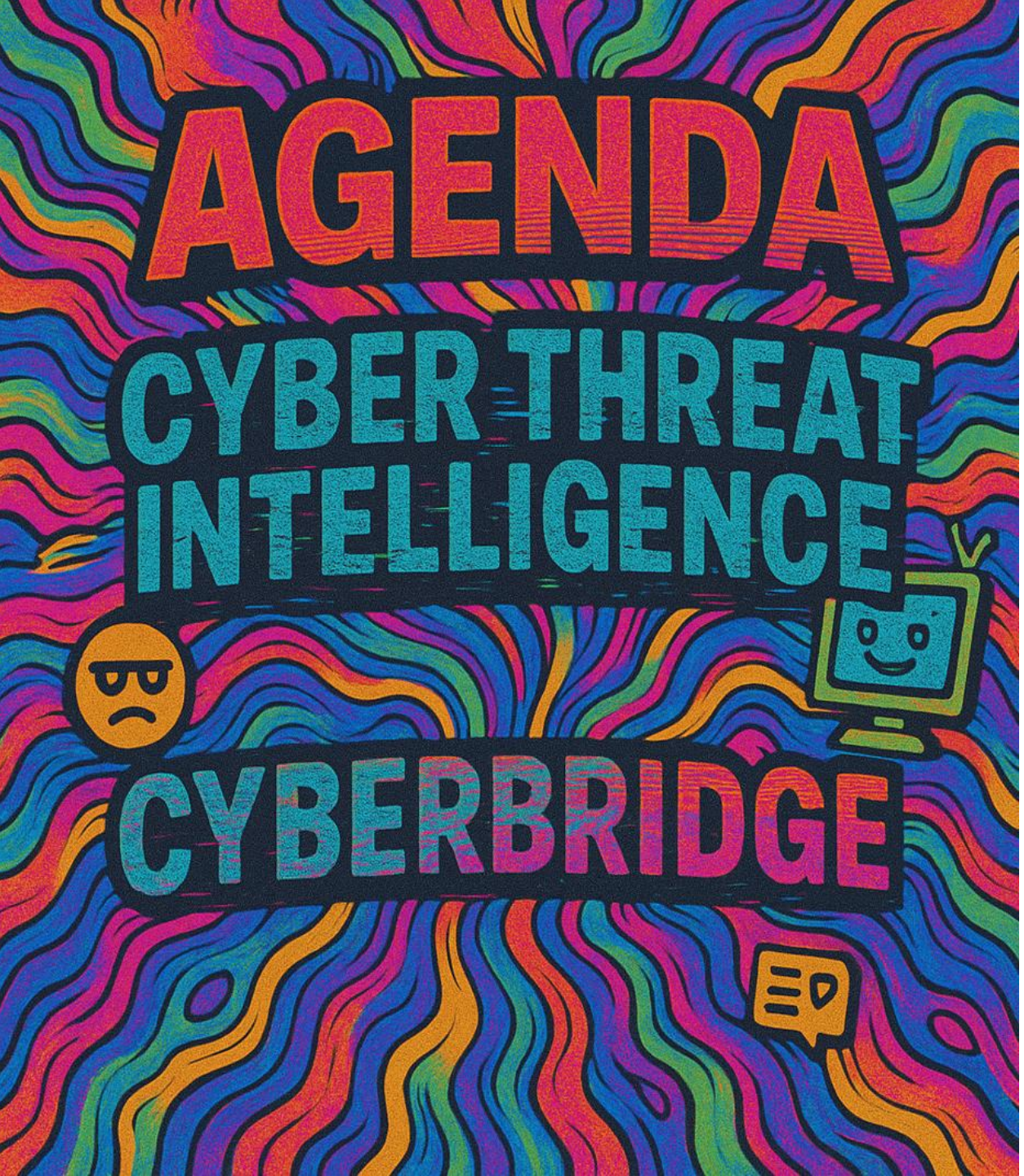
.the tech collective
powered by Implement

CYBERBRIDGE SUMMER BOOTCAMP

CYBER THREAT INTELLIGENCE IN PRACTICE

– FROM PROCESS TO PLATFORM



- What is Cyber Threat Intelligence (CTI)
  - The CTI Lifecycle
  - Sources and Collection Methods
  - Applications and Use Cases of CTI
- What is OSINT?
  - Utilising OSINT to solve challenges
  - OSINT Collection
- Obsidian
  - Second Brain
  - Exercise
- OSINTer
- CTI Competition

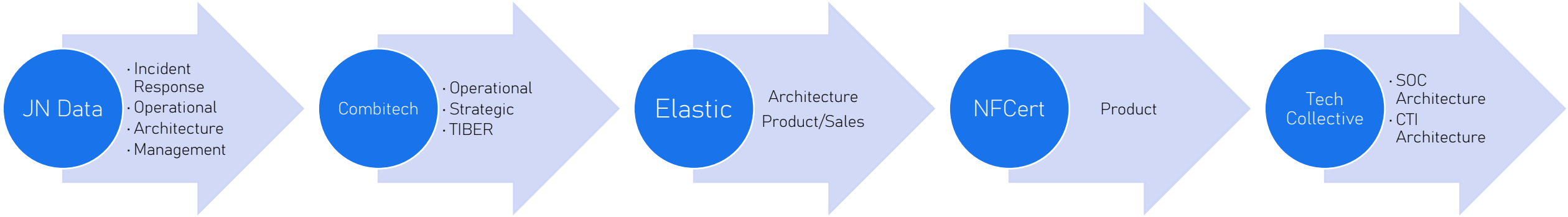
.the tech collective
powered by Implement

whoami

- 11 years in Cyber Security
  - Architecture (SIM3 Auditor)
- Co-Founder (OSINTer)
- Community Supporter
  - Guest Lecturer
  - Education Advisor
  - CTF Organiser
- Blogger
- And much much more…

.the tech collective
powered by Implement

My career so far



.the tech collective
powered by Implement

What is Cyber Threat Intelligence?

