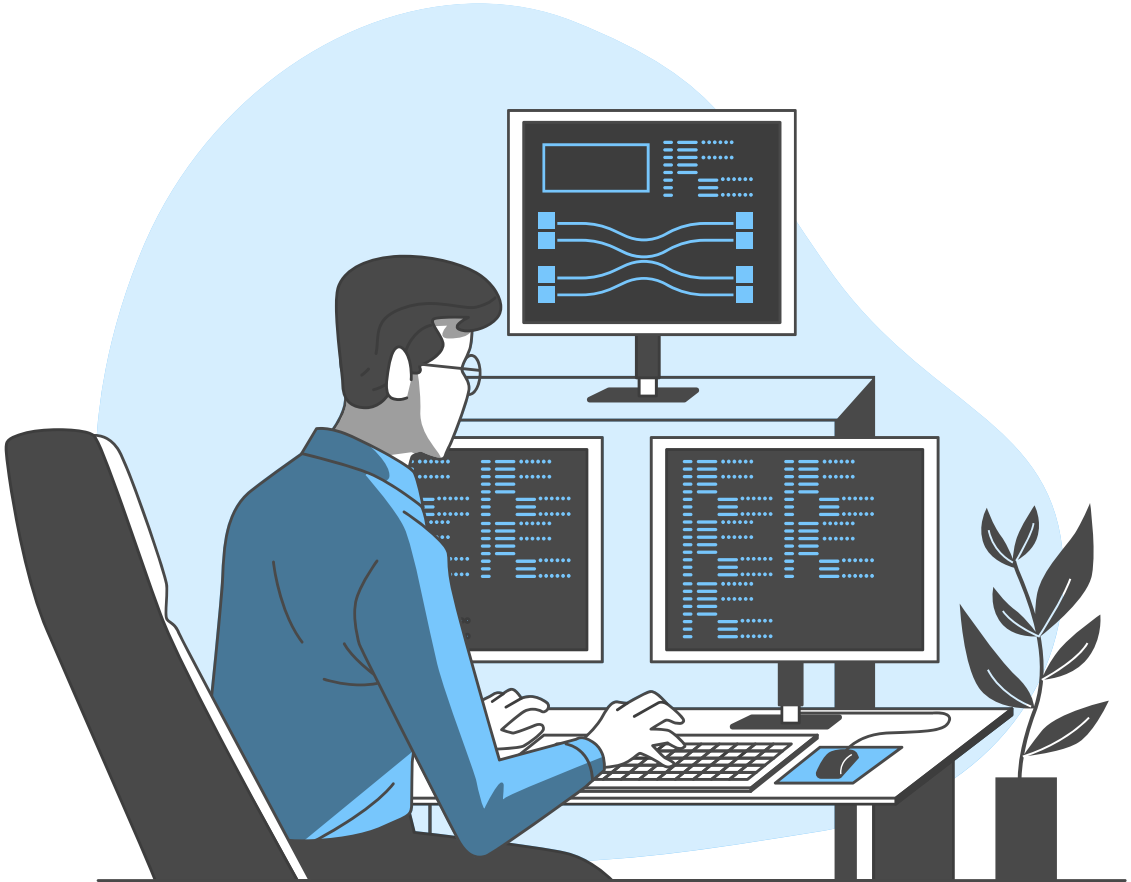


TALLER OSINT

Sergio Lucero Corchado

¿OSINT?

OSINT proviene de **O**pen **S**ource **INT**elligence, y como su propio nombre indica, es la práctica de recopilar y analizar información de fuentes abiertas.

Sergio Lucero Corchado

¿Para qué fue creado?

Vamos a ver para que ha sido creado OSINT:

1. Análisis de posibles robos y fugas de información tanto de empresas, gobiernos, etc.
2. Investigación de personas, organizaciones, eventos, objetivos...
3. Monitorización de tendencias sobre lo que se habla en Internet, ya sea de una organización, producto, persona, o incluso, sobre diferentes temas de actualidad.
4. Análisis de relaciones entre personas, empresas, gobiernos, partidos políticos, etc.
5. Detección de fallos de configuración que expongan información en la red.
6. Monitorización de investigación de phishing y posibles páginas malintencionadas.

Usos más comunes

01

Reconocimiento en pentesting

Recopilar toda la información posible en la primera etapa de pentesting.

02

Ingeniería social

Usar toda la información disponible de un usuario para hacer un ataque de ingeniería social a medida.

