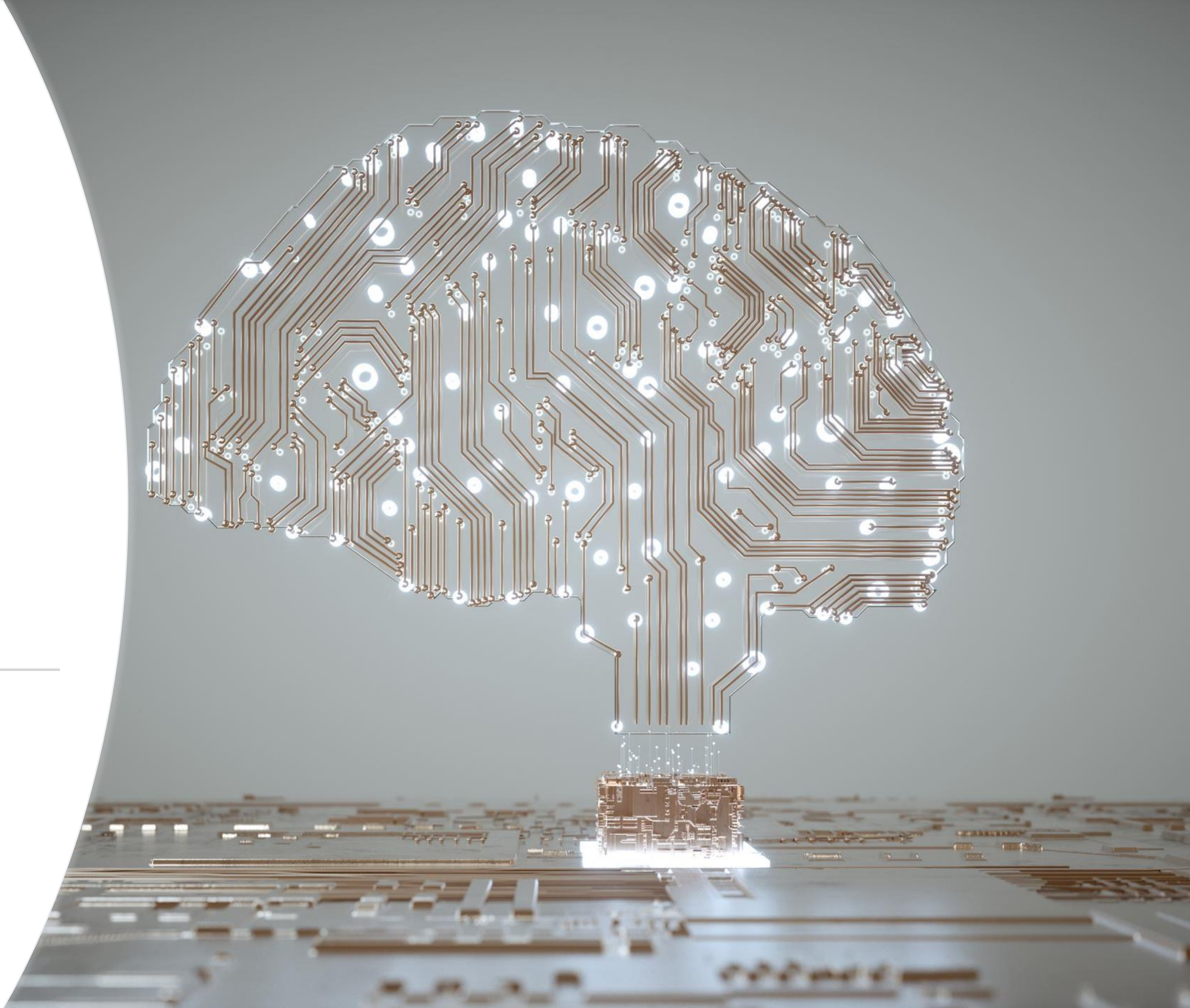
Intelligence Collection

Cybersecurity Student Association



Open-Source Intelligence (OSINT)

- **What is OSINT?**
  - Open-source intelligence (OSINT) is the collection and analysis of public information
  - Sources include the internet, news media, social media, and government documents
- **Why is it important?**
  - Provide information that theoretically everyone has access to
  - Can reveal to an organization how much publicly exposed data is open source
  - Provides real time news and data like social media to show where hackers might move next
- **How to collect it**
  - Manual searches, automated tools, social media monitoring, and RSS ingestion
- **Tools and resources**
  - Maltego, The Harvester, Recon-NG, social-analyzer
  - https://github.com/topics/osint-tools
  - https://github.com/OffcierCia/non-typical-OSINT-guide

Human Intelligence (HUMINT)

What is HUMINT?

