

FUNDAMENTAL OF OSINT METHOD AND RECCON (1)

START



TOPICS

WHAT IS OSINT

OSINT METHODE

INTELLIGENCE CYCLE

OPSEC

STUDY CASE

RECONNAISSANCE



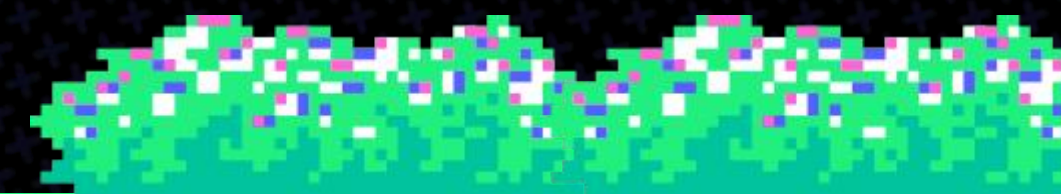
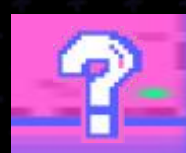
SIGN IN



BACK TO AGENDA PAGE



OSINT



KEEP A NOTES KEY OF OSINT

➦ ALWAYS LEARN AND LEARN ALSO CURIOUS

➦ MONITORING AND DATA COLLECTION

➦ BEWARE FAKE NEWS, PROPAGANDA, PYSOPS AND OTHER

ROLE OF OSINT

➤ JOURNALISM

➤ NATIONAL DEFENSE

➤ GENERAL

LEGAL AND RULE OF OSINT

➤ PUBLIC INFORMATION (OPEN SOURCE DATA)

➤ ETHICS, BOUNDARIES, ETHICS AND COMPLIANCE

➤ COMPLIANCE WITH RELEVANT LOCAL, NATIONAL AND INTERNATIONAL LAWS

LEGAL CONSIDERATIONS AND INTERNATIONAL LAW

➤ INDONESIA E.G UU PDP, UU ITE

➤ EUROPE E.G GDPR

➤ UNITED STATE E.G CCPA

ETHIC IN OSINT

➦ RESPECT FOR PRIVACY AND AVOIDANCE OF HARM

➦ DATA ACCURACY AND TRANSPARENCY

➦ MISUSE OF AUTHORITY

WHERE IS DATA COME FROM

➦ INTERNET (PUBLICATION, NEWS, FORUM AND DATASET)

➦ SOCIAL MEDIA

➦ GIS (GEOGRAPHIC INFORMATION SYSTEM)

CHALLENGE IN OSINT

➦ TO MANY INFORMATION AND UPDATES QUICKLY (DYNAMIC INFORMATION)

➦ DISINFO AND PROPAGANDA AND DEEPPFAKE

➦ ACCURAY AND VALIDATE DATA

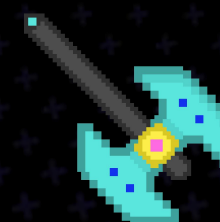
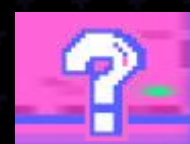
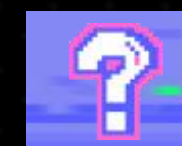
SIGN IN



BACK TO AGENDA PAGE



WHY OSINT IS IMPORTANT?



IMPORTANT OF OSINT

➦ BRAND REPUTATION

➦ EARLY THREAT DETECTION

➦ ENHANCES SITUATIONAL AWARENESS E.G TRENDS, ISSUE, GEOPOLOTICS

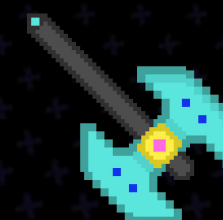
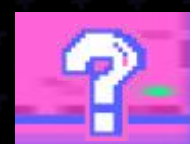
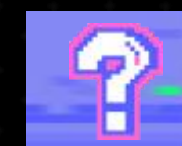
SIGN IN



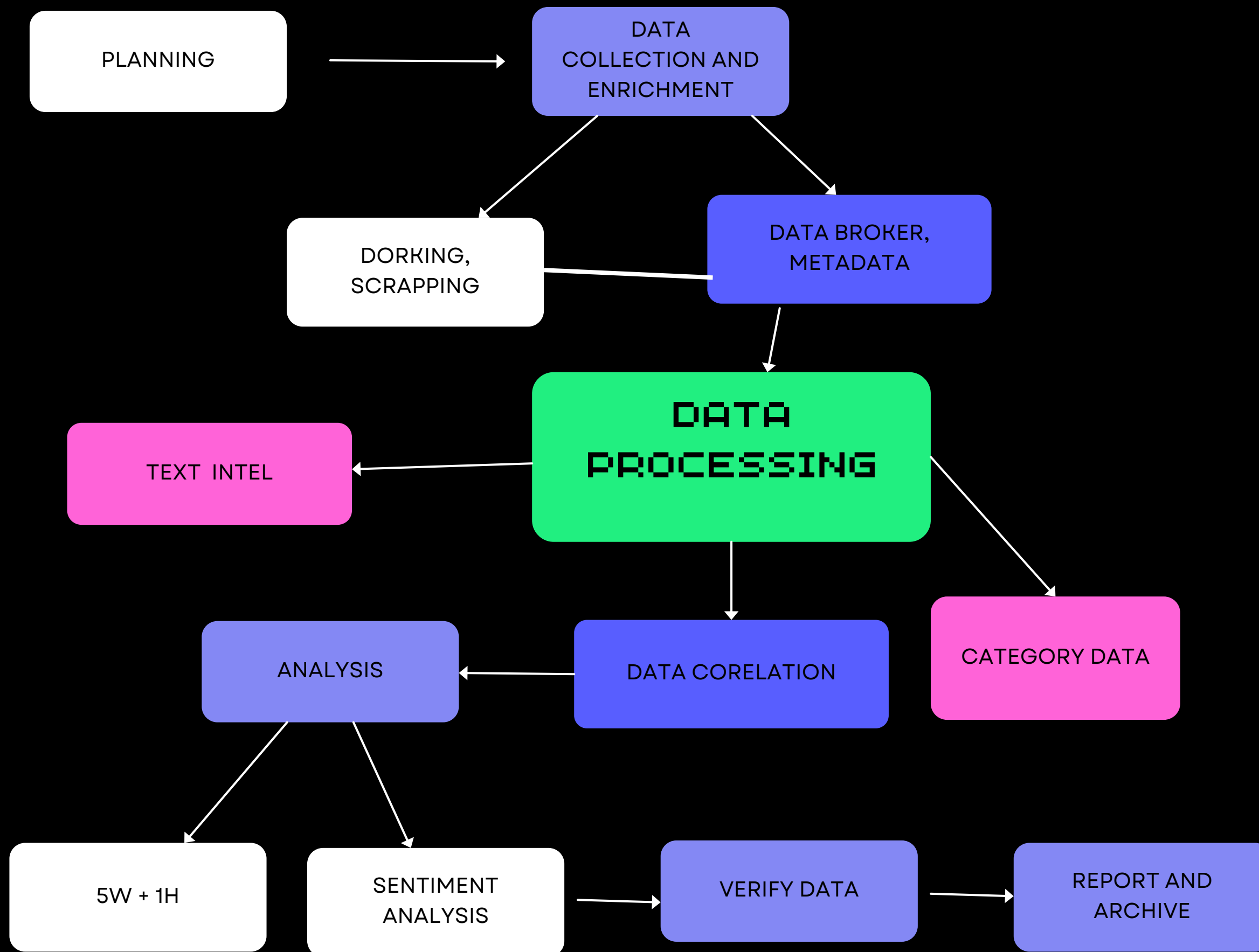
BACK TO AGENDA PAGE



METHODE OF OSINT



HOW OSINT WORK IN INTELLIGENCE



JIEYAB INTEL BASE

J

Jieyab89-OSINT-Cheat-sheet-Wiki-Tips

Search...

