OSINT Fundamentals for Beginners

The following activity is designed for educational purposes only, to demonstrate OSINT techniques in a controlled and ethical manner

cyber673

Presented by
Fauzan Salleh

OK

whoami

Fauzan Salleh

Cyber Security Operation Specialist
Red Team Unit
Cybersecurity Department

CTF Enthusiast

ITIL 4 Foundation

CompTIA Security+

AGENDA

01

WHAT

02

APPLICATION

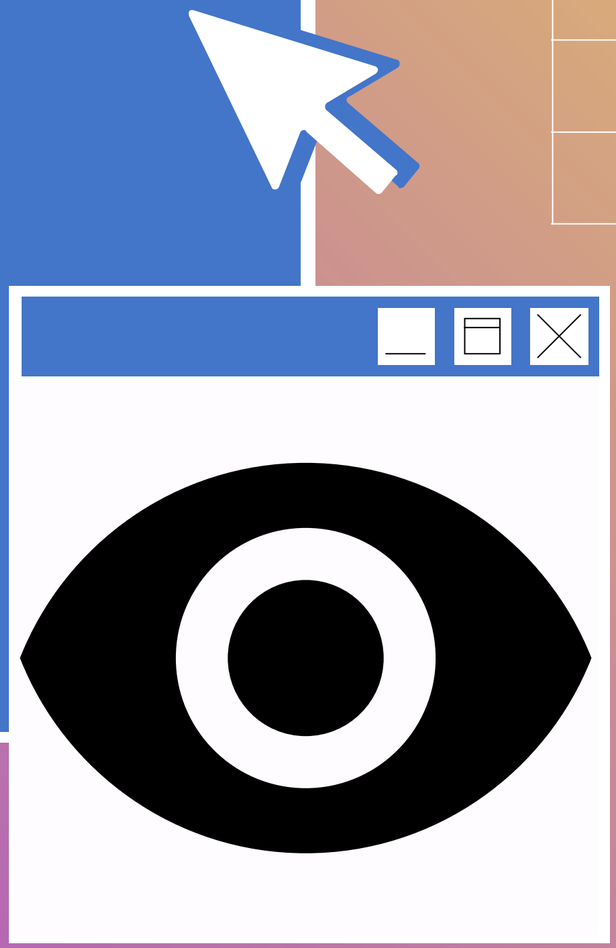
03

METHODS

04

TOOLS

01
WHAT IS OSINT?



WHAT IS OSINT?

DEFINITION

- OSINT is the **collection** and **analysis** of data from **publicly** available sources to generate actionable **intelligence**.

SOURCE

- Social media (e.g., Facebook, X)
- Websites, forums, news articles
- Public records, academic publications

INFORMATION VS INTELLIGENCE

INFORMATION

RAW DATA

(e.g., a list of social media posts)

INTELLIGENCE

ANALYZED DATA

Reveals patterns or insights (e.g., public perception of a company)

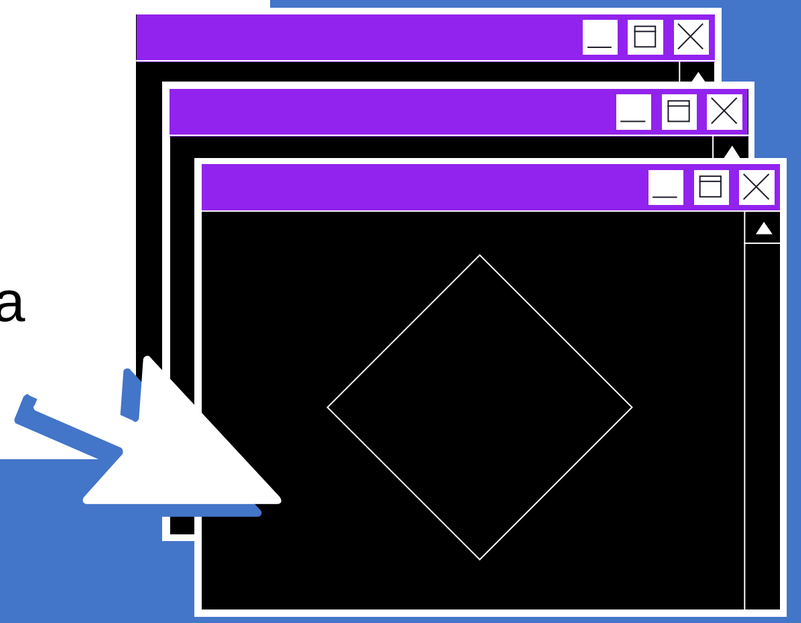
REAL-WORLD EXAMPLE OF OSINT

Cybersecurity Use Case:

- Collecting data from a company’s website to identify exposed server details.
- Analyzing the data to assess potential vulnerabilities.

