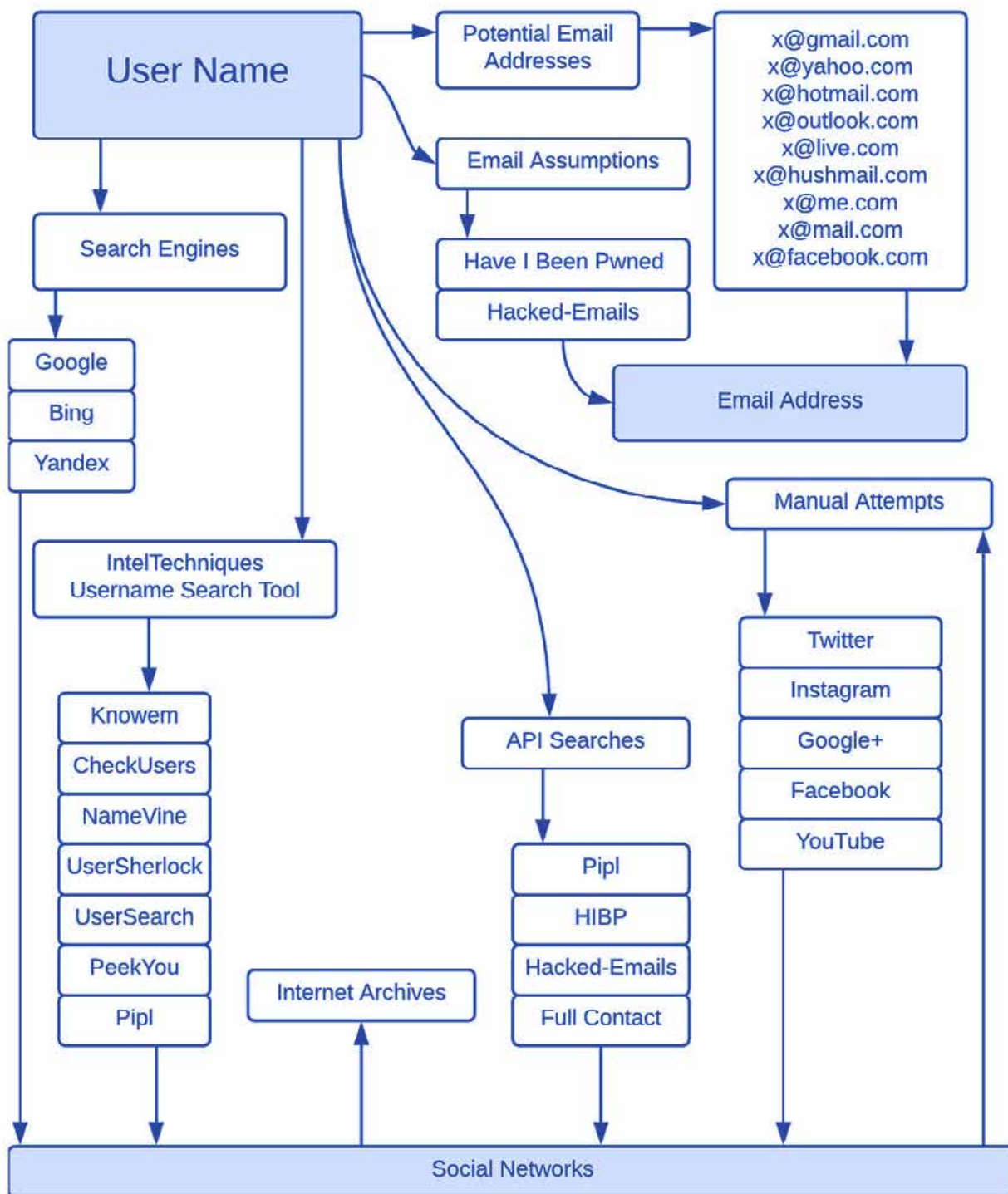
En segundo lugar, mientras que la OSINT trabaja principalmente con información disponible públicamente, aunque sea difícil de encontrar, como gestor de fraudes tienes una gran cantidad de datos internos a tu disposición que pueden ayudarte.