CtrlK

Welcome

OSINT RESOURCES

OSINT Resources

INTELLIGENCE BASE

Home

Intelligence Base & Knowledge Base

All About Doxing

All About OSINT Matters Things in OSINT

All About SIGINT Signal Intelligence

Cell Investigations

Geospatial Intelligence

How to OSINT Collection the Data

Powered by GitBook

INTELLIGENCE BASE

Copy

 **Intelligence Base & Knowledge Base**

OSINT and Other Category (Intelligence Base)

1. OSINT

Open Source Intelligence. In point one, OSINT search and Collection of information through open sources or the public internet. In contrast to intelligence obtained through secret methods or hidden, OSINT utilizes information available to general.

2. MASINT

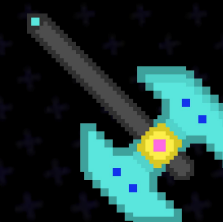
Signature Measurement and Intelligence focuses on collection and analysis of data from various forms of temperature measurements and changes or climate. In contrast to intelligence which is based on visual reconnaissance or communications, MASINT relies on technology to detect and analyzing signals that cannot be detected directly by human senses.

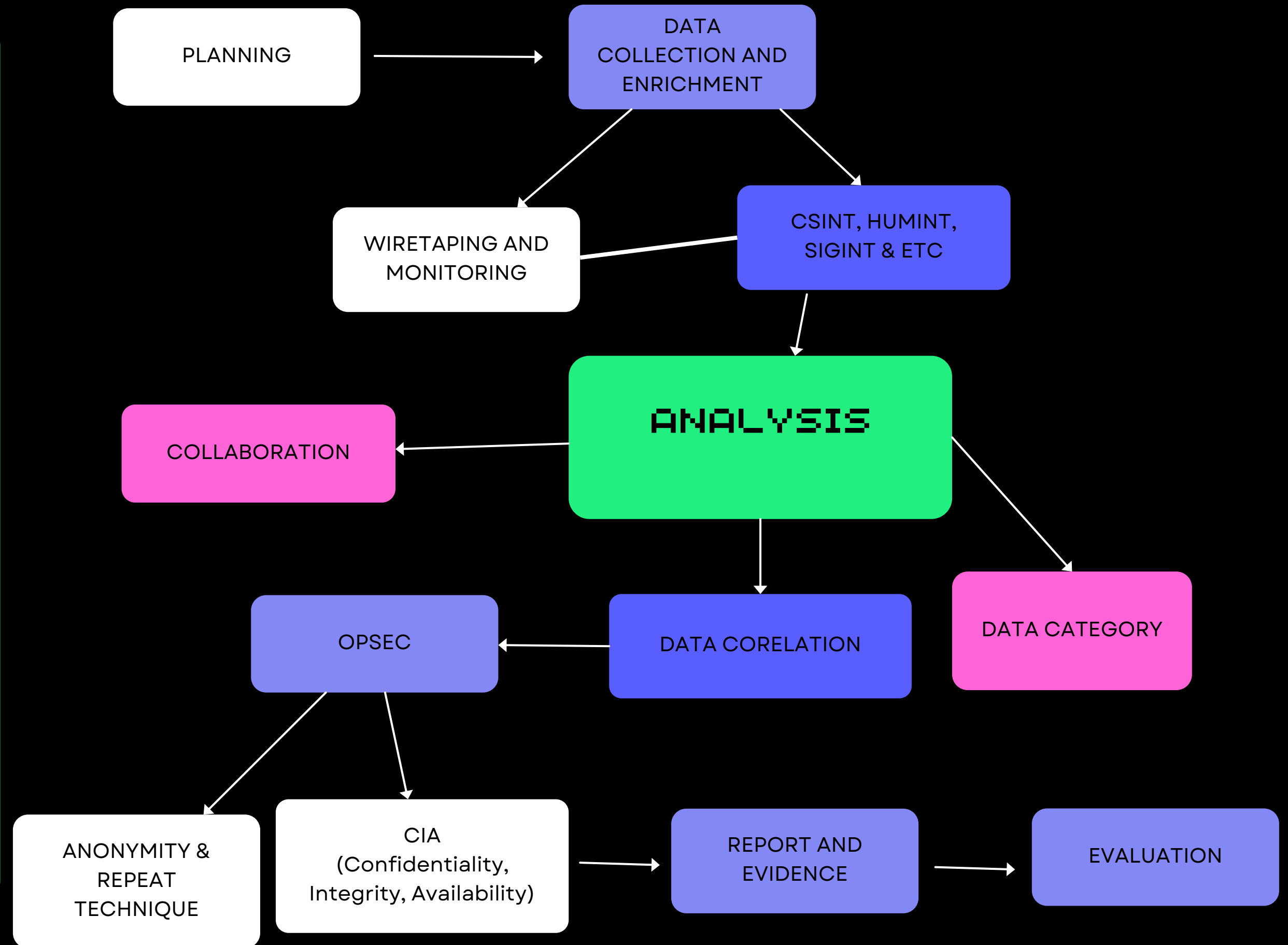
SIGN IN



BACK TO AGENDA PAGE



CYCLE OF INTELLIGENCE



JIEYAB89 THINGS IN OSINT

J

Jieyab89-OSINT-Cheat-sheet-Wiki-Tips

Search...Ctrl K

Welcome

OSINT RESOURCES

OSINT Resources

INTELLIGENCE BASE

Home

Intelligence Base & Knowledge Base

All About Doxing

All About OSINT Matters Things in OSINT

All About SIGINT Signal Intelligence

Cell Investigations

Geospatial Intelligence

How to OSINT Collection the Data

How to Verify Content & Discover Content

IMINT - Image and Video Analysis

OSINT for Academic Literature

OSINT for Email Lookup Tips

OSINT for Historical

OSINT for Journalism

OSINT for OPSEC

Powered by GitBook

INTELLIGENCE BASE

Copy

🔗

All About OSINT Matters Things in OSINT

How to start gather information in OSINT something you should know and understand

```
graph LR; Start([Start]) --> Unknown[/Unknown Target/]; Start --> Known[/Known Target/]; Unknown --> Dorking1[Dorking & Scrapping]; Known --> Dorking2[Dorking & Scrapping]; Dorking1 --> Check1[Checking Their Info]; Dorking2 --> Check2[Checking Their Info]; Check1 --> Validate{Validate}; Check2 --> Validate; Validate -- Yes --> Analysis[Analysis]; Validate -- No --> Search[Searching Other & Unique Info]; Search --> Analysis; Analysis --> Archives[Archives]; Archives --> Finish([Finish]);
```