What Is Cyber Threat Intelligence?

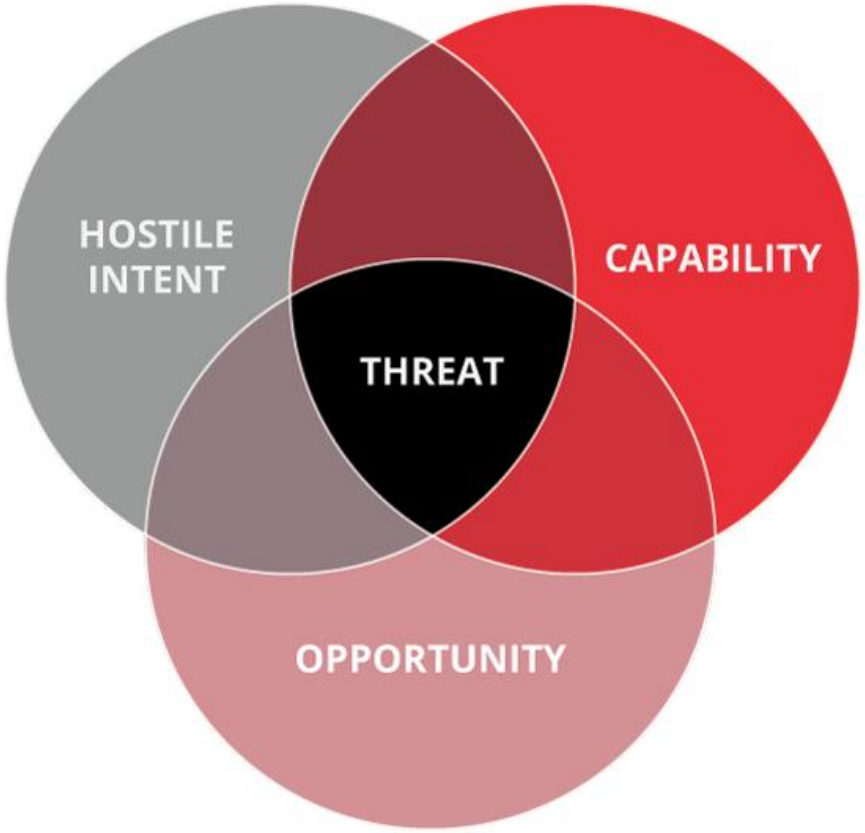
- Cyber Threat Intelligence involves gathering and analyzing data about cyber threats to enhance security measures.

Purpose and Benefits

- It enables organizations to anticipate and prepare for cyber attacks, improving response and defense capabilities.

What is Threat?

What is a threat?



.the tech collective
powered by Implement

Lack of intent

.the tech collective
powered by Implement

Lack of capability

.the tech collective
powered by Implement

Lack of opportunity

.the tech collective
powered by Implement

Threat!

.the tech collective
powered by Implement

But what can we do?

INTENT

- Financially Motivated
- Espionage
  - Corporate
  - Nation State

Then what?

- Don't be successful
- Don't piss anyone off

.the tech collective
powered by Implement

CAPABILITY

- Tactics
- Techniques
- Procedures
  - (TTPs)
- Tools etc

Then what?

- Detection – Endpoint detect and response (EDR)
- Prevention – Anti Virus (AV)
- Response – Incident Response (IR)

.the tech collective
powered by Implement

- Vulnerabilities
  - Technical – CVE's
  - People – Social Engineering
    - Phishing
    - Spearphishing etc

Then what?

- Vulnerability Management
  - Tools
  - Processes
- User Awareness

.the tech collective
powered by Implement

Cyber Threat Intelligence

This is where CTI comes in…

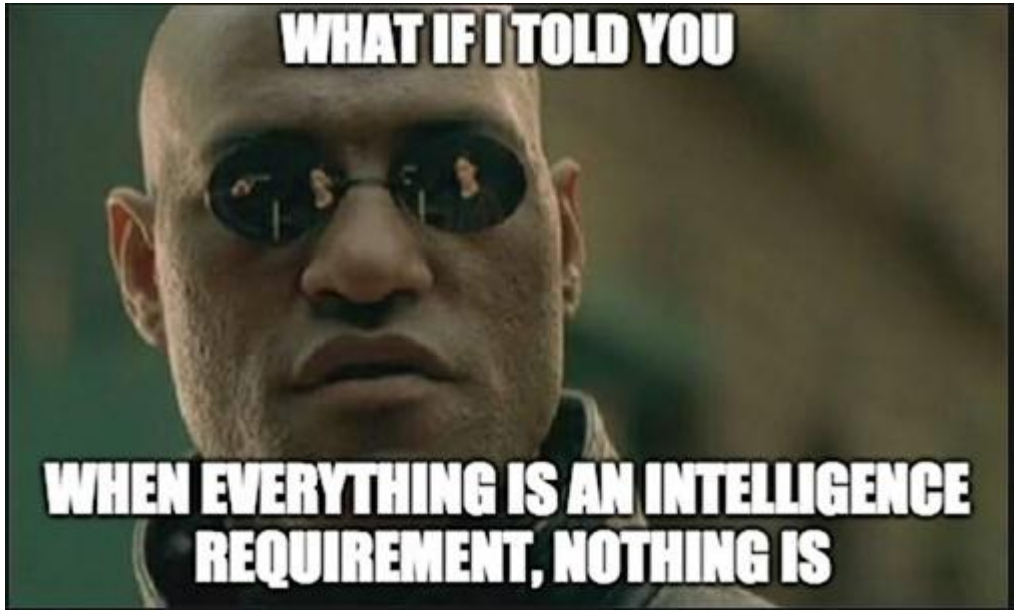
- CTI gives us a way of learning from previous cyber attacks
  - To understand what kind of capabilities and opportunities are being utilised out there in the wild.