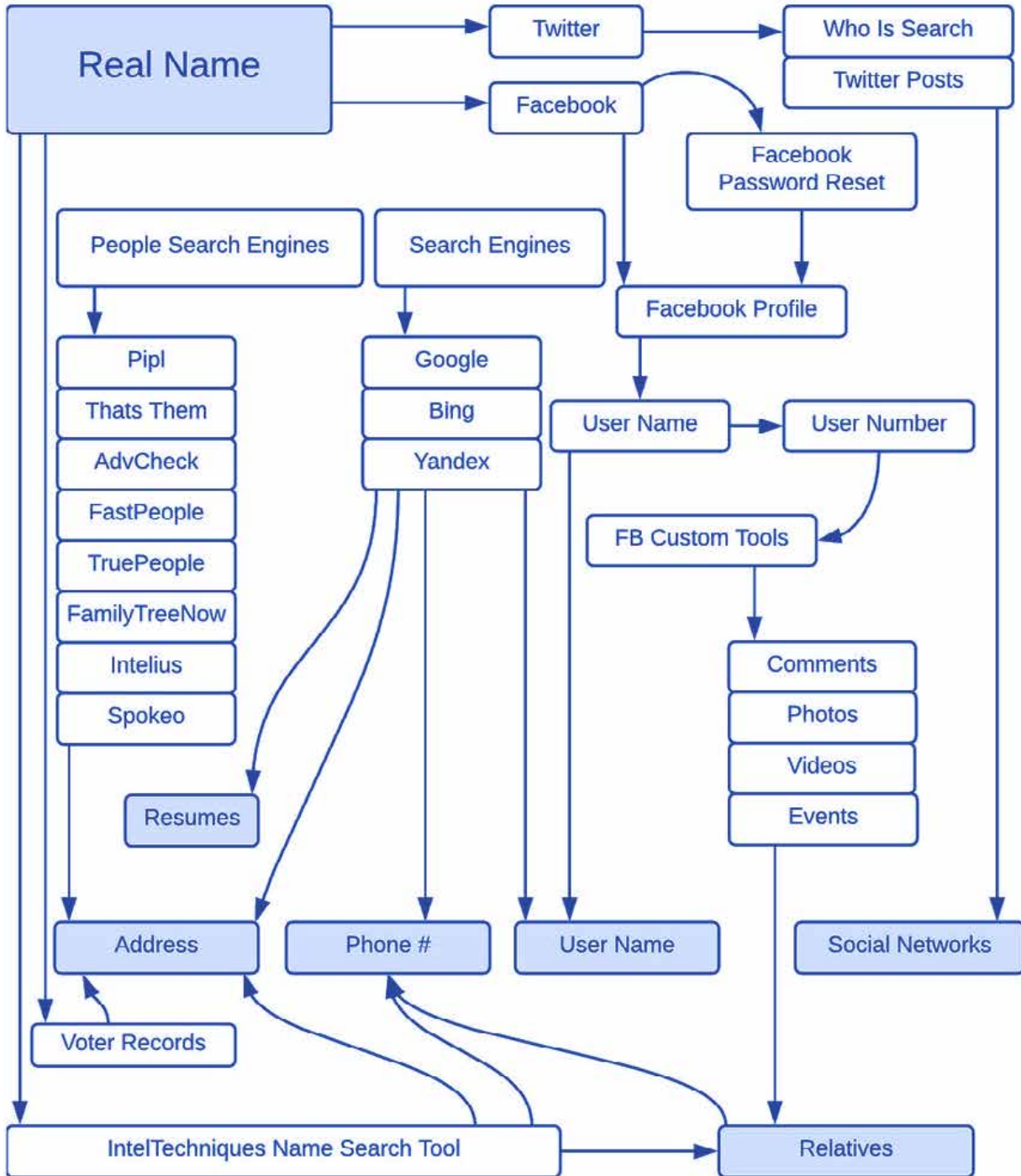
Esto significa buscar usuarios y entidades conectadas en el sistema y realizar una investigación OSINT sobre ellos.

