CYBERLINX

People | Process | Technology


# OPEN-SOURCE INTELLIGENCE (OSINT): HOW IT WORKS AND THE IMPORTANT ROLE IT PLAYS

## What is OSINT?

A staggering amount of data is published on the internet every minute. A great portion of this data is publicly accessible. This has major implications for data collection and intelligence. Open-Source Intelligence (OSINT) is the gathering of information that is publicly available. The most common sources of this information includes various social media sites, blogs, company news sites and search engine results (e.g. Google).

## How is OSINT used?

The first stage in the cyber kill chain is reconnaissance. This refers to the gathering of information to target specific users or organisations. OSINT plays a great role in the information gathering stage, where adversaries will use information that is available to the public to gain further insight into their targets. A good example of this is using social media to gather further information about a target and sculpting customised mails for spear phishing campaigns towards targets. With OSINT tools, the reconnaissance process gets streamlined, enabling a more efficient narrowing-down to the target.

## OSINT Tools

Although there are many different tools that can be used for OSINT, below are 3 examples of information gathering tools and their functions to give you an idea of how information can be gathered in the OSINT stage:

- Shodan – Shodan is a website that acts as a search engine for interconnected devices that are exposed publicly on the internet. By using Shodan one may be able to find a server with vulnerable web services exposed to the internet.
- HaveIBeenPwned – This is a website that allows you to search specific email addresses and check whether they have been exposed in any breaches.
- Google Dorks – Google Dorks is not a tool per se, but rather a way of systematically defining search terms in google to find vulnerable openings in websites.

## Defence against OSINT

OSINT is not only used for malicious purposes, it can also be used for counter-intelligence. OSINT generally forms part of a Pen-Test and can help an organisation understand how their threat vectors are exposed to the public. Below are a few recommendations on how to defend against OSINT:

- Organisations need to structure a policy that limits end-users from using company email addresses to sign up for non-business-related third-party services.
- Social Media Profiles need to be made private and users need to be extremely aware of what they share.
- Organisations need to do frequent OSINT checks on themselves to see what information is publicly available on them, and to ensure that services that shouldn't be publicly visible are found by themselves first rather than adversaries.

Written by: Michael Frese