Human intelligence (HUMINT) is the collection of information through human interaction like interviews, conversations, observations, or espionage

Why is it important?

HUMINT is essential to threat intelligence as it can reveal plans from adversaries that are not publicly available as well as identify their motivations

How to collect it

Interviews, conversations, observation, espionage, and social engineering

Ethics and considerations

Respect the privacy of others, for intelligence collection reasons only (not manipulation)

https://github.com/giuliacassara/awesome-social-engineering

Cyber Intelligence (CYBINT)

What is CYBINT?

Cyber Intelligence (CYBINT) is the collection of information about cyber threats and vulnerabilities.

Why is it important?

Companies need to understand the connection and patterns between attacks against your organization and other organizations.

Provides information for companies to mitigate common attacks in their industry and against common vulnerabilities

How to collect it

Network traffic analysis, malware analysis, syslog and event log analysis, vulnerability scanning

News aggregators and parsers

Tools and Resources

https://freshrss.org/index.html

https://github.com/okhosting/awesome-cyber-security

https://github.com/vatsalgupta67/All-In-One-CyberSecurity-Resources

Signals Intelligence (SIGINT)

What is SIGINT?

Signals intelligence (SIGINT) is the collection of electronic signals such as radio, radar, and communication signals.

Why is it important?

Can provide communications from adversaries on next targets

Extremely useful for governments to understand where nations may attack physically or digitally next

How to collect it

Interception of electronic communications, monitoring radio and radar signals, analysis of satellite imagery

Software Defined Radio

Legal and Ethical Considerations

When collecting this kind of information, please remember to be ethical and law-abiding.

If you aren't sure what you are doing is legal, research it first!

The importance of combining OSINT, HUMINT, CYBINT, and SIGINT

A holistic approach to threat intelligence

Understanding the threat landscape with more depth

Find inconsistencies and deeper truths beyond what one can give

Involves both past intelligence and timely intelligence

Gaining a deeper understanding of adversaries

Understand threats from every angle

Create countermeasures to those threats more actively

Synthesize intelligences to create a map of threat activity to predict next attacks

OSINT Collection Methods

- Search engines and social media
  - Social-analyzer
  - Google Dorking
- Public Records and Databases
  - Voter Registration, Genealogy tools (MyHeritage, Ancestry, Family Search)
  - Phone Books
  - https://www.shodan.io/
  - https://ipinfo.io/
  - https://scamalytics.com/
- News Sources
- OSINT Tools
  - Maltego, theHarvester, recon-ng, WIGLE
  - https://github.com/jivoi/awesome-osint
  - https://github.com/Jieyab89/OSINT-Cheat-sheet