Several stages in the OSINT search. Things to know and do:

1. Know your search object, define variables for the search object e.g. name, company, information to search for
2. Perform multiple data searches, such as you can do dorking or scrapping for data searches. You can also utilize data brokers to complete your data. After that, collect your data and prepare some comparative data as well as save some existing evidence
3. Checking the information, is the object you are looking for correct? Chek some other variables such as, close friends for example or other information contained with your target, look and observe
4. Validate, check some of the data you find for example from satellite data, existing datasets, sensor data and make sure there are 5W + 1H elements to get the essence and differentiation of the data object you are looking for, observe to make sure there are no differences and data manipulation (BIAS)

ON THIS PAGE

How to start gather information in OSINT something you should know and understand

- Legit Check
- Propaganda
- Deepfake
- Timezone
- Geospatial
- Mental and Psychology
- BIAS
- Laws
- Risk
- Captcha and Rate Limiting (WAF)
- Confidential
- Transaction
- Combat Tools (OPSEC)
- Language
- Platform ToS (Term and services)
- Knowing Your Area
- Blind Spot
- Espionage and Wiretapping or Human Error
- User or Account Privacy Settings

🌞

🖨

🌙

OPSEC TIPS FOR OSINT

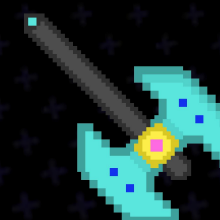
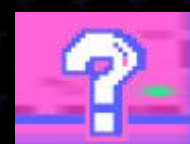
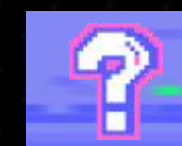
SIGN IN



[BACK TO AGENDA PAGE](#)



OPSEC



OPSEC FOR OSINT

J

Jieyab89-OSINT-Cheat-sheet-Wiki-Tips

Search...

CtrlK

SCRIPT FOR OSINT

RESOURCES USAGE

Home

How to Spot a Deepfake

Guide Satellite Imagery

What is Social Engineering

Sexual Abuse - How to Revenge

OSINT for Military

OSINT for Journalist and Activist

OSINT for Blockchain

OSINT and SOCMINT Tips

All About HUMINT

Levaraging AI Agent (LLM) for OSINT

OSINT for Medic and Forensic Dead Body

Protect Your Fingerprint and Sock Account

Hardware Pentesting

Red Team and Wiretapping

Attacking AI and ML Prompt Injection

All About Darkweb

Powered by GitBook

INTELLIGENCE BASE

Copy

OSINT for OPSEC (Operational security)

What is OPSEC (Operational security)?

How to Threat Model for OPSEC

What is the OPSEC process?

Why is OPSEC important?

Why is OPSEC important to OSINT investigators?

Best Practices for Good OPSEC

What is OPSEC (Operational security)?

OPSEC stands for Operational Security and is a term derived from the United States Military. Since its introduction, OPSEC has been adopted by many organizations and sectors to safeguard sensitive information in various contexts beyond the military. The objective of OPSEC is to prevent sensitive information from getting into the hands of an adversary, primarily by denying access to the data. First, we want to identify the data that can be compromised and then take steps to reduce the exploitation of this data and minimize the risk.

How to Threat Model for OPSEC

OPSEC is not a static concept. Depending on the types of activities you are conducting, you will need to adapt your OPSEC measures. In order to evaluate your activities, their risk, and the necessary measures to be implemented, we need to conduct threat modelling. This allows us to determine the degree of security which we want to achieve. This threat modelling can be done in a fairly informal manner, merely by taking the time to write down the basic information pertaining to the following points:

- Know your target. A project investigating Threat Actors or organized crime groups, or malware and its developer, has a different level of OPSEC requirements from a project looking into the social media profile of a 16-year-old forum troll.
- Identify potential threats. Possible threats to sensitive data need to be identified and potentially documented. Consider that threats may exist externally through third parties, as well as internally. Data theft or breaches (either accidental or deliberate) can publish a wealth of data about you personally without your knowledge.

ON THIS PAGE

What is OPSEC (Operational security)?

How to Threat Model for OPSEC

What is the OPSEC process?

Why is OPSEC important?

Why is OPSEC important to OSINT investigators?