03

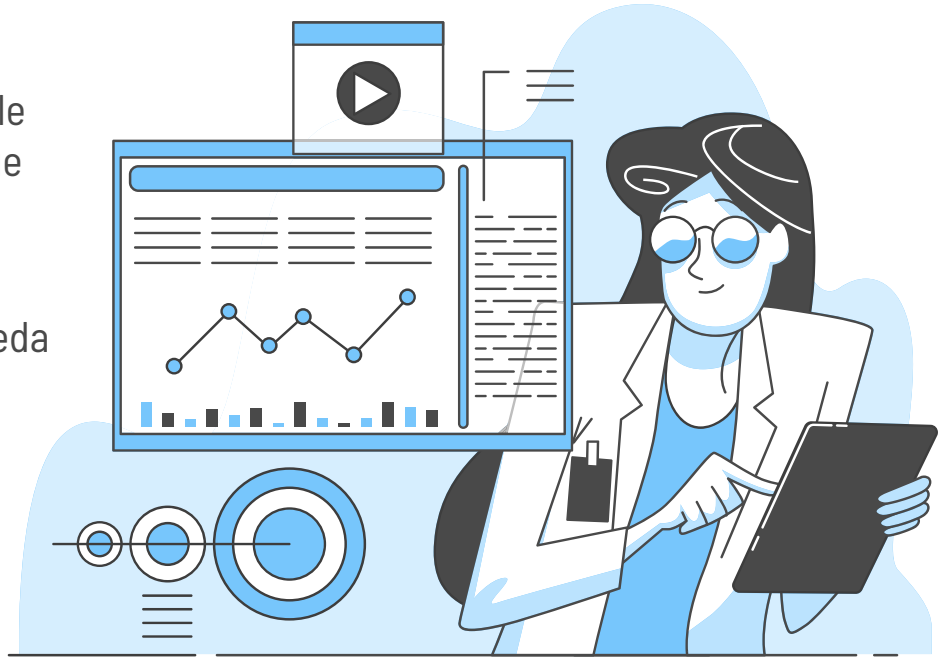
Prevención de ataques

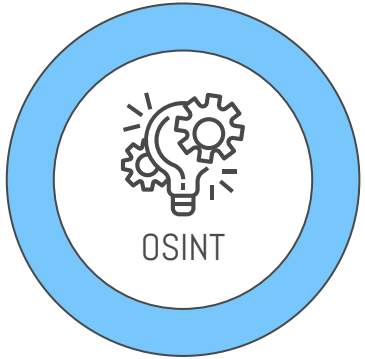
Obtención de información que pueda revelar un posible ataque frente a una organización.

04

Investigaciones

A día de hoy se usa mucho a la hora de casi cualquier tipo de investigación.





Ejemplo en el que sería útil

Un grupo de hacktivistas se está organizando para realizar un DDoS a un organismo público. Están usando RRSS y foros para organizarse.
¿Cómo evitar este ataque? Si se buscase información sobre próximos ataques DDoS podríamos localizar la información en RRSS y foros, ya que estos hacktivistas están utilizando sitios de libre acceso.

...

Sergio Lucero Corchado

“Si conoces al enemigo y te conoces a ti mismo, no debes temer el resultado de cien batallas.”

—Sun Tzu

¿De dónde se puede obtener la información?

- Internet (RRSS, foros, webs...)
- Medios de comunicación (radio, TV...)
- Publicaciones profesionales y académicas (tesis, artículos, disertaciones...)
- Literatura gris (patentes, informes técnicos...)
- Datos gubernamentales (boletines oficiales, conferencias...)
- Datos comerciales (evaluaciones financieras...)

