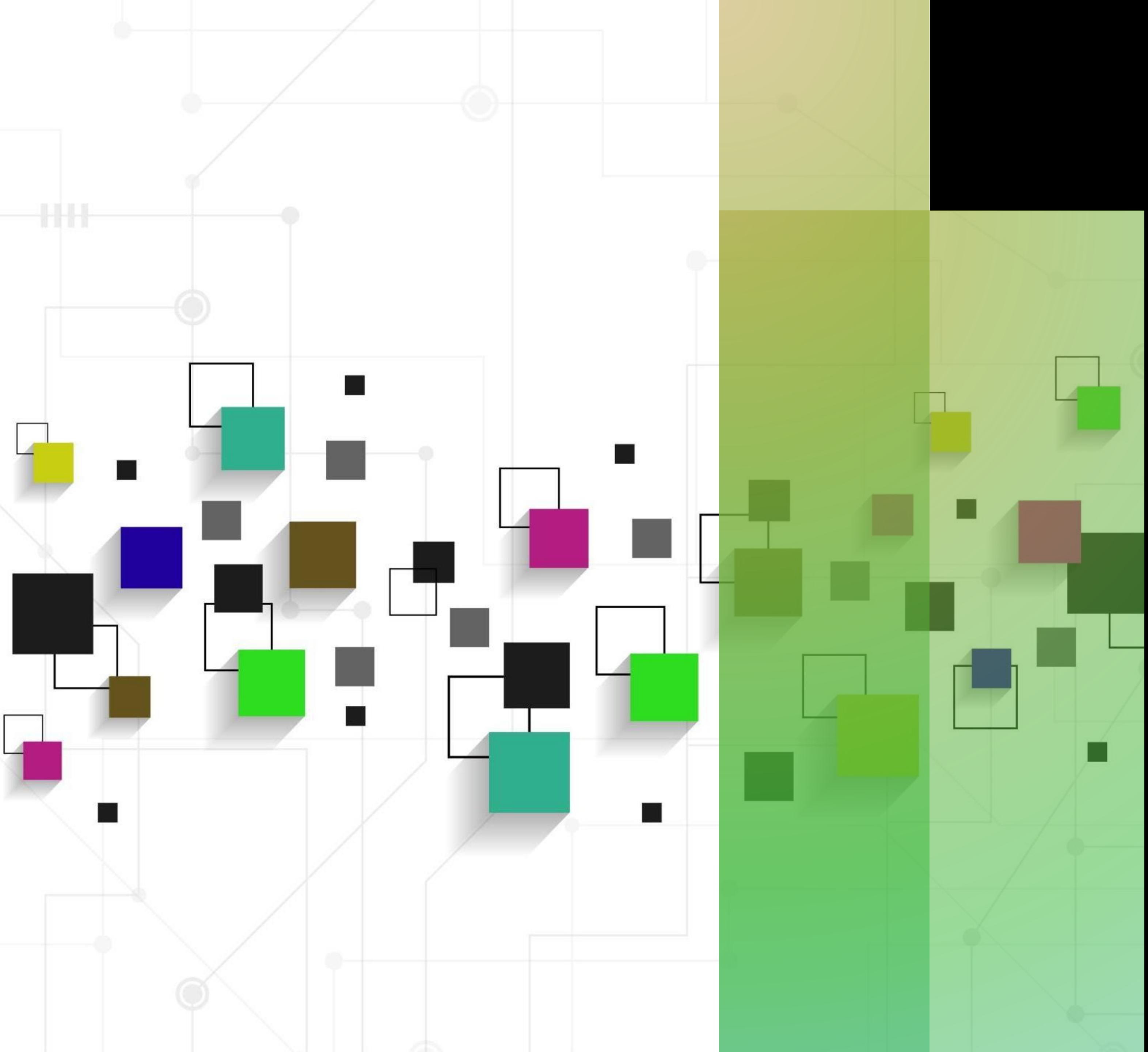


OSINT

Open-Source Intelligence

Click Here for Technique Sharing File

By: Alain G. Picard and Natasha Raddatz

What is OSINT?