Best Practices for Good OPSEC

⚙️

🖨️

🌙

OPSEC TIPS FOR OSINT

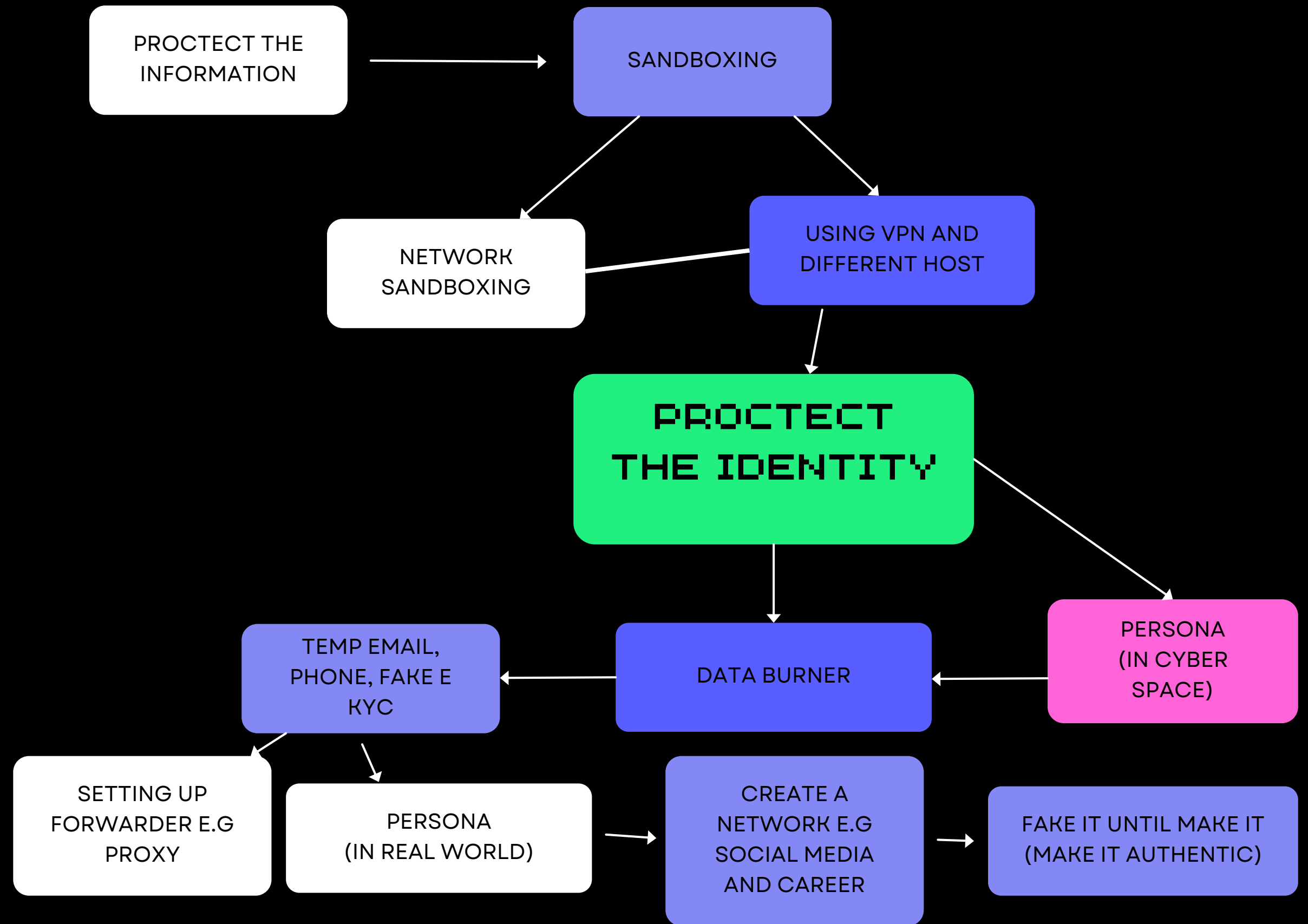
FUNDAMENTAL OF OPSEC

➤ CONFIDENTIALITY

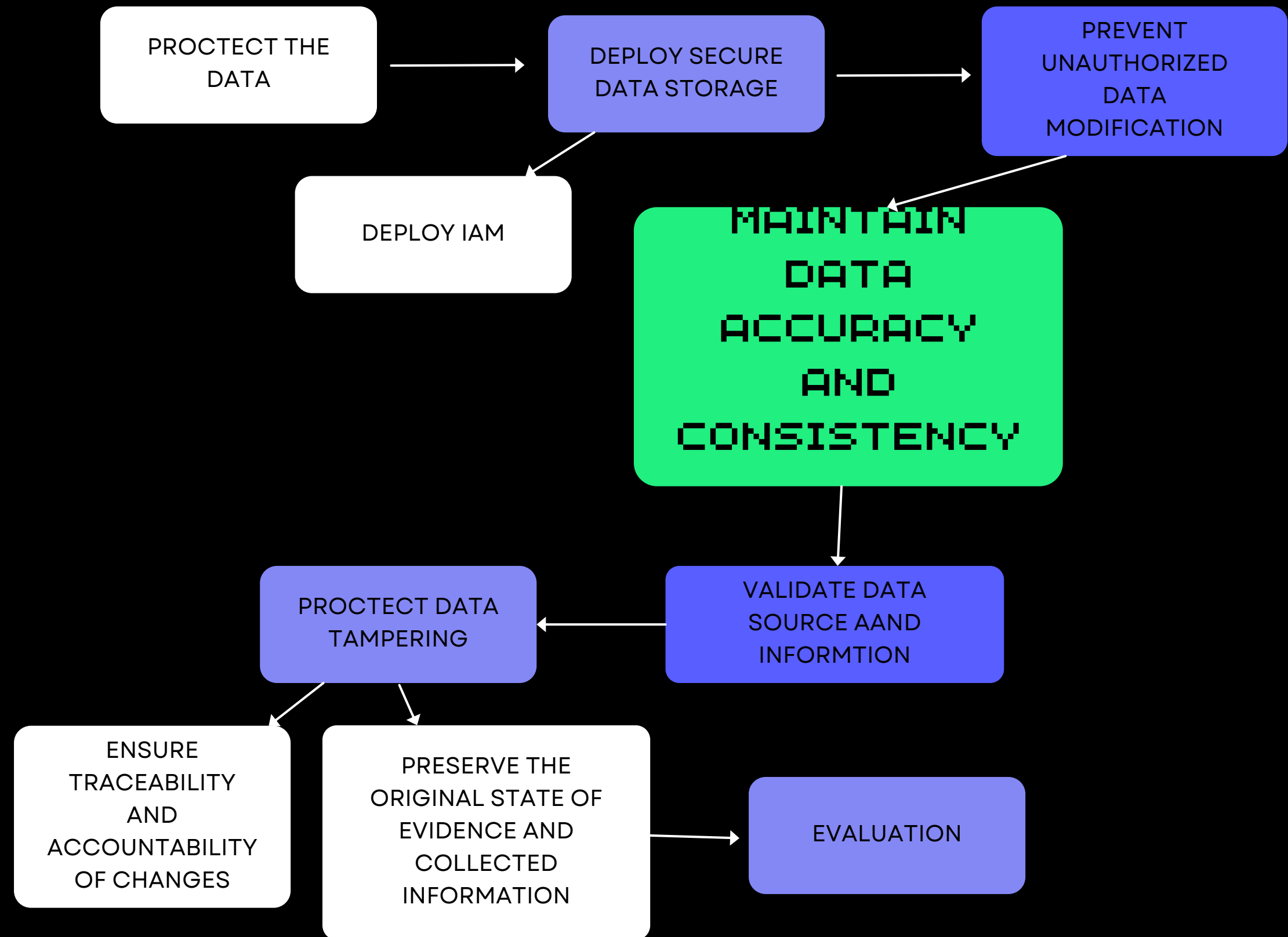
➤ INTEGRITY

