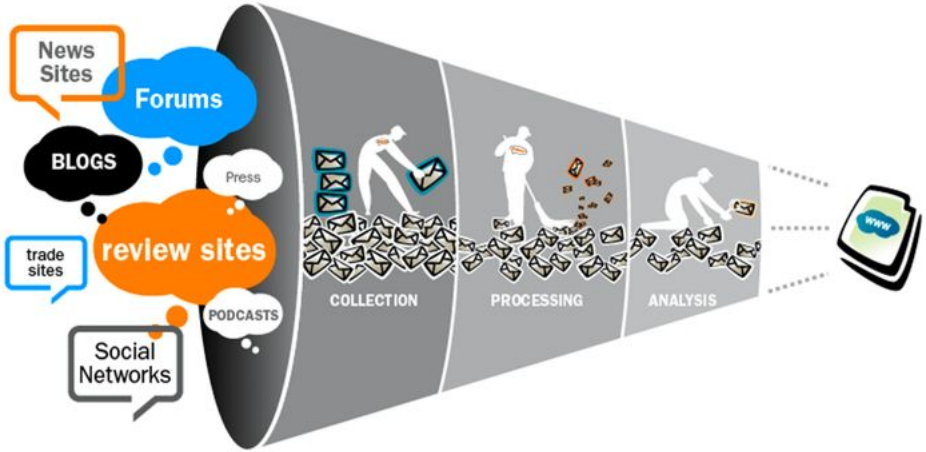
Open Source Intelligence (OSINT)

Aha!

Today's Agenda

1. Introduction to OSINT
2. How OSINT can be used?
3. Dark Side of OSINT
4. Tools and Techniques



What is OSINT?

OSINT stands for open source intelligence, which refers to any information that can legally be gathered from free, public sources about an individual or organization.

In practice, that tends to mean information found on the internet, but technically any public information falls into the category of OSINT whether it’s books or reports in a public library, articles in a newspaper or statements in a press release.

How it can be used

Effective OSINT gathering is essential for journalists, cyber security professionals and in the corporate world, such as the banking sector, to detect potential fraud, phishing scams, money laundering, counterfeit production and other issues.

Dark Side of OSINT

Anything that can be found by security professionals can also be found (and used) by threat actors. The attacker can use open source intelligence tools and techniques to identify potential targets and exploit weaknesses in target networks.

Tools and Techniques

Following are the tools and techniques used while performing OSINT:-

1. Google Dorks
2. Shodan
3. Wayback Machine
4. social-searcher.com
5. Exif Tool
6. Hunter.io
7. Buscador
8. Wappalyzer

Any Questions?

Thank you!