But which ones are important to us/our organisation and why?

Intelligence Requirements

For me when I teach CTI or advise organisations on utilising CTI, I always like to link back to a set of questions.

What do you really want to know about what's happening to enable you or your org to make good decisions.



.the tech collective
powered by Implement

Break

Questions to ask...

"Which departments in my organisation caused the most incidents last year from being tricked by phishing."

This is a concrete question that we can go and find an answer for.

This answer will help decide where that awareness budget will be focused and will be used to reduce the opportunity for attackers.

Applications and Use Cases of CTI

Threat Detection and Incident Response

Improved Detection Capabilities

- Enhances threat detection by identifying patterns and potential indicators of compromise early.

Indicators of Compromise

- Provides detailed indicators that help identify malicious activity within networks promptly.

Threat Actor Behavior Analysis

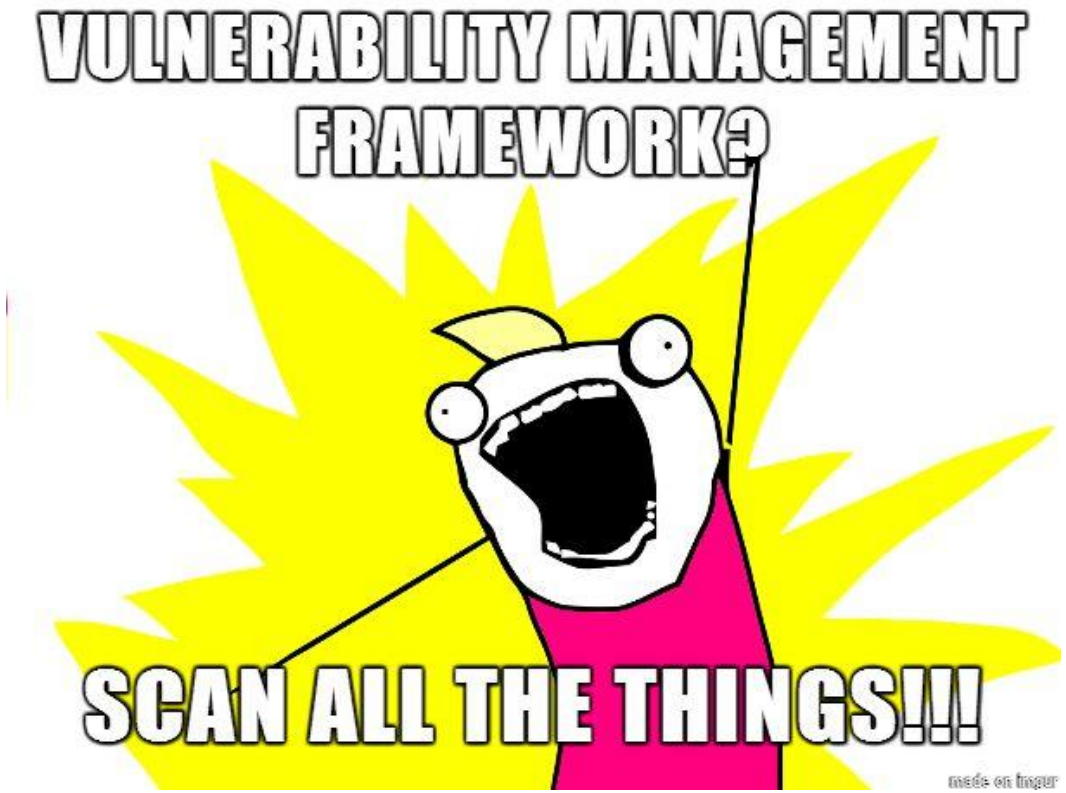
- Understanding threat actor behaviors enables anticipation and mitigation of emerging threats effectively.

Faster Incident Response

- Respond more quickly and effectively to security incidents.

.the tech collective
powered by Implement

Vulnerability Management and Risk Assessment



Attacker Methods Understanding

- Knowing attacker techniques helps identify and prioritize critical vulnerabilities effectively.

Prioritizing Vulnerabilities

- Prioritization based on threat intelligence ensures focused patching and mitigation efforts.

Optimizing Mitigation Efforts

- Risk assessments guide efficient allocation of resources for patching and defense strategies.

.the tech collective
powered by Implement

Strategic Decision-Making and Security Awareness

Leadership Insights for Security

- CTI provides leaders with up-to-date threat trends that guide strategic security decision-making and planning.

Employee Security Awareness

- Informed training programs enhance employee awareness of security risks and promote best practices in the workplace.