➤ AVAILABILITY

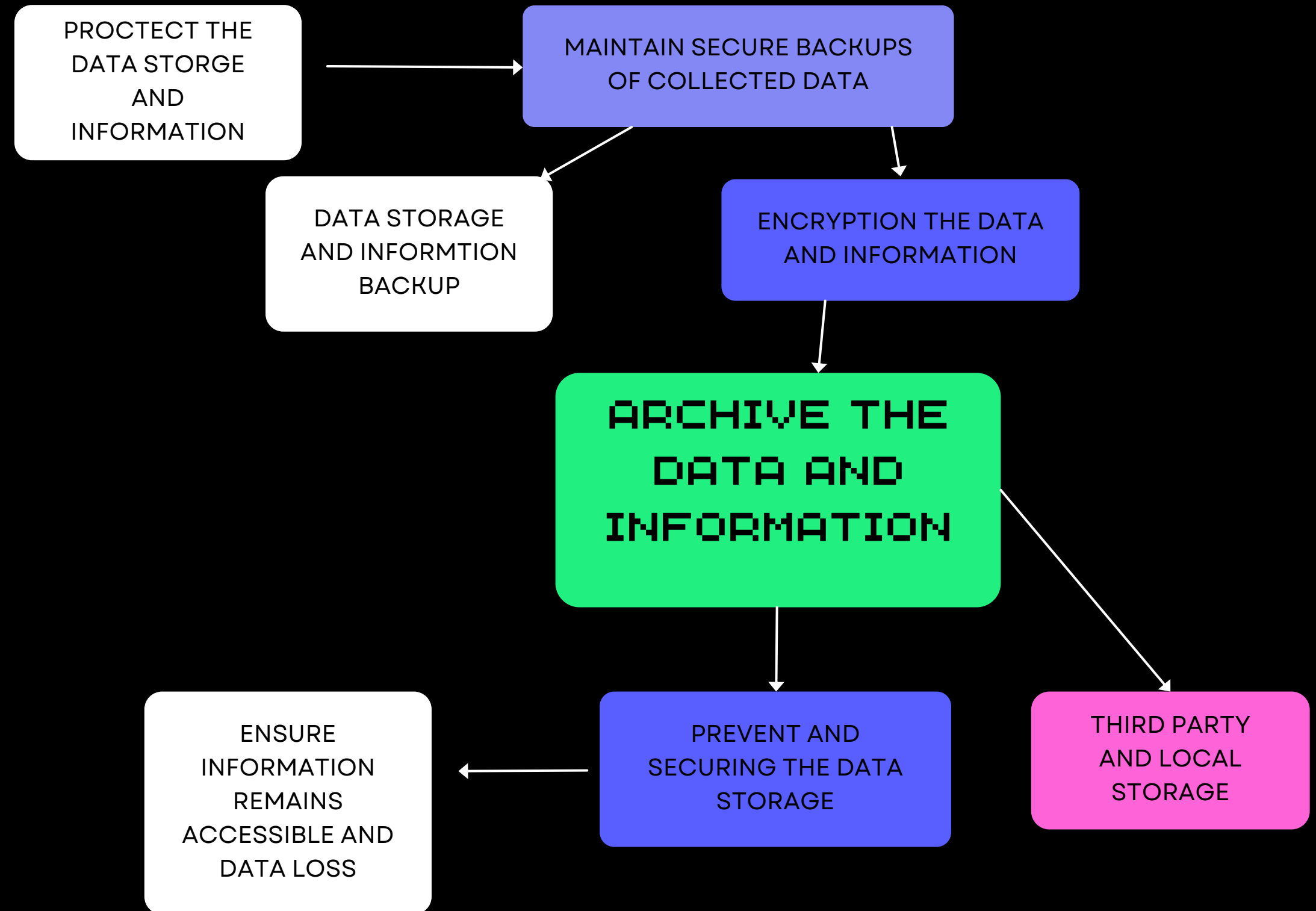
CONFIDENTIALITY



INTEGRITY



AVAILABILITY



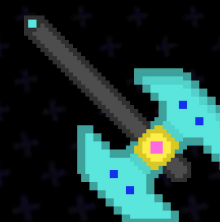
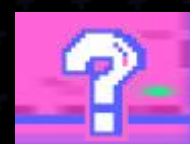
SIGN IN