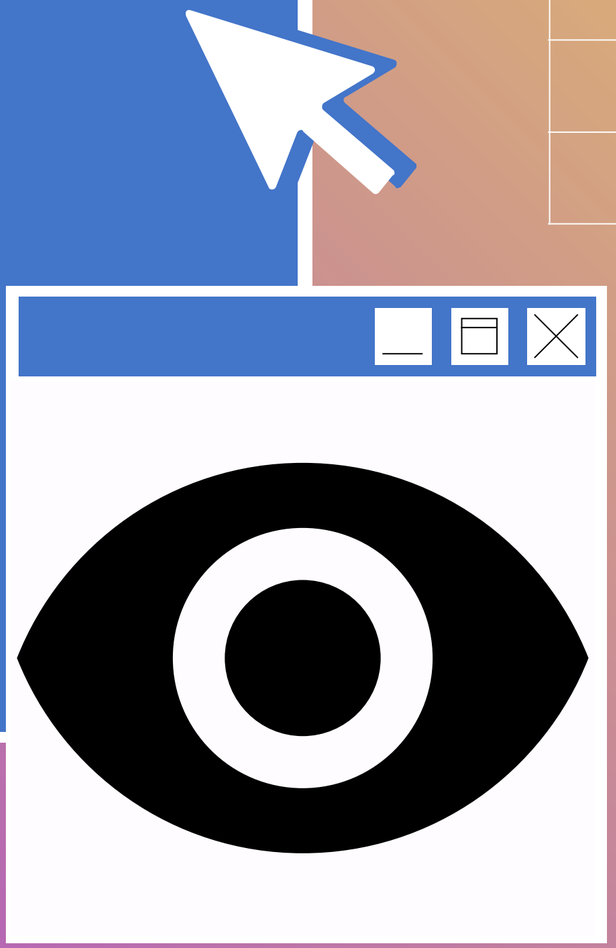
Other Example:

- Tracking public reactions to news events via social media.



02

APPLICATION OF OSINT?



APPLICATION OF OSINT - Beneficial

Threat Intelligence

Identifying emerging cyber threats (e.g., new malware)

Law Enforcement

Investigating crimes using public posts or geolocation data

Business Intelligence

Analyzing competitors and market trends

Journalism

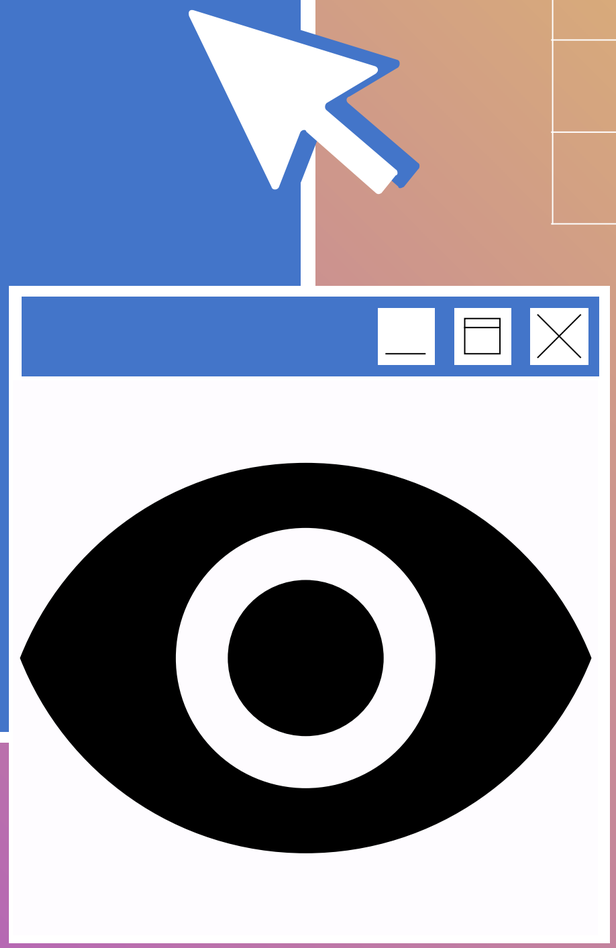
Verifying facts and sourcing information from public databases