.the tech collective
powered by Implement

Types of CTI

Strategic Threat Intelligence

Focuses on high-level insights to support decision making and policy formulation in cybersecurity.

Tactical Threat Intelligence

Provides information on tactics and techniques used by adversaries to assist security teams.

Operational Threat Intelligence

Supports defense operations with timely and actionable information about ongoing threats.

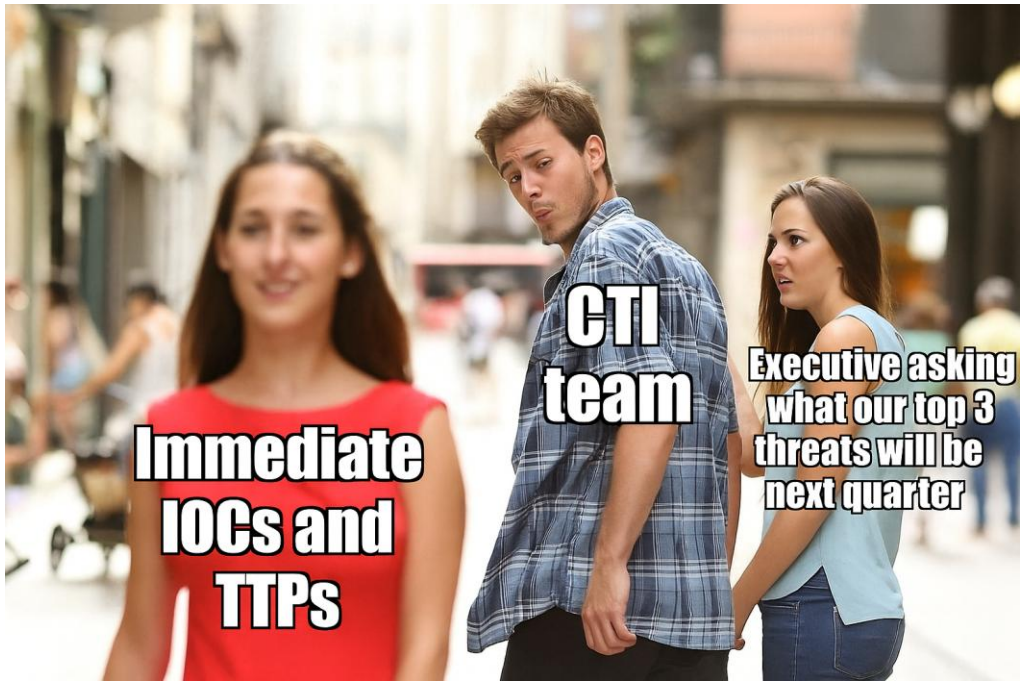
.the tech collective
powered by Implement

Strategic Questions

"What are the top emerging cyber threats to our industry over the next 12 months?"

"What is our exposure to supply chain compromise based on recent threat activity?"

"How do we compare to industry peers in terms of threat targeting and exposure?"



.the tech collective
powered by Implement

Tactical Questions

"What recent TTPs have been observed from actors targeting our tech stack?"

"What techniques are being used to bypass our current EDR or email filtering controls?"

"Are any known threat actors exploiting [[CVE-2025-XXXX]] in the wild?"

.the tech collective
powered by Implement

Operational Questions

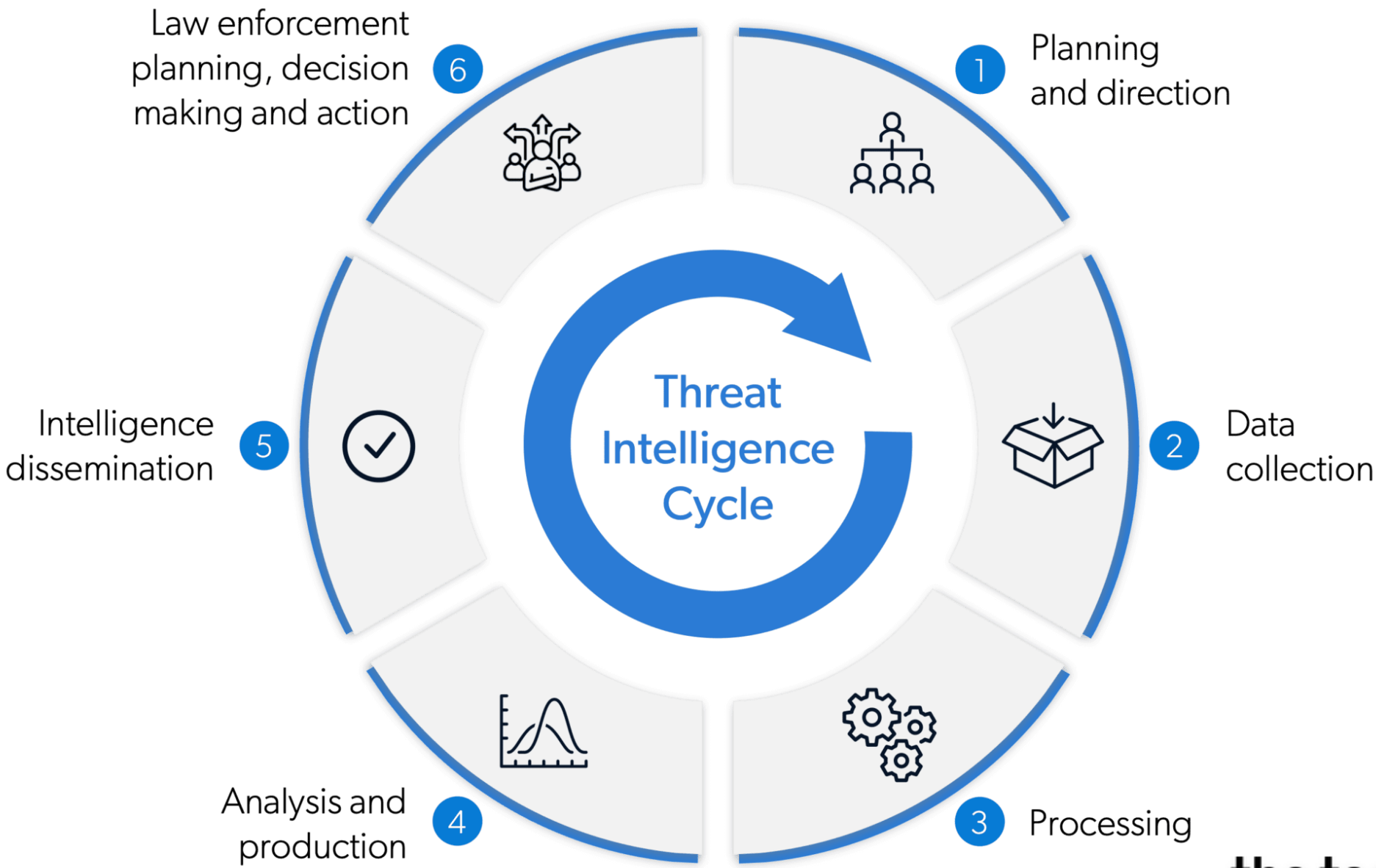
"Are we effectively detecting the initial access vector used in the XYZ campaign?"