Sergio Lucero Corchado

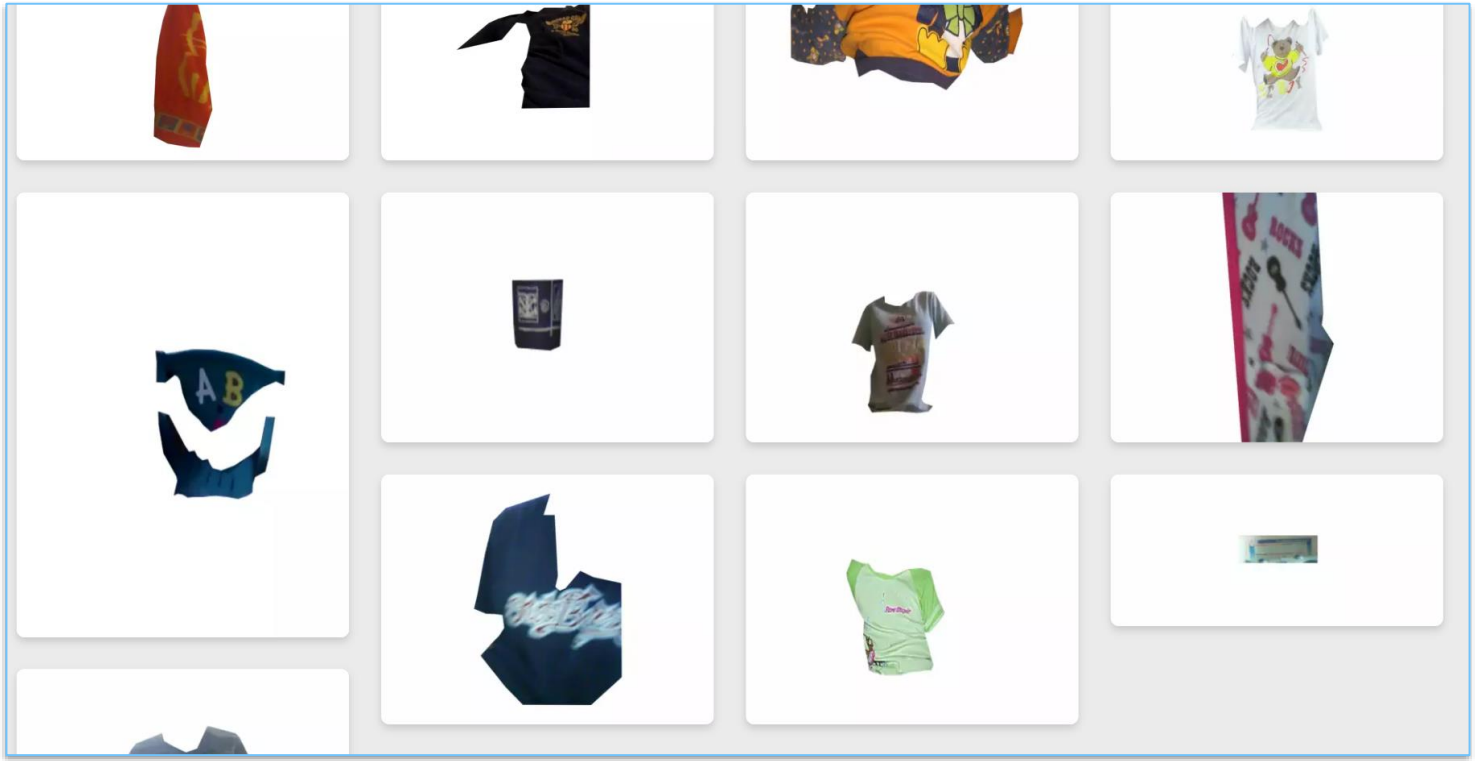
Uso de Google Dorks

- **cache**: este dork mostrará la versión en caché de cualquier sitio web, por ejemplo, *cache:nombredelaweb.com*
- **allintext**: busca texto específico en cualquier página web, por ejemplo, *allintext: autor Exploitables*
- **allintitle**: exactamente igual que allintext, pero mostrará páginas que contienen títulos con lo que deseamos buscar, por ejemplo, *allintitle:"Exploitables contacto"*
- **allinurl**: se puede utilizar para obtener resultados cuya URL contiene el texto que buscamos, por ejemplo: *allinurl:contacto-exploitables*
- **filetype**: se utiliza para buscar cualquier tipo de extensiones de archivo, por ejemplo, si se desea buscar archivos .pdf podemos usar: *correo electrónico exploitables: pdf*
- **inurl**: esto es exactamente lo mismo que allinurl, pero solo es útil para una sola palabra clave, por ejemplo, *inurl:admin*
- **intitle**: se utiliza para buscar varias palabras clave dentro del título, por ejemplo, *intitle:autor contacto* buscará títulos que comiencen con "autor", pero "contacto" puede estar en otro lugar de la página.
- **site**: mostrará la lista completa de todas las URL indexadas para el dominio y subdominio especificados, por ejemplo, *site:exploitables-security.blogspot.com*