- OSINT stands for Open-Source Intelligence.
- It is defined as the gathering of information by use of free tools and resources.
- OSINT has many use cases and is used by individuals as well as by organizations of all different shapes and sizes.

Different Techniques used for OSINT

ONLINE SEARCHING

SOCIAL MEDIA ANALYSIS

DOMAIN RESEARCH

Online Searching

There are many resources available online to utilize when researching OSINT data on the internet. Three examples of resources are:

- Toddington International Inc.
- Maltego
- DarkSearch.io

Toddington International Inc.

- Offers a free checklist for Online Investigators. It's an active reference guide of where and what to look for on the internet, when investigating a case
- Offers an Advanced Search Techniques cheat sheet of how to get the best results out of search engines

Maltego

- OSINT and graphical link analysis tool
  - Visual interface where all information that has been gathered is linked and combined to visually represent results – up to 10,000 data points
  - Over 58 data integrations from over 35 data partners. Choose from OSINT data sources, CaseFile Entities, and more.
  - Multiple ways to map data – block, hierarchical, circular, organic – to analyze data and patterns in results

DarkSearch.io

- A dark web search engine that can be accessed through a regular web browser
- Good platform for investigators who are just starting out with their research activities
- Free API (application programming interface)
- Don't need to use .onion site or Tor to utilize search engine

Social Media Analysis

Social media platforms are full of data that can be used for threat assessments, competitive analysis, criminal investigations, and more. Each platform has its own specific OSINT capabilities.

- Facebook
- TikTok
- YouTube
- LinkedIn

Facebook

With it's overwhelmingly large user base and various features, investigators can retrieve the following data:

- Profile analysis
- Geolocation
- Content Analysis

Investigators can find data on their suspect by viewing:

- Mutual friends' profiles
- Photos & Comments
- Relatives' profiles

Tiktok

TikTok is a platform where users share short videos, whether of their own original content, duet another user's video, or share someone's video with a friend.

OSINT techniques useable for TikTok include:

- Video analysis
- Hashtag monitoring
- User profiling

YouTube

YouTube's platform is plentiful with multimedia content, primarily videos.

YouTube has built-in features that enable OSINT techniques used by investigators such as:

- Location of content being uploaded
- Extracting metadata from videos, playlists, and channels
- Extracting video transcripts
- Comment analysis
- User profiling

LinkedIn

LinkedIn is a platform that allows people to create and maintain ad professional profile, online. Employers as well as employees can benefit from using this platform.