"Are there signs that stolen credentials from recent breaches are being used against us?"

"Is the malware used in the current incident linked to known threat actors or broader campaigns?"

.the tech collective
powered by Implement

CTI Lifecycle



.the tech collective
powered by Implement

I have talked A LOT… Time for some fun!

Maybe just a little more talking...

I promise fun is coming...

Break

Second Brain

A **Second Brain** is a trusted, external system for capturing and organizing knowledge—so your real brain can focus on thinking, not remembering.

How It Works (Simplified):

1. **Capture** → Save useful info from anywhere
2. **Organize** → Tag and structure it meaningfully
3. **Connect** → Link related ideas over time
4. **Resurface** → Regularly revisit and reuse notes

.the tech collective
powered by Implement

Obsidian

What Is Obsidian?

Obsidian is a **local-first** note-taking app that turns plain text markdown files into a powerful **linked knowledge base**.

1. Create a Vault — your personal note collection
2. Write Notes — use markdown for formatting
3. Link Notes — use [[double brackets]] to create connections
4. Use Tags — like #CTI, #TTPs, #ThreatActors for organization
5. Explore — use the graph view to spot patterns and clusters

Collection Sources

Collection Sources

Technical Sources

- **Internal telemetry:** Logs from firewalls, EDR, IDS/IPS, proxies, mail gateways
- **Sensor networks / honeypots:** Deception systems that collect attacker behavior
- **Passive DNS / SSL cert data:** Infrastructure tracking and pattern correlation
- **Malware sandboxes:** Behavior analysis and IOC extraction

Open Source Intelligence (OSINT)

- **Threat reports & blogs:** CrowdStrike, Mandiant, etc.
- **Social media & forums:** Twitter/X, Reddit, hacking forums
- **Paste sites & code repos:** Pastebin, GitHub (TTPs, dropped payloads)
- **Dark web monitoring:** Underground market intelligence

Human Intelligence (HUMINT) & Trusted Sharing

- Information Sharing and Analysis Centers (ISACs)
- Government CERTs & LEAs
- Private intel sharing groups (e.g., CTI Slack, MISP communities)

Commercial Intelligence Providers

- **Feeds:** Structured IOCs, malware indicators
- **Contextual reports:** Actor profiles, campaign TTPs, sector targeting
- **Enrichment services:** WHOIS, geolocation, threat scoring

dclayton454/cyberbridge-summerschool

Download CTI Sources.zip

Unzip the file
Open Obsidian
Open the extracted file as a Vault

Exercise:

Visit each of the sources listed

Add links to the sources back to which type of CTI the sources represent

To tag, add the item you want to tag into [[insert here]]

Sharing Rules
davidclayton454@gmail.com

.the tech collective
powered by Implement

Sharing Rules

TLP: RED

Not For Disclosure

This information cannot be disseminated to third parties unless the sender permits it

Only participating groups can have access to it.

TLP: AMBER

Limited Disclosure

This information can be shared with participants of an organization or some members of a community

Additional restrictions can be made.

TLP: GREEN

Community-Wide Disclosure

This information can be shared with everyone in a particular community

However, it cannot be published publicly on the Internet.