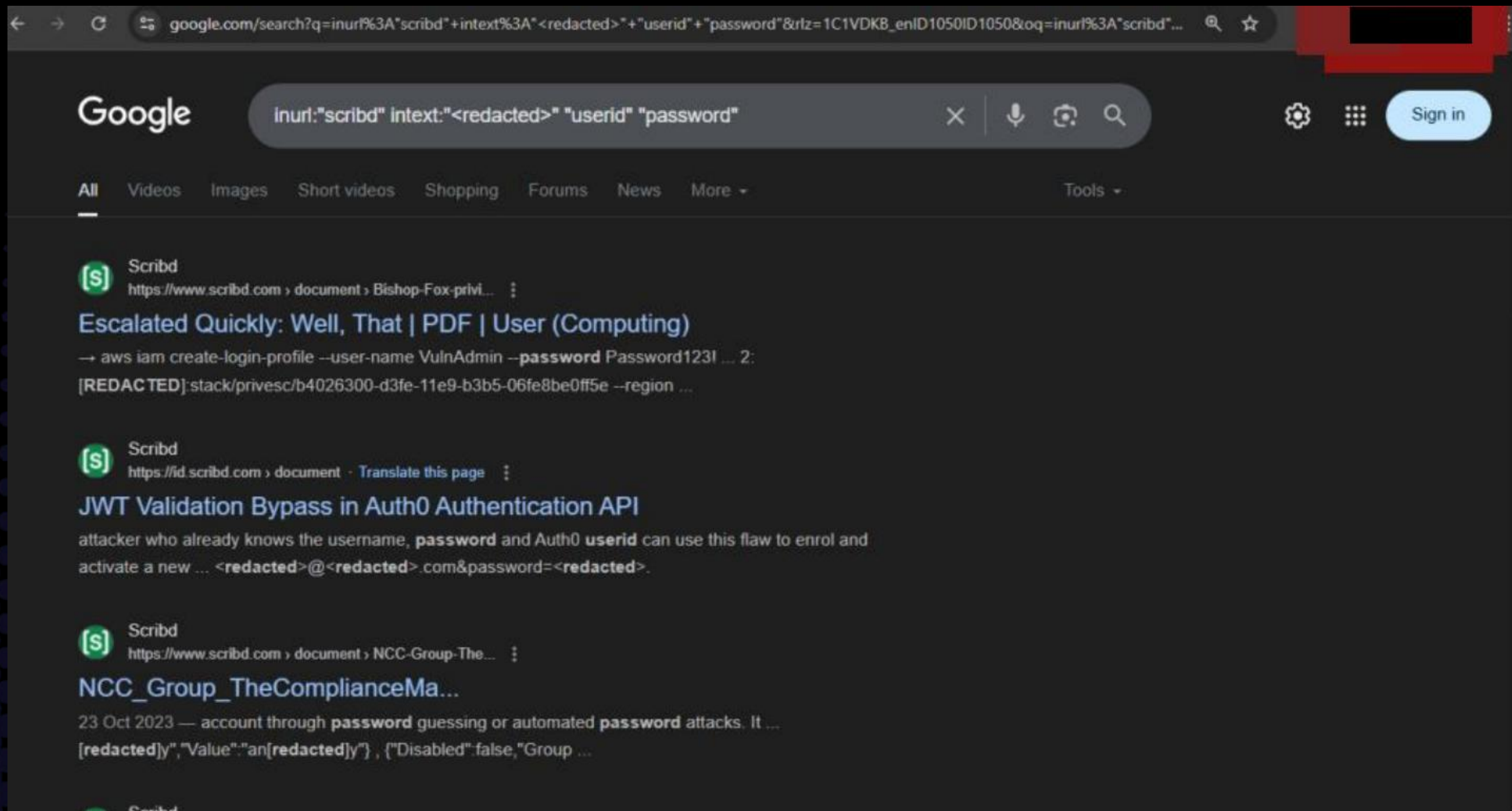
BACK TO AGENDA PAGE



OSINT BASIC PRACTICE

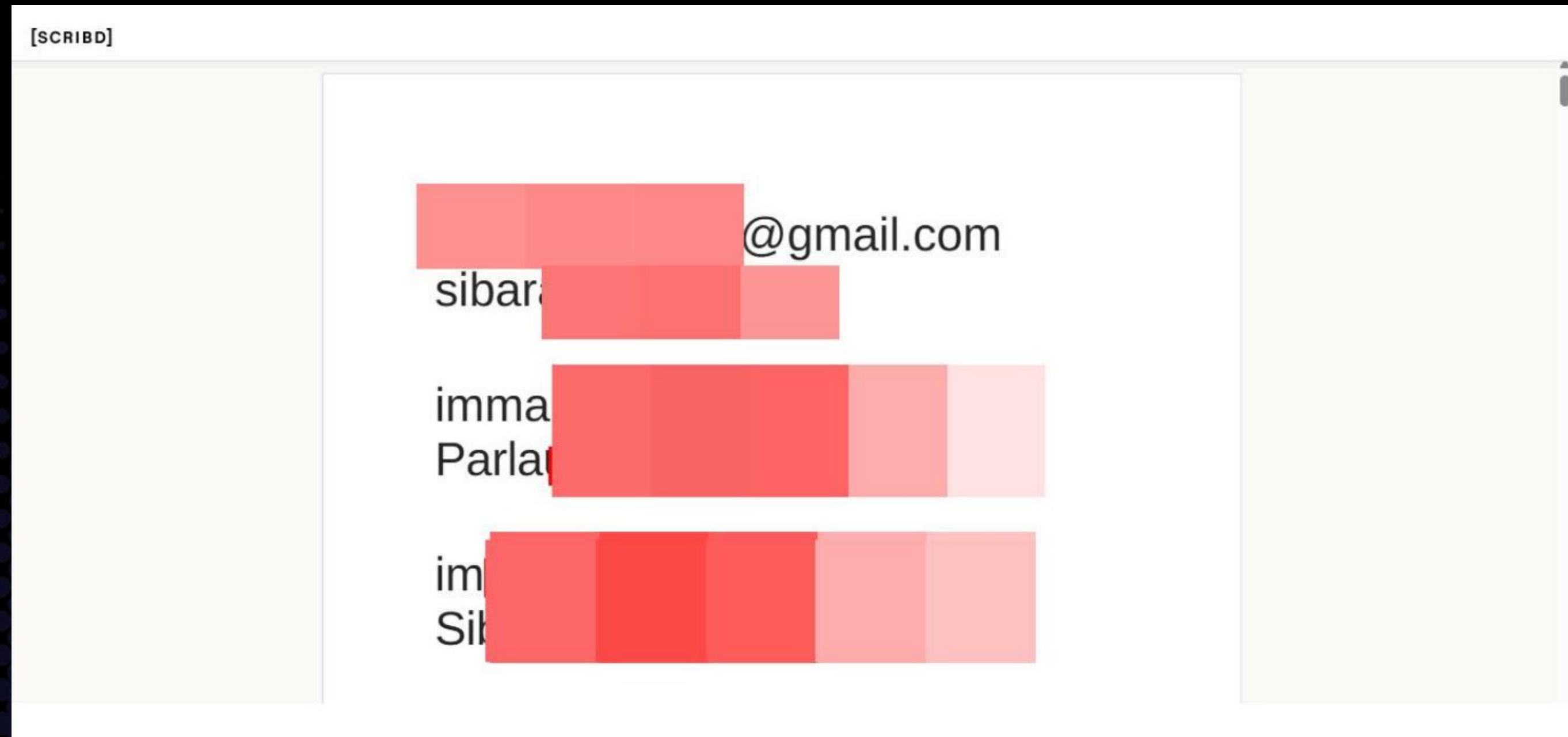


GOOGLE DORKING



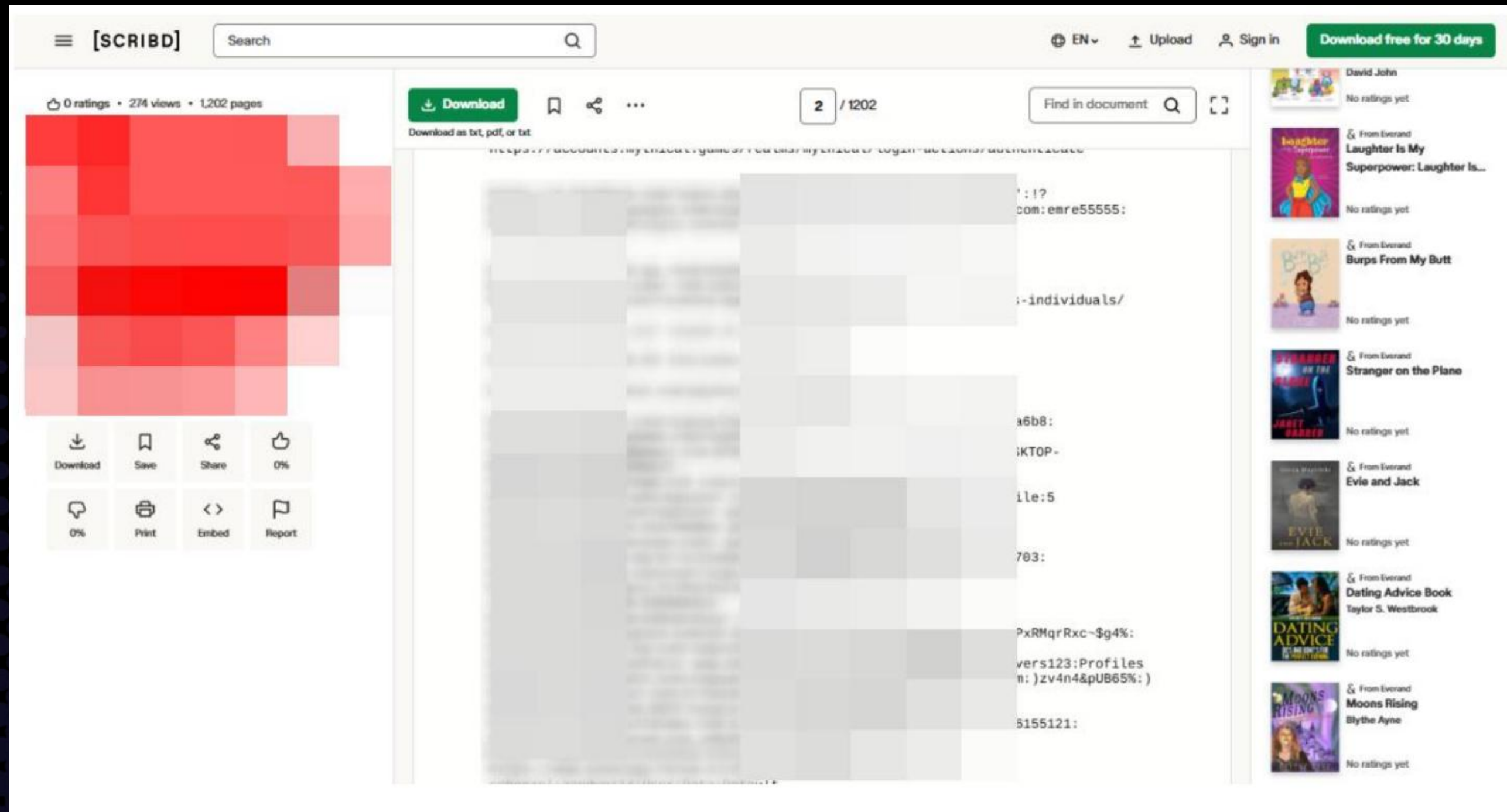
GOOGLE DORKING

GOOGLE DORKING



GOOGLE DORKING

GOOGLE DORKING



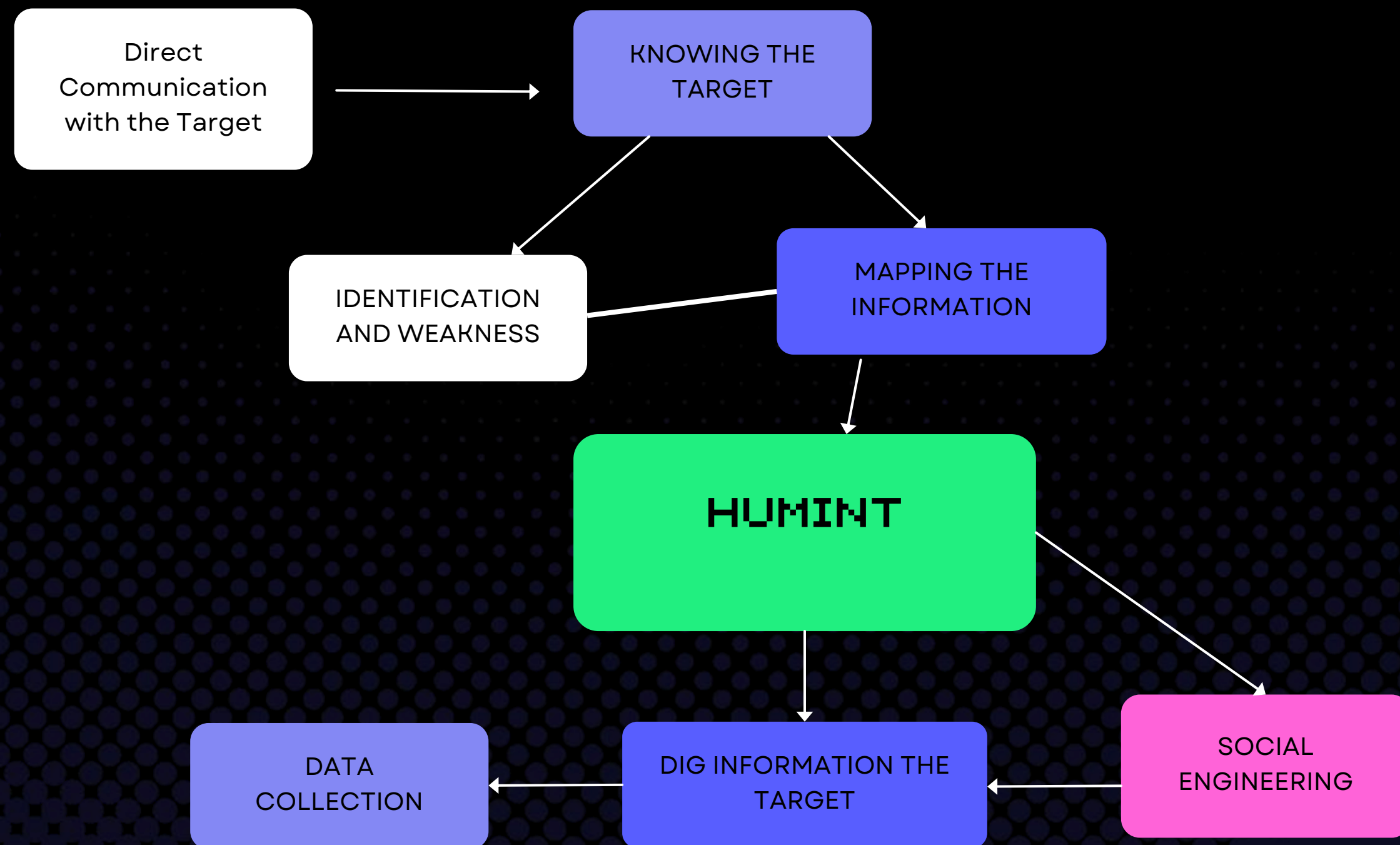
GOOGLE DORKING

RECONNAISSANCE

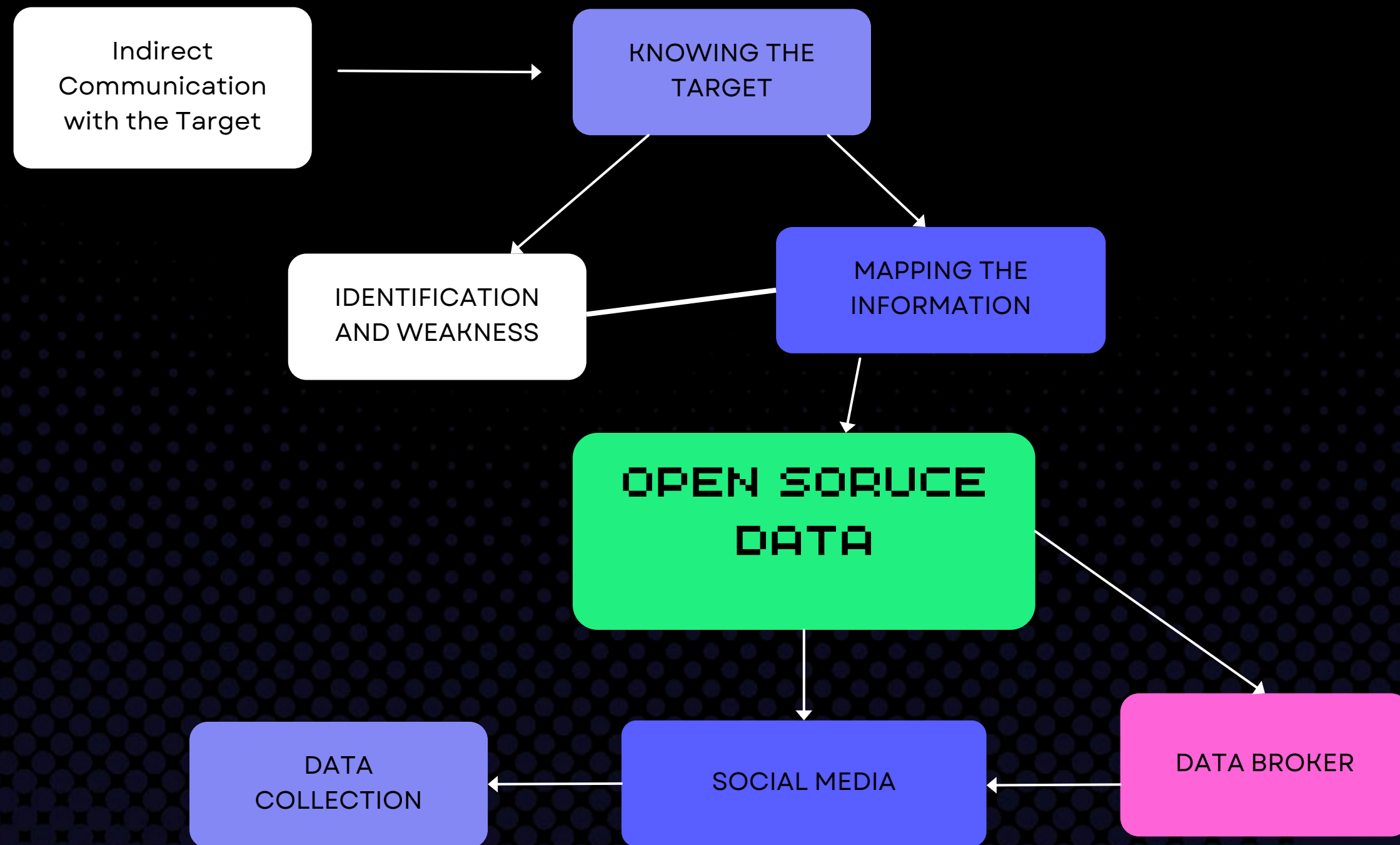
➤ ACTIVE RECON

➤ PASSIVE RECON

RECONNAISSANCE - ACTIVE



RECONNAISSANCE - PASSIVE



RECONNAISSANCE - ACTIVE

➤ REALTIME DATA AND INFORMATION

➤ ACCESS TO ADDITIONAL INFORMATION AND HIGH RISK OF DETECTION

➤ DEEPER INSIGHT AND HIGH COST

RECONNAISSANCE - PASSIVE

➤ LIMITED DATA AND INFORMATION

➤ LEGAL AND ETHICAL SAFETY AND LOW RISK OF DETECTION

➤ COST-EFFECTIVE AND OPEN SOURCE DATA

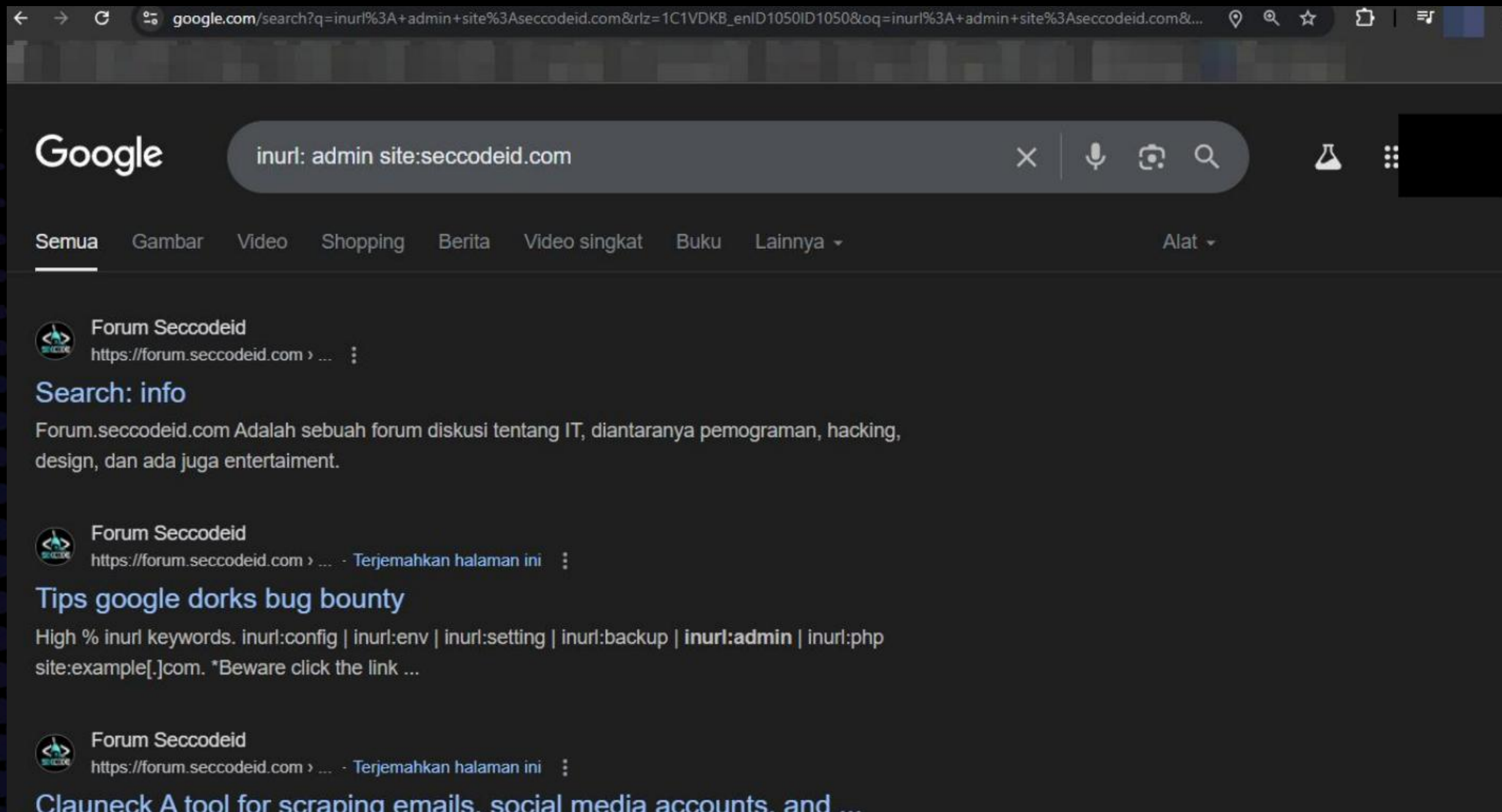
RECONNAISSANCE - ACTIVE EXAMPLE



```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ rustscan -a 10.10.10.239  
  