Fuente: Exploitables

Vídeo

Europol – Trace an Object

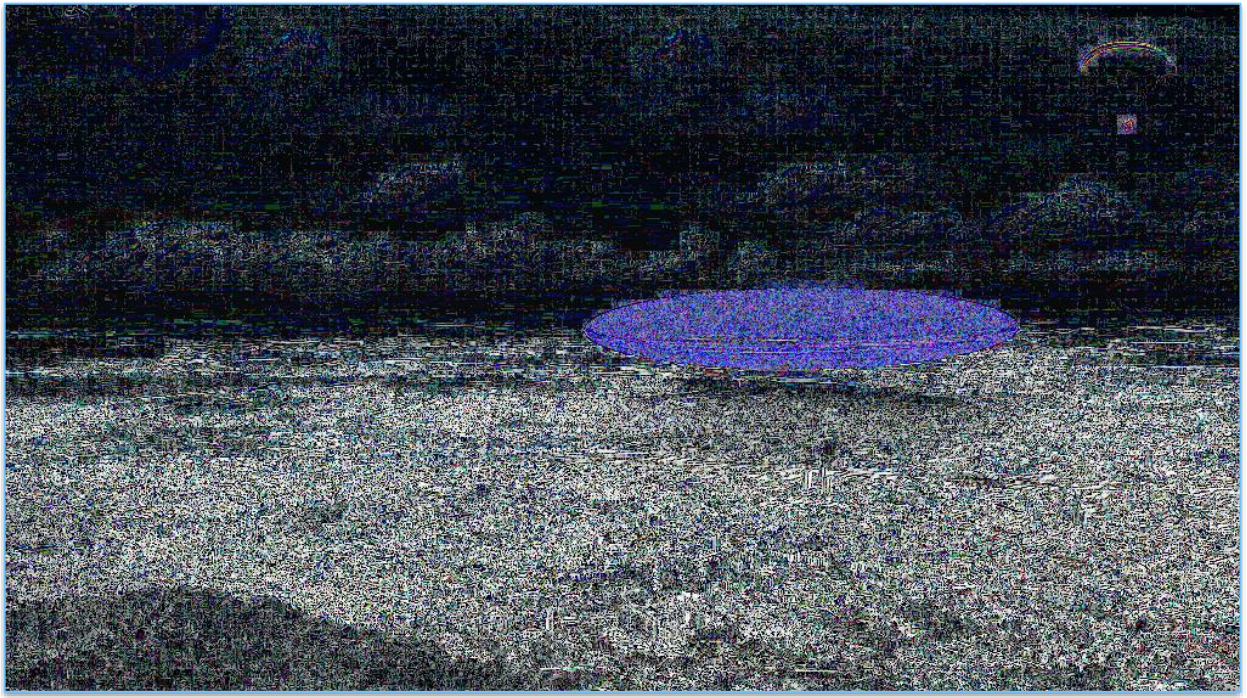


Link a la página

Sergio Lucero Corchado

Detectando fakes

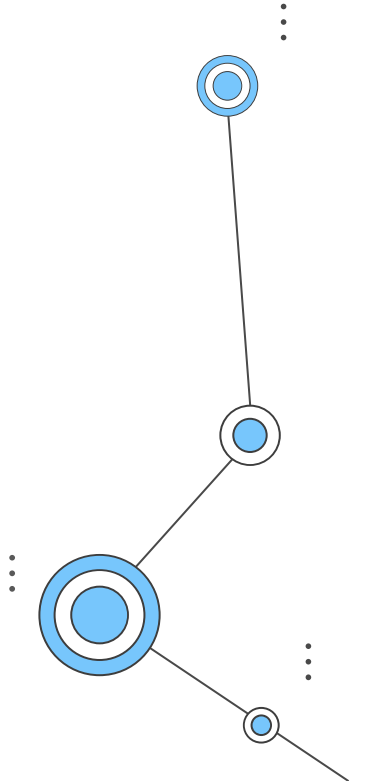
Detectando fakes

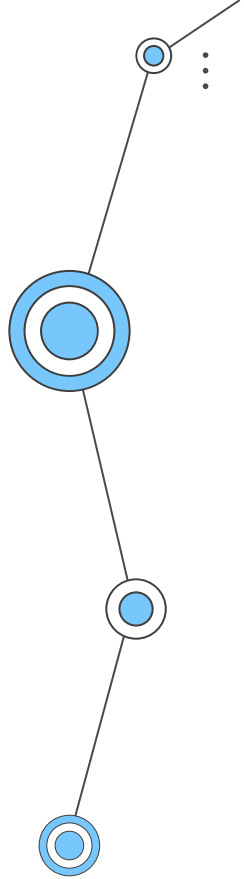


Análisis de ruido con la heramienta Forensically

FIN

¿Alguna pregunta?





Exploitables.security @Exploitables1