OSINT DEMO

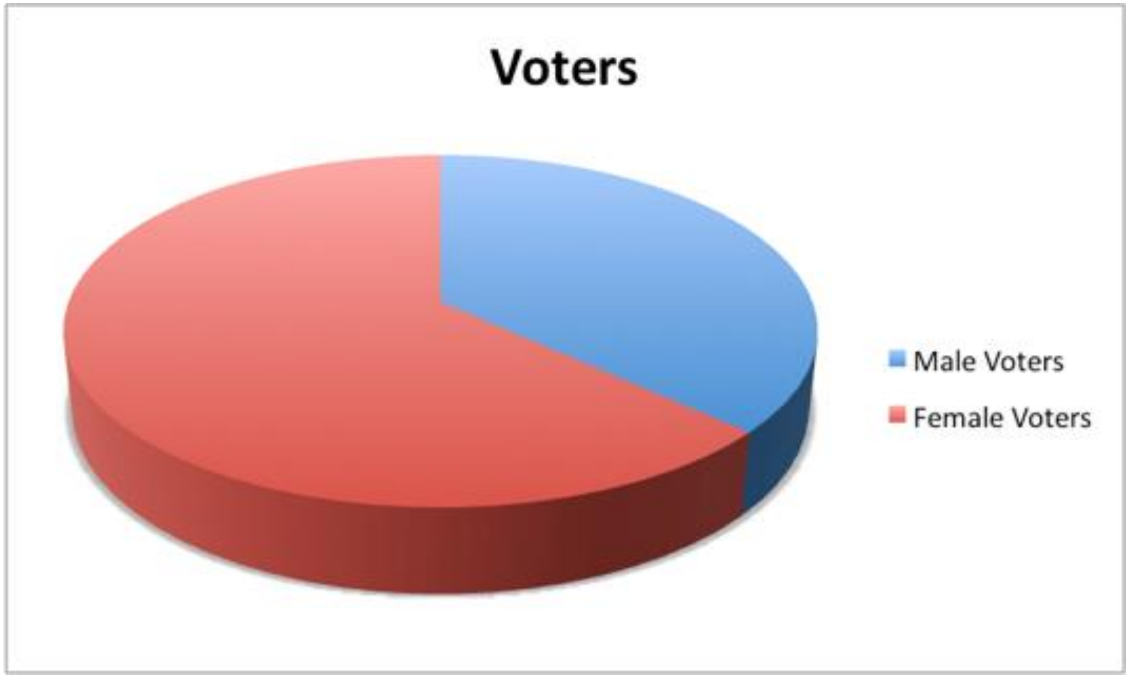
HUMINT Collection Methods

- Phishing, Vishing, Smishing
- Social Engineering
- Espionage
- Interviews
- Observation

Real –World Examples

- https://www.youtube.com/watch?v=xuYoMs6CLEw
- https://www.leadingauthorities.com/speakers/video/rachel-tobac-watch-cnn-reporter-get-hacked