A menudo descubrirás que los enlaces que están presentes internamente pueden encontrarse también en la web abierta. Y viceversa: utilizando la inteligencia obtenida a través de herramientas OSINT, se pueden descubrir nuevos puntos de interés buscando internamente, incluso si no estaban vinculados originalmente por otros puntos de datos. Esto es bastante común cuando se disuelven las redes fraudulentas.

Existen varios flujos de trabajo OSINT -recopilados originalmente por Michael Bazzell en IntelTechniques.com- que puedes memorizar y practicar hasta que se conviertan en algo natural.







OSINT: Captura de pruebas y toma de notas

Para investigaciones muy básicas, recoger los enlaces a la información encontrada junto a tus notas y explicaciones debería ser suficiente. Pero no solo es real la bit rot (degradación de datos), sino que tendrás que lidiar con indicios y pruebas. Además, los buenos ciberdelincuentes no solo practican la seguridad operativa (OpSec), sino que también intentarán ocultar sus huellas.

Esto significa que necesitas utilizar herramientas como archive.is o archive.org (The Wayback Machine), varios plugins de captura de pantalla para tu navegador de elección, o la extensión Hunchly, estándar en la industria (que tiene licencias anuales).

¿Qué herramientas OSINT están disponibles para la detección y prevención del fraude?

Si estás leyendo esto, probablemente estés pensando que todo esto suena como un montón de trabajo. Hacer OSINT manualmente ciertamente lo es, y un analista solo puede ser tan bueno y rápido que los servicios empezarán a pensar que son bots.

En SEON, nuestra función de búsqueda manual te permite recopilar rápidamente las huellas digitales de un usuario utilizando solo su dirección de correo electrónico o su número de teléfono, y ya es compatible con más de 35 redes sociales y plataformas web (y sigue creciendo).

Puedes utilizarla como una [extensión de Chrome](#) o una API, y viene incorporada a nuestra pila de prevención del fraude, donde puedes utilizarla para aplicar automáticamente puntuaciones de riesgo a las transacciones.