[~] RustScan 2.0.2  
[~] The Modern Day Port Scanner.  
[~] : http://discord.skerritt.blog :  
[~] : https://github.com/RustScan/RustScan :  
[~] RustScan: Where '404 Not Found' meets '200 OK'.  
[~] The config file is expected to be at "/home/kali/.rustscan.toml"  
[!] File limit is lower than default batch size. Consider upping with --ulimit. May cause harm to sensitive servers  
[!] Your file limit is very small, which negatively impacts RustScan's speed. Use the Docker image, or up the Ulimit with '--ulimit 5000'.  
Open 10.10.10.239:80  
Open 10.10.10.239:82  
Open 10.10.10.239:135  
Open 10.10.10.239:139  
Open 10.10.10.239:443  
Open 10.10.10.239:445  
[~]
```

ACTIVE
RECCON

RECONNAISSANCE - PASSIVE EXAMPLE



PASSIVE
RECCON

OSINT TOOL LIST

Jieyab89 / OSINT-Cheat-sheet

Type to search

<> Code

Issues

Pull requests

Discussions

Actions

Projects

Wiki

Security

Insights

Settings

OSINT-Cheat-sheet

Public

Pin

Watch

Fork 231

Starred 1.5k

main

Branches

Tags

Add file

<> Code

About

725 Commits

Jieyab-Presentation-Archive

Script

Web-Based

mail

wiki

README.md

awesome-article.md

contribution.md

OSINT cheat sheet, list OSINT tools, wiki, dataset, article, book , red team OSINT for hackers and OSINT tips and OSINT branch. This repository will grow every time will research, there is a research, science and technology, tutorial. Please use it wisely.

jieyab89.github.io/OSINT-Cheat-sheet/W...

science education osint tools

wiki scraping hacking journalism

cheatsheet cybersecurity datasets

information-security red-team

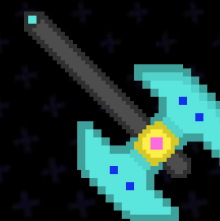
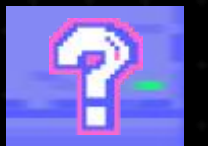
information-gathering reconnaissance

socmint osint-tool imint masint

SIGN IN



BACK TO AGENDA PAGE



MENU



THANK YOU!