TLP: WHITE

Unlimited Disclosure

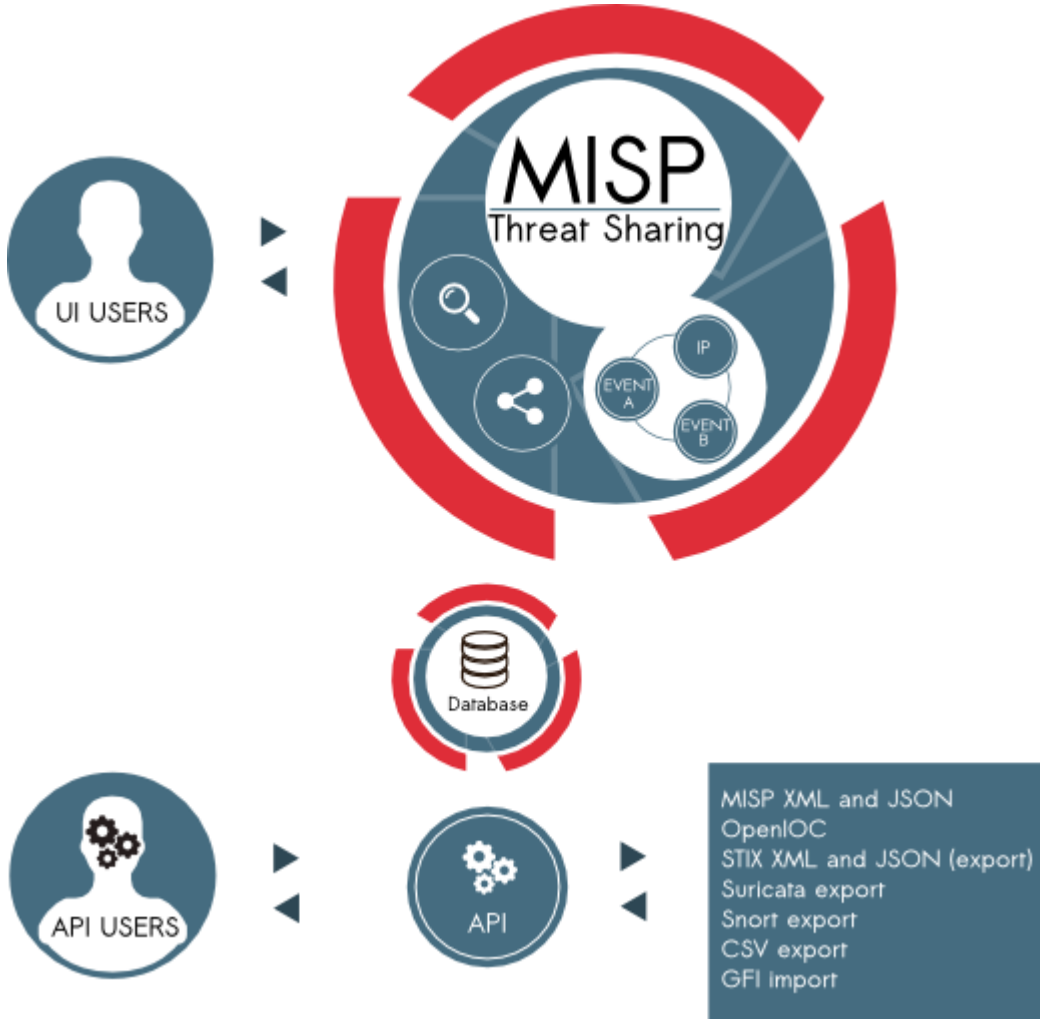
This information can be shared publicly with everyone