APPLICATION OF OSINT - Malicious

Cybercrime
Gathering personal data for phishing or social engineering

Espionage
State actors collecting intelligence on foreign entities

03 METHODS OF OSINT?



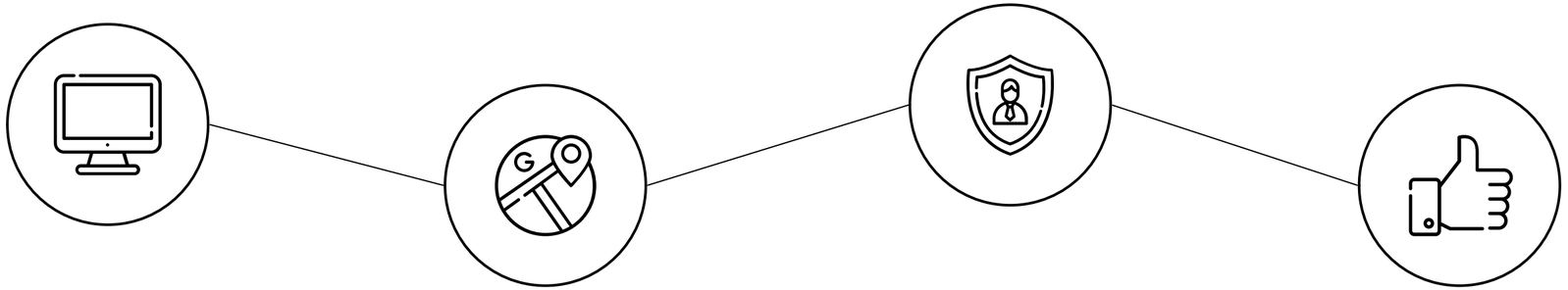
METHODS OF OSINT - Structure

Planning

Define the objective

Analysis

Analyze data for patterns or insights



Collection

Identify and gather data from sources

Dissemination

Report findings

METHODS OF OSINT - Basic

Search Engine Queries

Using Google with advanced operators

Social Media Monitoring

Analyzing profiles and posts for insights

Web Scraping

Automating data collection from websites (with legal compliance)

METHODS OF OSINT - Advanced

Domain and IP Research

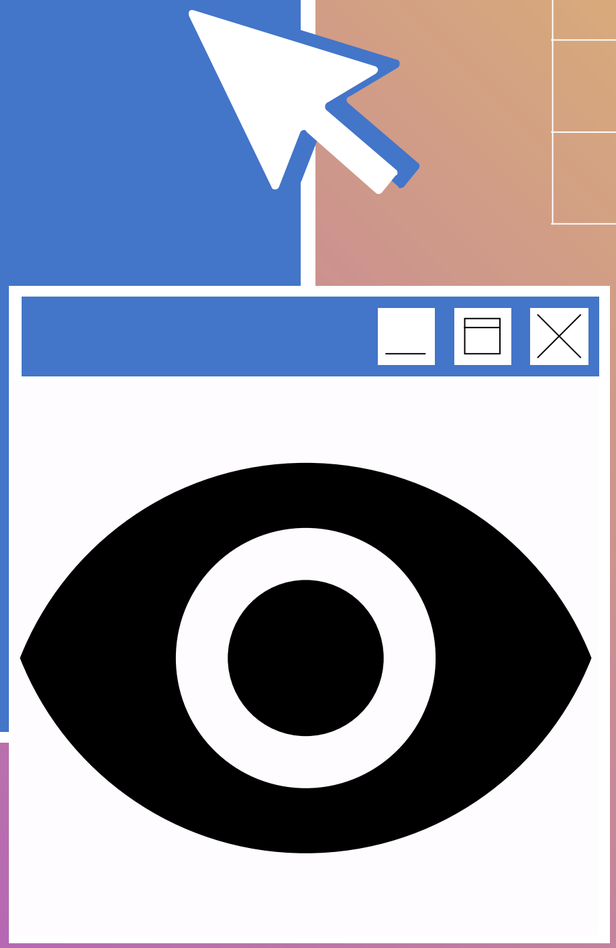
Investigating domain registrations or IP addresses

Geolocalization

Determining physical locations from IP data or maps

04

TOOLS FOR OSINT?



TOOLS FOR OSINT - Basic

Google

For basic and advanced searches using operators

Social Media Platforms

Facebook, X, LinkedIn for personal and organizational data

OSINT Framework

A directory of tools and resources (osintframework.com).

TOOLS FOR OSINT - Advanced

Maltego

Visualizes relationships between data points (e.g., email to social media accounts)

Shodan

Searches for internet-connected devices (e.g., exposed servers)

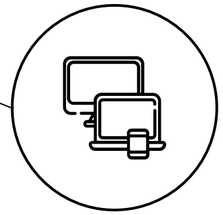
SpiderFoot

Automates OSINT collection from over 200 sources

GOOGLE DORKS

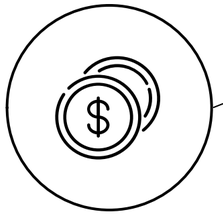
site:

Specifically searches that particular site and lists all the results for that site



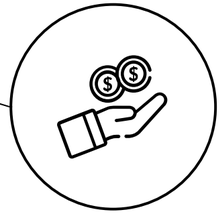
intext:

Searches for the occurrences of keywords all at once or one at a time



inurl:

Searches for a URL matching one of the keywords



filetype:

Searches for a particular filetype mentioned in the query

GOOGLE DORKS - Example and Responsible use

inurl:admin login

to find admin login
pages

intitle:"index of" password

to locate directories
with password files

GOOGLE DORKS - Example and Responsible use

```
site:*.bn intitle:"index of"
```

THANKS!