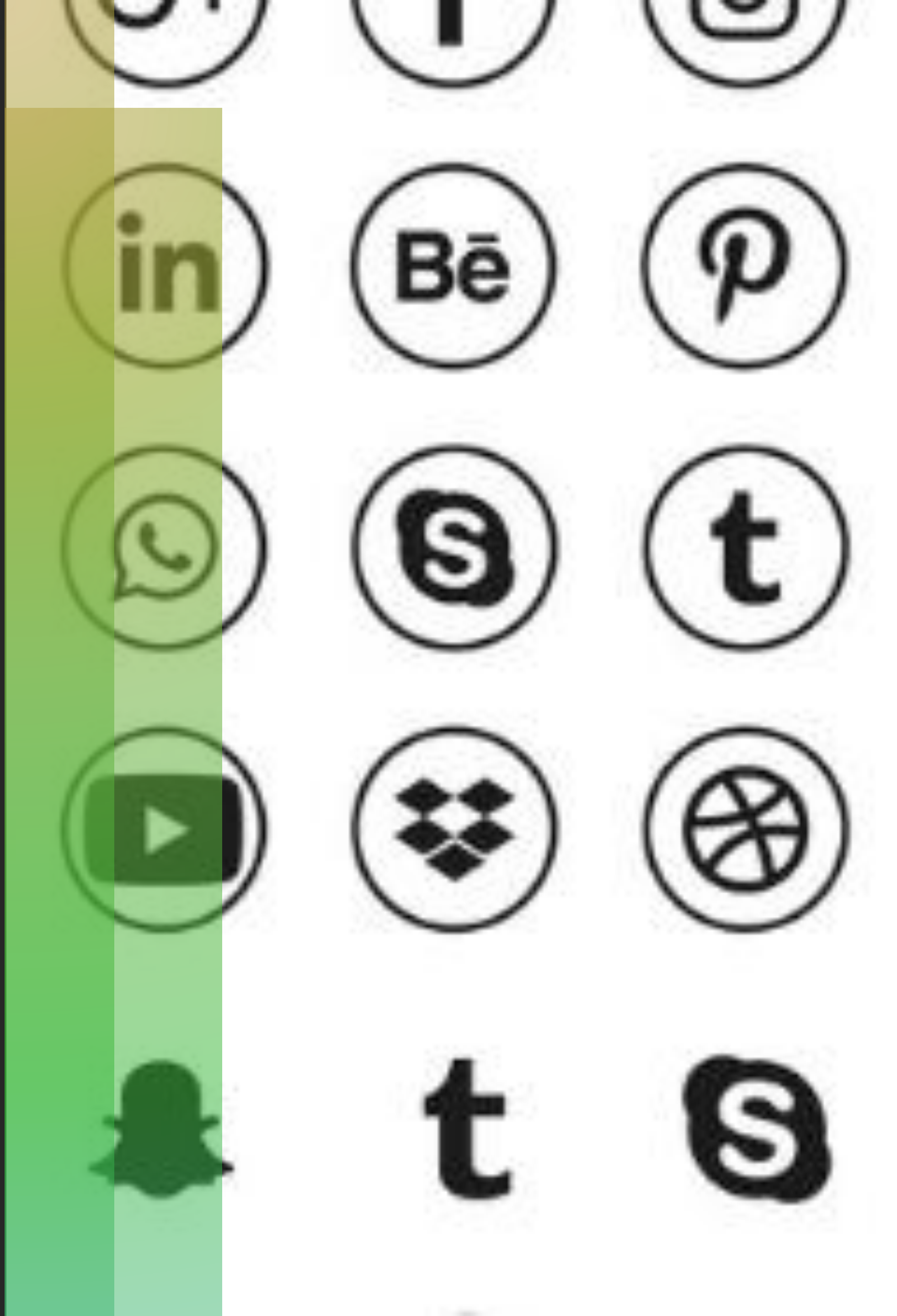
LinkedIn aides OSINT techniques by offering:

- Profile analysis
- Network mapping
- Job positing analysis

Social Media Analysis Examples

Social media OSINT has been used for:

- Terrorism & Extremism Monitoring
- Corporate Espionage & Competitive Analysis
- Missing Persons & Criminal Investigations
- Geopolitical Analysis



Domain Name Research

Domain Name Research is an OSINT technique which involves using a domain name or IP address.

The domain name or IP address is used to locate specific information about the domain name owner.

Domain Name Research
Online Tools

- There are several online tools that can be used to perform domain name research.
- Some of the available tools include:
  - Viewdns.info
  - Whoisology
  - DomainBigData

Viewdns.info

This tool will display the owner/contact information for a given domain name or IP address.

This tool can also be used to see if a domain name is registered or not.

Viewdns.info is able to provide the name, address, phone number, and email address of the registrant and administrator.

Whoisology

- Whoisology will display the owner/contact information for a given domain name or IP address.
- Just like Viewdns.info, Whoisology can be used to see if a domain name is registered or not.
- It is able to provide the name, address, phone number, and email address of the registrant and administrator.

DomainBigData

- DomainBigData can provide the date a website was created.
- Can provide other domains owned by the same individual or company.
- DomainBigData can provide Geolocation.
- Can provide historic registrant information which can be used to potentially link different entities together.