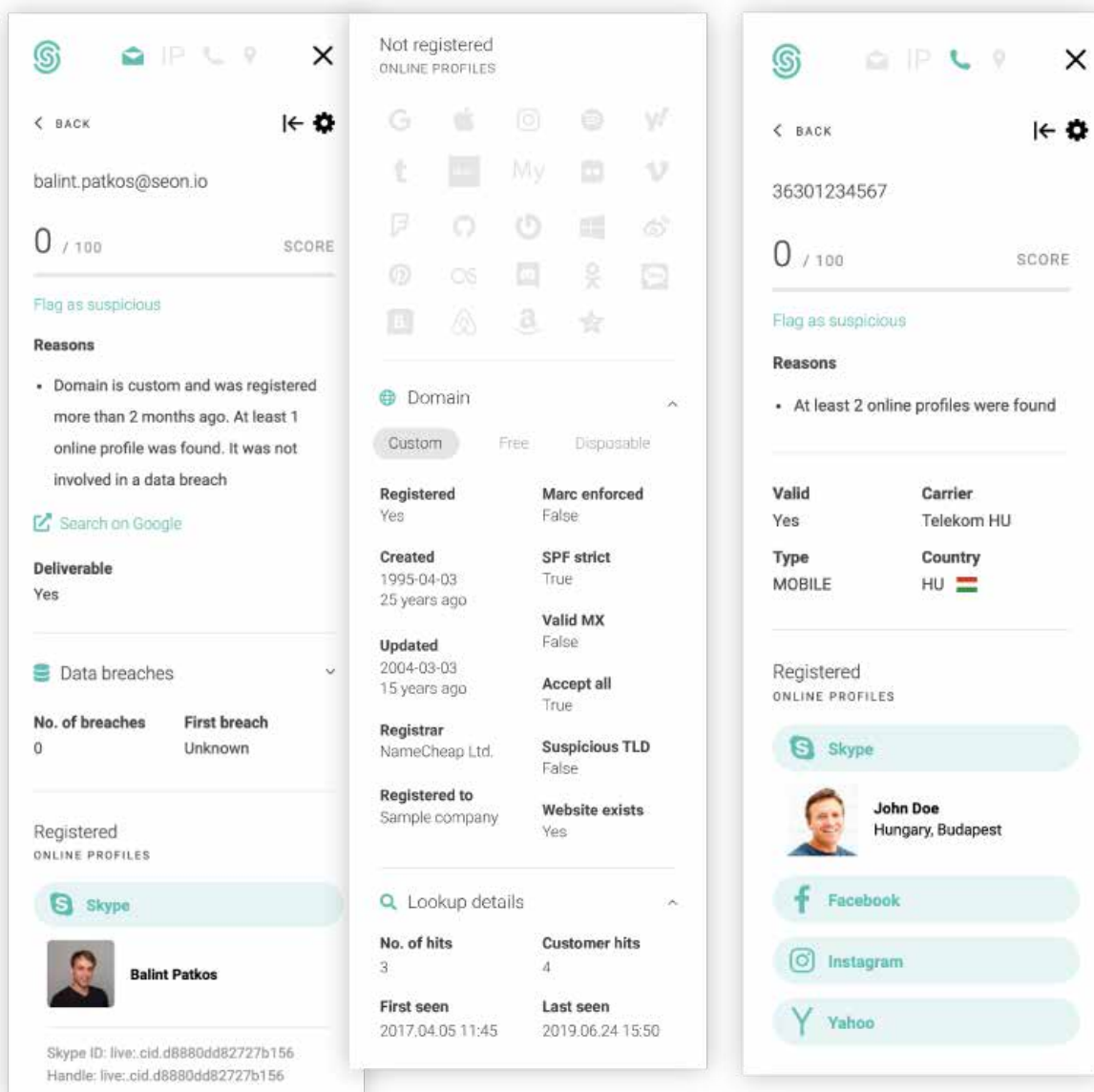
Otras herramientas de calidad industrial disponibles en el mercado son:

Maltego: El traje de poder de investigación compleja. Aunque la edición comunitaria es gratuita y muy limitada, las licencias son caras, pero la cantidad de transformaciones que se pueden hacer hacen que el precio merezca la pena.

Skopenow: Una suite OSINT más moderna, diseñada para investigaciones de todo tipo. Su punto más fuerte es encontrar personas, empresas y sus asociados, convirtiendo casos complejos en abiertos y cerrados.

Netwatch: Se enorgullece de ser la opción número 1 de inteligencia en línea y en redes sociales, y trabaja con una amplia gama de socios de datos para investigaciones de grado industrial.

Effect Group: Una elegante plataforma de inteligencia creada especialmente para investigaciones OSINT, que se paga por acción, lo que permite a los analistas compilar perfiles de forma rápida y relativamente barata.



También vale la pena señalar que hay máquinas virtuales prefabricadas y creadas especialmente para las necesidades de OSINT.

Conclusión

La inteligencia de código abierto es como una navaja suiza en la caja de herramientas del analista. Es extremadamente útil en el contexto de la prevención del fraude, ya que los ciberdelincuentes se especializan en vencer los sistemas de seguridad automatizados que montamos contra ellos.

Dominar este arte puede resumirse en ser capaz de encontrar información que alguien no quiere que encuentres.

Aunque hay bastantes opciones disponibles para automatizar el proceso, a fin de cuentas, lo que importa es la determinación, así como ser capaz de manejar la información en el contexto adecuado, sacar las conclusiones correctas y tomar decisiones basadas en ello.





Para ver cómo SEON puede ayudar a su empresa a prepararse para el futuro, visite seon.io

O programe ahora una llamada de presentación de productos personalizada.

Visite nuestro sitio web

Programe una llamada