However, the laws of Copyright still need to be applied

.the tech collective
powered by Implement

Sharing OSINT

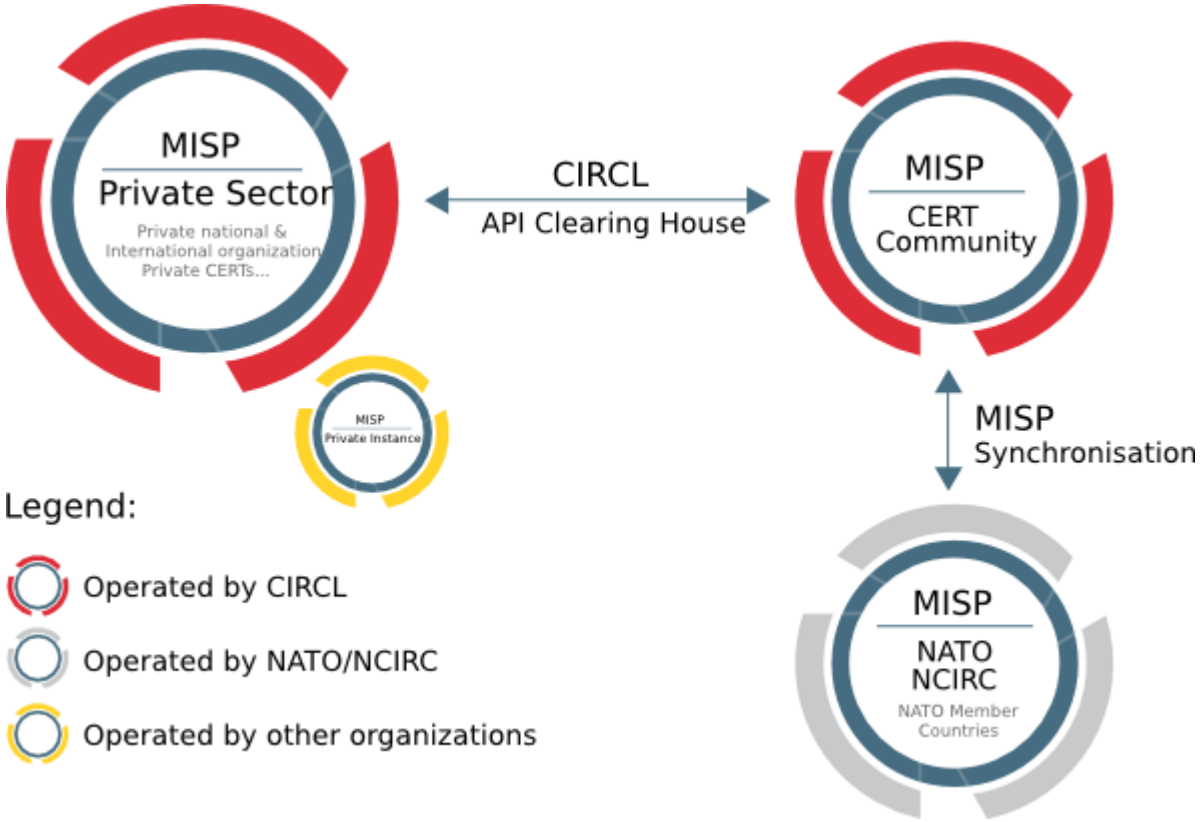
MISP



MISP (Malware Information Sharing Platform & Threat Sharing) is an **open-source threat intelligence platform** designed to help organizations **collect, store, share, and correlate** structured information about cybersecurity threats.

It enables security teams, CERTs, SOCs, and intelligence analysts to collaborate on **Indicators of Compromise (IOCs)**, TTPs, and threat actor profiles in a structured, machine-readable way.

.the tech collective
powered by Implement



.the tech collective
powered by Implement

Exercise

Navigate to:

https://iglocska.eu/users/login

User: summer@bootcamp.com

Password: ***

Search for:

7a5a694ac7d4068f580be624ece44f4f

Exercise Pt 2

Access event id 1800

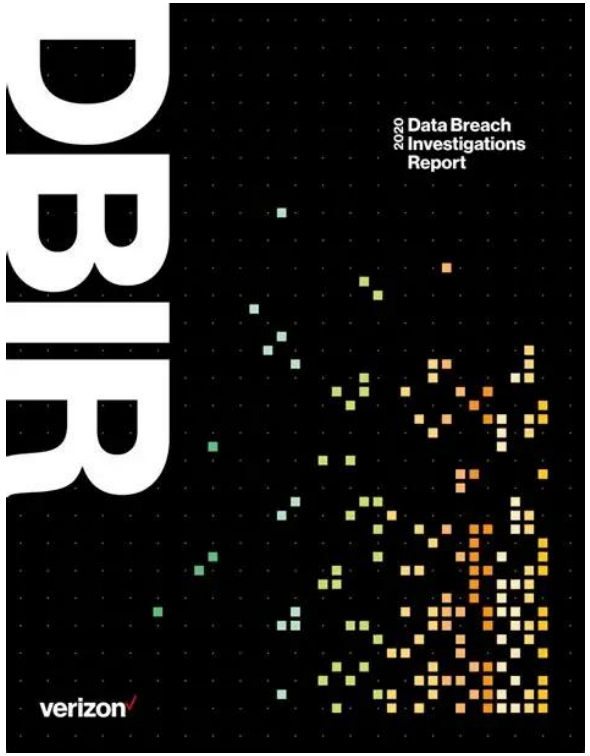
Click on threat actor

“LivingOffTheLOLz” galaxy

View both events that come up

Structuring Data

Incident Classification Languages



What Are Incident Classification Languages?

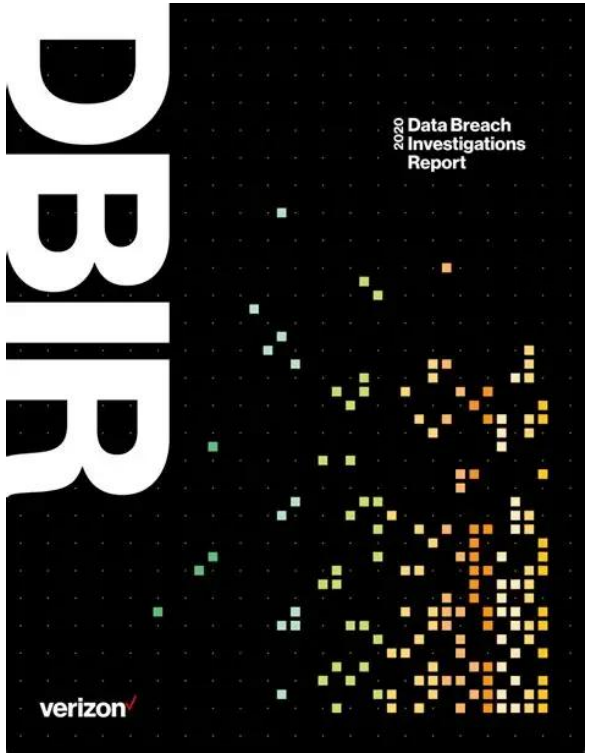
- Incident classification languages provide structured, standardized ways to describe and analyze cyber incidents, making it easier to share, compare, and learn from incidents across organizations.

Why They Matter:

- Enable consistent reporting across teams and industries
- Support data-driven analysis of trends and threats
- Improve communication between technical and non-technical stakeholders
- Feed into CTI, risk assessments, and compliance

.the tech collective
powered by Implement

VERIS



What Is VERIS?

- VERIS is a structured framework designed to record security incident details in a consistent format. Developed by Verizon, it's used in the Data Breach Investigations Report (DBIR).

VERIS Core Components (4 A's):

- Actors – Who caused the incident (external, internal, partner)
- Actions – What they did (hacking, malware, social, etc.)
- Assets – What was affected (servers, endpoints, data)
- Attributes – Impact types (confidentiality, integrity, availability)

The VERIS Framework

.the tech collective
powered by Implement

Incident/Intrusion Analysis

What Is MITRE ATT&CK?