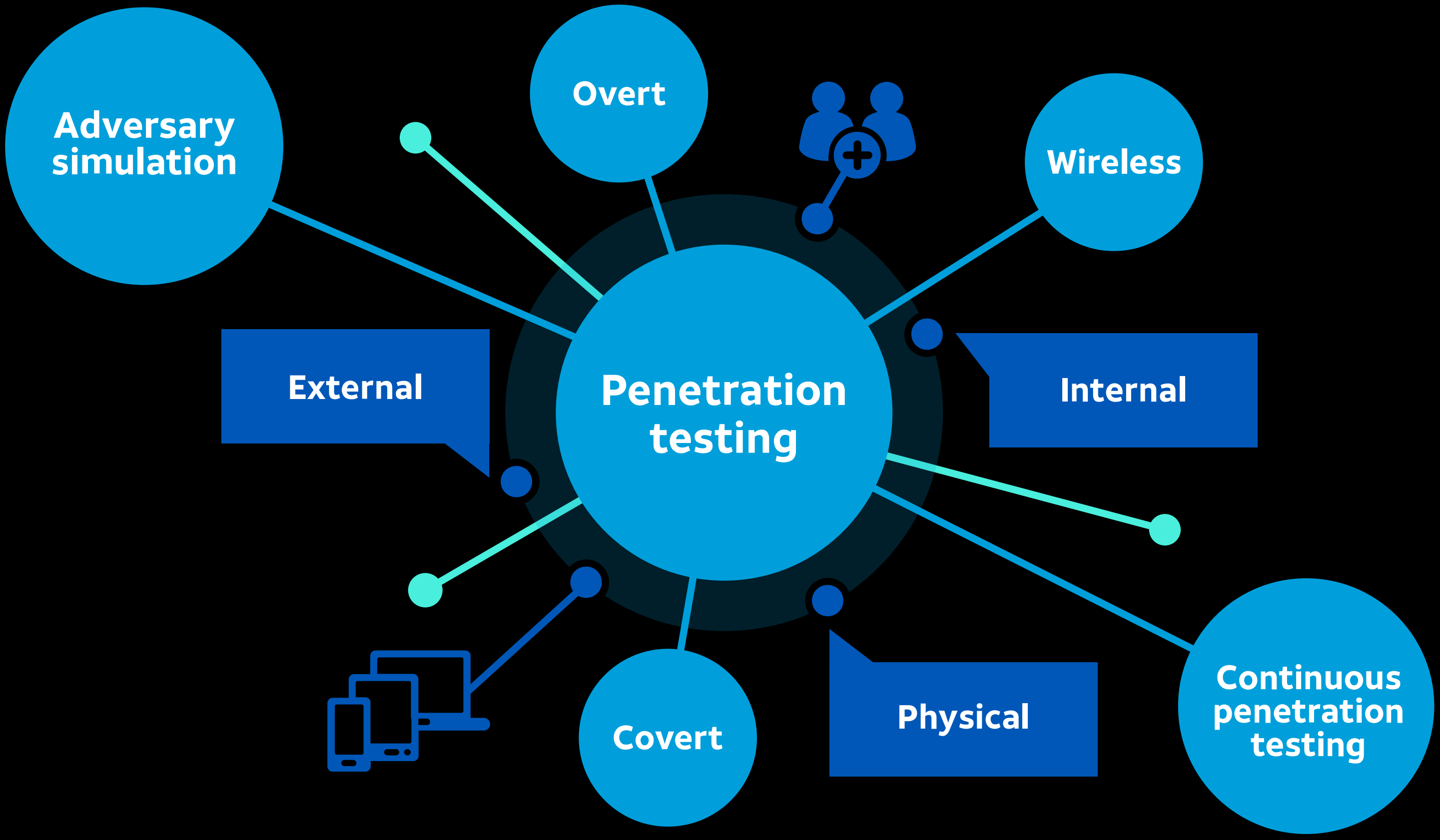
Use Cases

There are different OSINT use cases, such as:

- Investigating potential security threats or vulnerabilities
- Conducting market research and competitive analysis
- Identifying potential leads and targets for business development
- Verifying the authenticity of information and sources.