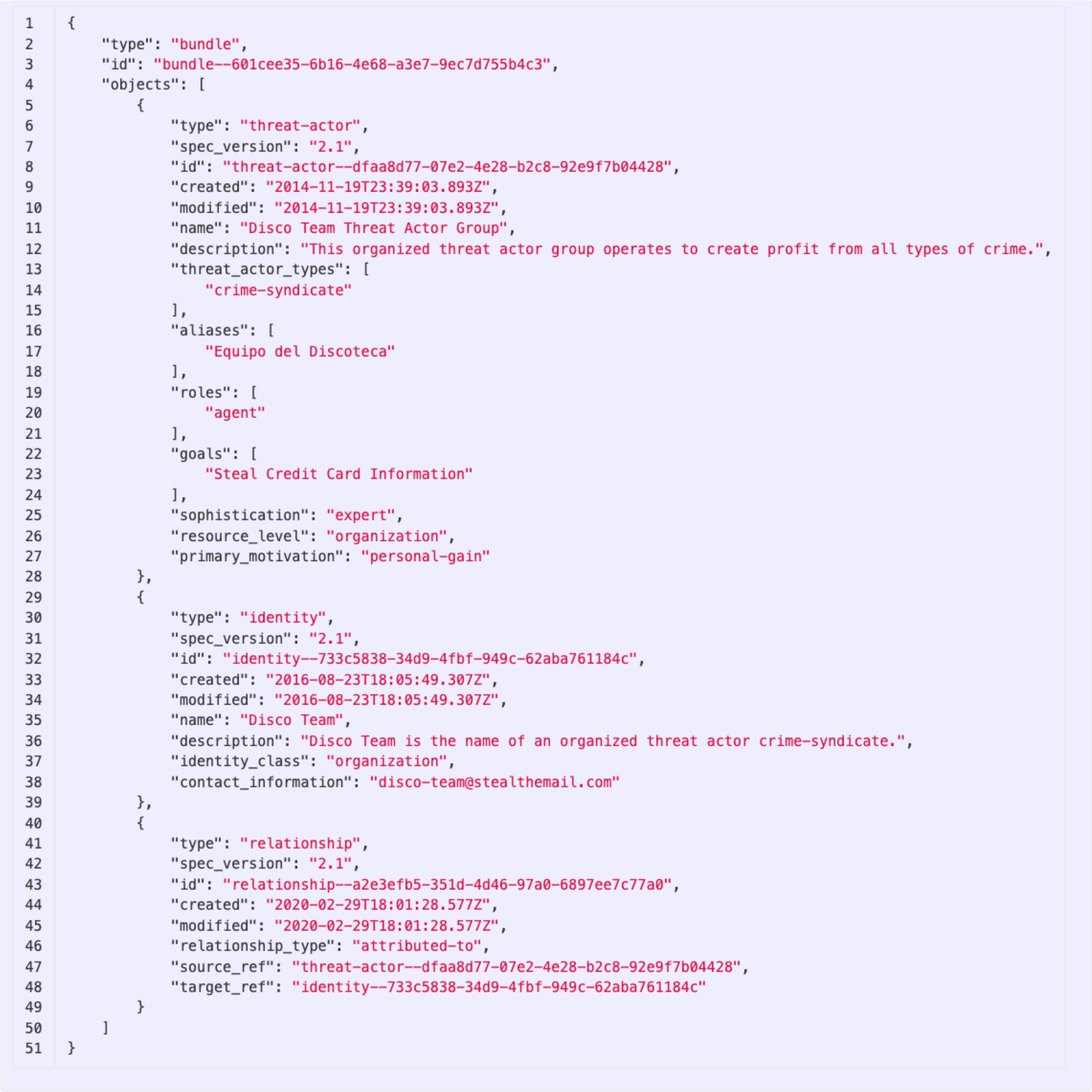
- Statistics



CYBINT Collection Methods

- Network Traffic Analysis
- Malware Analysis
- Syslog and Event Log Analysis
- Vulnerability Scanning
- News Sources
- STIX Sources

STIX Example



```
{
    "type": "bundle",
    "id": "bundle--601cee35-6b16-4e68-a3e7-9ec7d755b4c3",
    "objects": [
        {
            "type": "threat-actor",
            "spec_version": "2.1",
            "id": "threat-actor--dfaa8d77-07e2-4e28-b2c8-92e9f7b04428",
            "created": "2014-11-19T23:39:03.893Z",
            "modified": "2014-11-19T23:39:03.893Z",
            "name": "Disco Team Threat Actor Group",
            "description": "This organized threat actor group operates to create profit from all types of crime.",
            "threat_actor_types": [
                "crime-syndicate"
            ],
            "aliases": [
                "Equipo del Discoteca"
            ],
            "roles": [
                "agent"
            ],
            "goals": [
                "Steal Credit Card Information"
            ],
            "sophistication": "expert",
            "resource_level": "organization",
            "primary_motivation": "personal-gain"
        },
        {
            "type": "identity",
            "spec_version": "2.1",
            "id": "identity--733c5838-34d9-4fbf-949c-62aba761184c",
            "created": "2016-08-23T18:05:49.307Z",
            "modified": "2016-08-23T18:05:49.307Z",
            "name": "Disco Team",
            "description": "Disco Team is the name of an organized threat actor crime-syndicate.",
            "identity_class": "organization",
            "contact_information": "disco-team@stealthemail.com"
        },
        {
            "type": "relationship",
            "spec_version": "2.1",
            "id": "relationship--a2e3efb5-351d-4d46-97a0-6897ee7c77a0",
            "created": "2020-02-29T18:01:28.577Z",
            "modified": "2020-02-29T18:01:28.577Z",
            "relationship_type": "attributed-to",
            "source_ref": "threat-actor--dfaa8d77-07e2-4e28-b2c8-92e9f7b04428",
            "target_ref": "identity--733c5838-34d9-4fbf-949c-62aba761184c"
        }
    ]
}
```