MITRE ATT&CK is a globally accessible knowledge base of real-world adversary behavior, maintained by MITRE.

- Maps how attackers operate — not just what tools they use, but how they move, evade, and persist.
- Standardize how we describe and understand threat actor behavior
- Support threat intelligence, detection engineering, and red/blue teamingEnable shared language across SOC, IR, CTI, and security leadership

MITRE ATT&CK®

.the tech collective
powered by Implement

Back into Obsidian

dclayton454/cyberbridge-summerschool

Download cyberbridge.zip

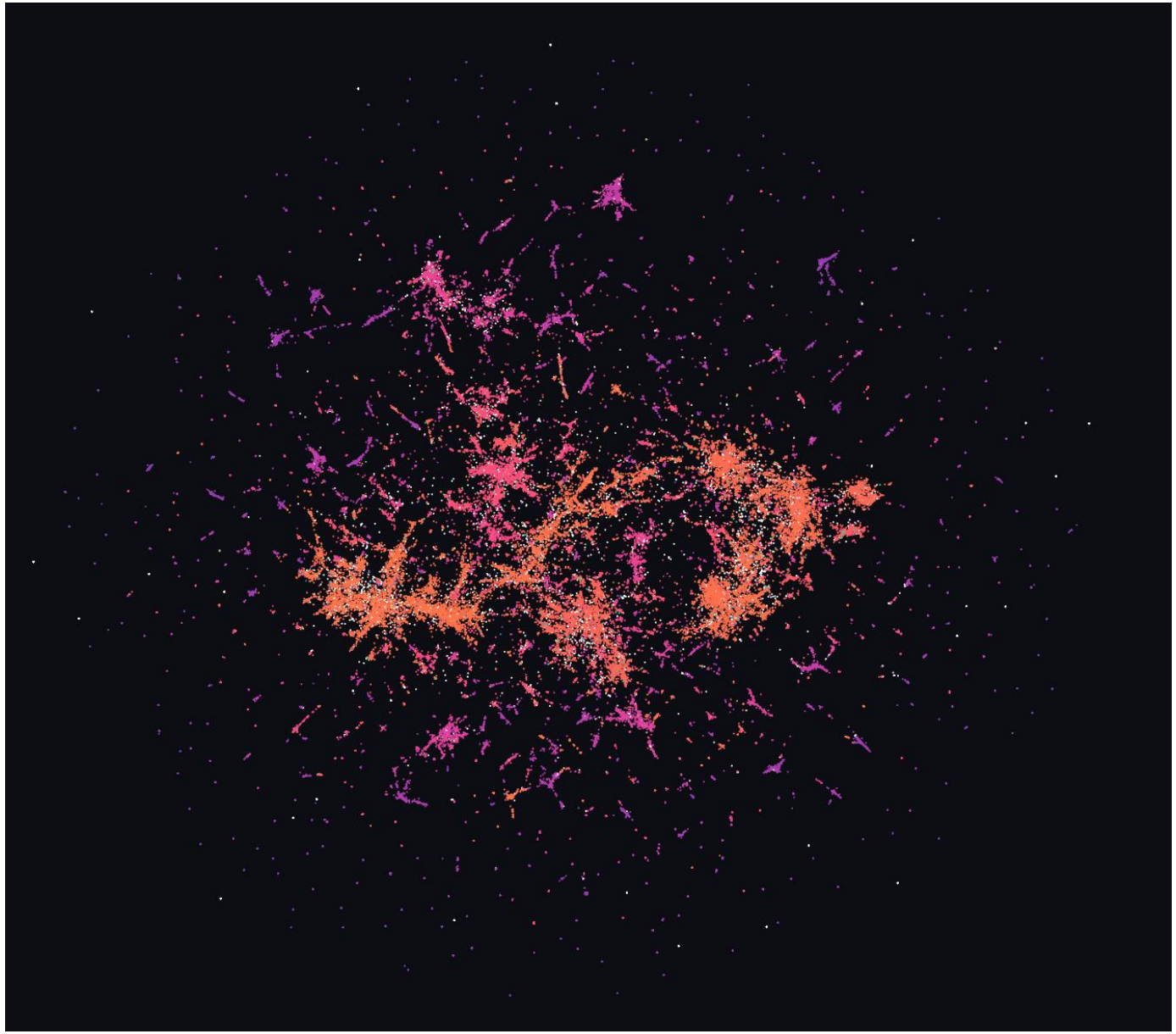
Extract the file
Open the folder as a vault in Obsidian

Exercise:
Add links to the articles back to which actors are involved

To tag, add the item you want to tag into [[insert here]]

Utilize VERIS and MITRE ATT&CK to analyze articles and add links to these frameworks

How do we do this on a large scale?



.the tech collective
powered by Implement

Navigate to: summerbootcamp.osinter.dk

Sign up with code: ****

.the tech collective
powered by Implement

CTF-Lite time!

Register a user: CyberBridge Summer Bootcamp

Use Obsidian to analyze the articles and threat actors to answer the questions. Utilize MITRE ATT&CK.

Some questions need you to use MISP too.

Bonus Exercise:

As a CISO working within the financial sector, which actors should I be aware of and fit into my threat landscape and why?

Write a simple report and send it to:

davidclayton454@gmail.com

Competition open until August 19th

.the tech collective
powered by Implement

.the tech collective
powered by Implement