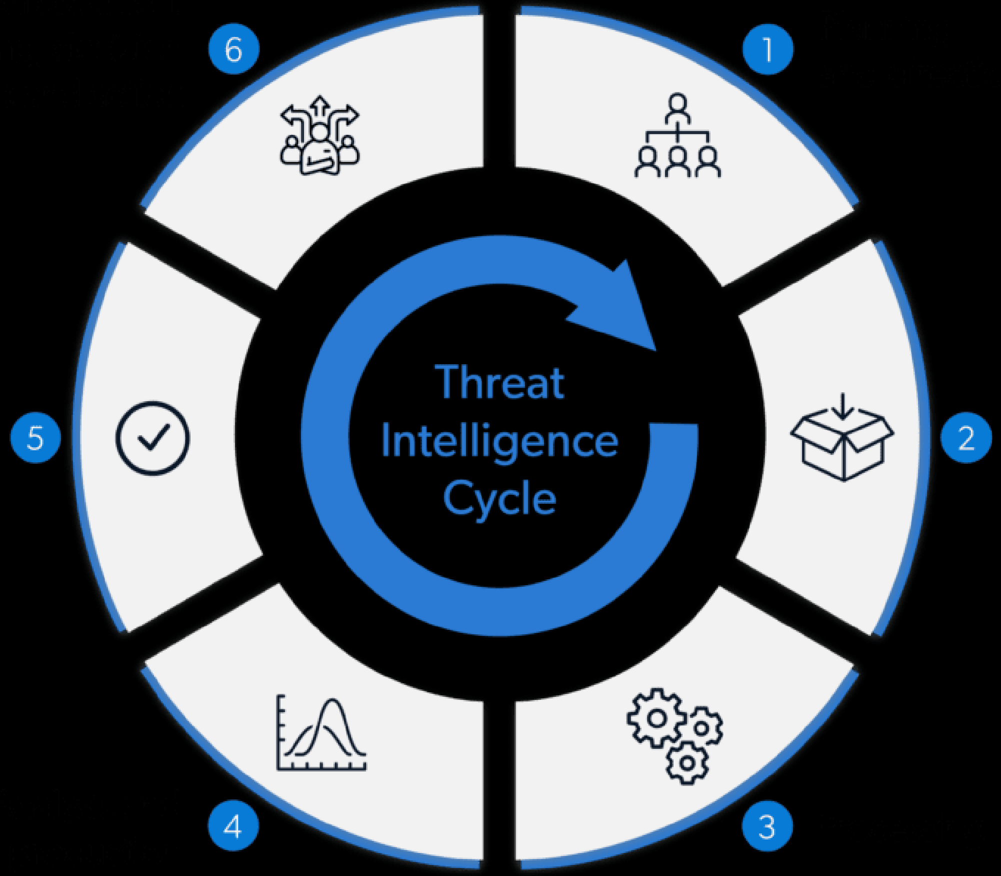
Use Cases

- The two most popular uses for OSINT are:
  - Measuring the risk to your own organization (penetration testing).
  - Understanding the actor, tactics and targets (threat intelligence).



Penetration Testing

Also known as ethical hacking, this is a simulation of a real-world cyberattack to test an organization's cybersecurity capabilities and expose vulnerabilities. Experts attempt to find and exploit vulnerabilities in a computer system.



Threat Intelligence

Data that is collected, processed, and analyzed to understand a threat actor's motives, targets, and attack behaviors (Baker, 2023).

Potential Ethical Considerations

- OSINT is a powerful tool and like other powerful tools, if not used correctly, can have unintended consequences.
  - One consideration is copyright and commercial requirements of various vendors.
  - Another thing to consider are corporate laws and policies.
- For example, creating a fake profile on Facebook in-order to view private content is against Facebook policy and would not be considered ethical.

Potential Ethical Considerations

- OSINT should never include any of the following techniques:
  - Hacking
  - Intrusion Testing
  - Physical Security Testing
  - Undercover Operations

Potential Ethical Considerations

- When utilizing OSINT, your goal should be to do more good than harm.
- Before applying OSINT, you should consider who will benefit and how they will benefit while at the same time consider who will be harmed and how they will be harmed.

Potential Ethical Considerations

You should consider the fact that all people have the right to live their own life without certain restrictions from an outside force.

People also have the right to privacy and the protection of personal data which can easily be compromised when engaging in OSINT.