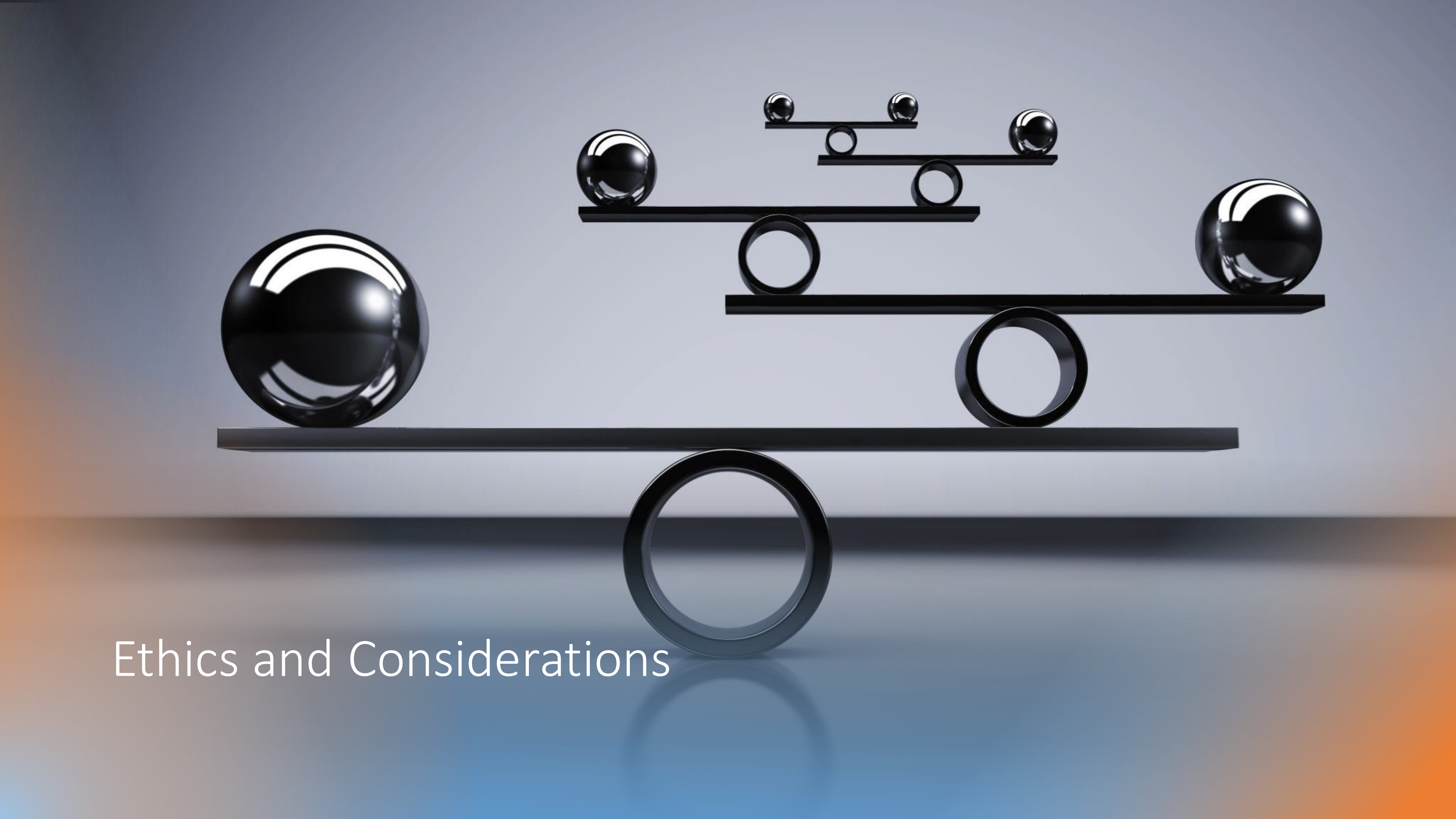
FreshRSS

DEMO

SIGINT Collection Methods

- Software Defined Radio (Demo)
- Tapping Wires

RTL-SDR.COM
QUICKSTART SETUP GUIDE: RTL-SDR.COM/QSG
DVB-T+DAB+FM+SDR
RTL2832U R820T2 TCXO+BIAS T+HF
V3



Ethics and Considerations

Questions?