OPENCTI TRAINING FOR FIMI ANALYSTS

Debunk.org
Disinformation analysis center

This project has received funding from the European Union's Horizon Europe Framework Programme under grant agreement Nº 101132494.

Saufex

Welcome!

Kindly allocate **90 minutes** of your time

Learn and apply correct FIMI and threat intelligence **terminology**

Understand how to use OpenCTI to **connect** and **analyze** data from **FIMI campaigns**

Explore OpenCTI through real FIMI **case studies** and **practical examples**

Test and consolidate your skills with interactive **exercises** and **quizzes**

CASE STUDY

Doppelgänger 101

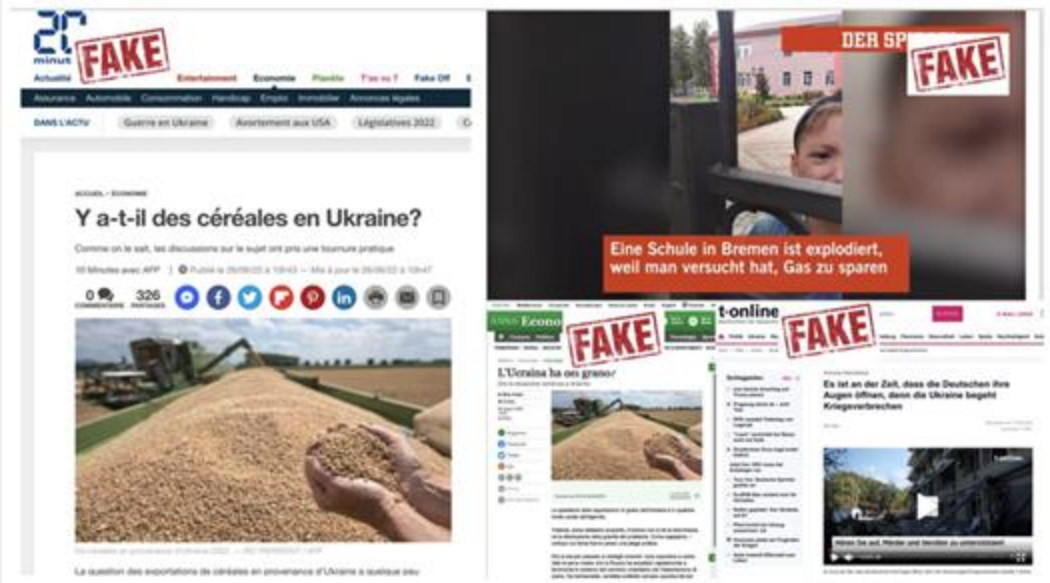
Origin & Operators: A Russian disinformation campaign first exposed in 2022, attributed to pro-Kremlin actors linked to information operations targeting Europe and North America.

Tactics: Used clone websites of major Western media outlets (e.g., The Guardian, Bild, Le Monde) with slightly altered domain names to publish fabricated articles.

Content Strategy: Articles spread anti-Ukrainian, anti-EU, anti-NATO narratives and attempted to undermine Western support for Ukraine.

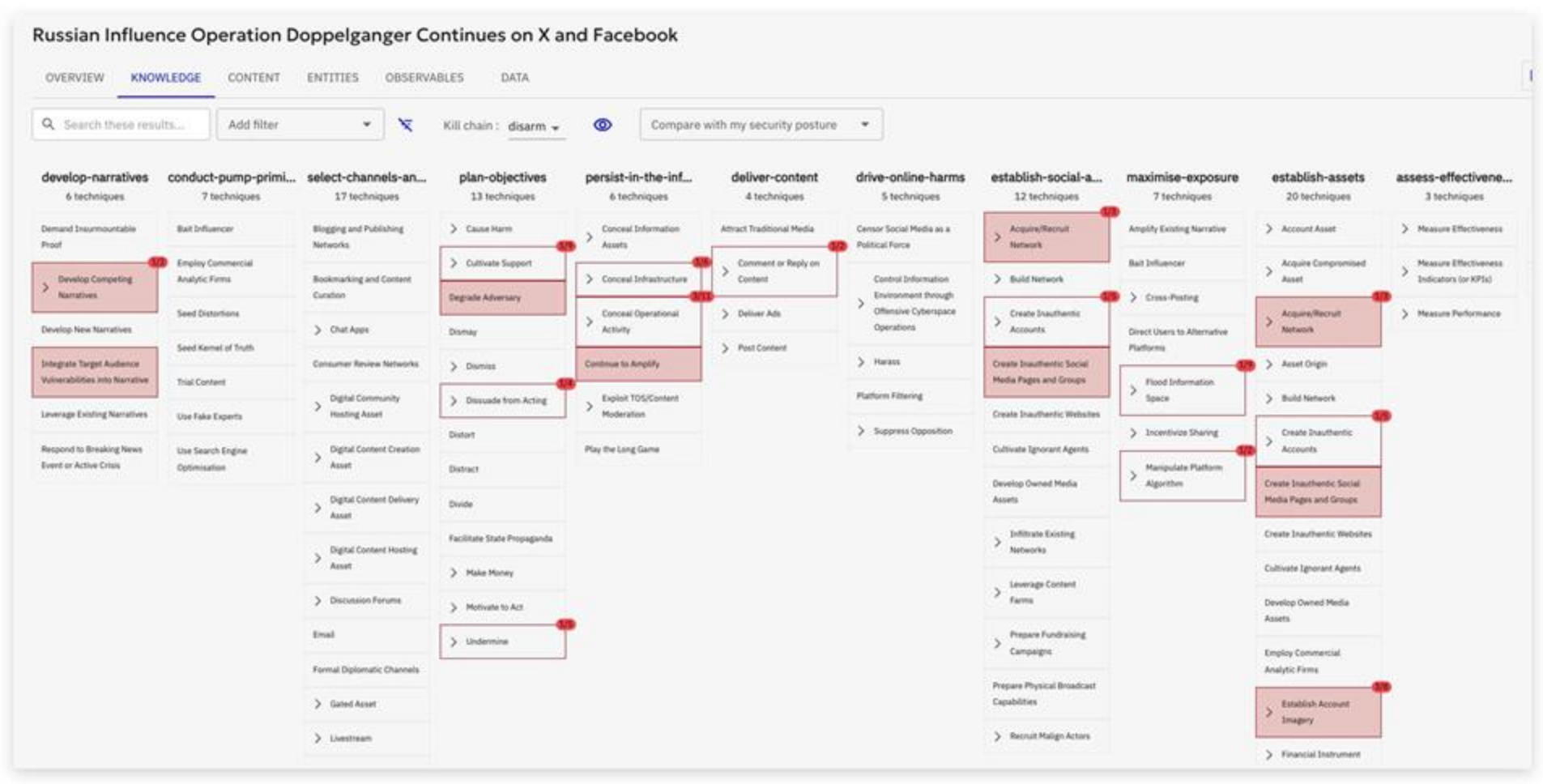
Amplification: Fake articles were pushed through social media accounts, bots, and spammed links to give the appearance of legitimacy and organic engagement.

Source: EU Disinfo Lab



Sample of fake stories on cloned media

Matrix view

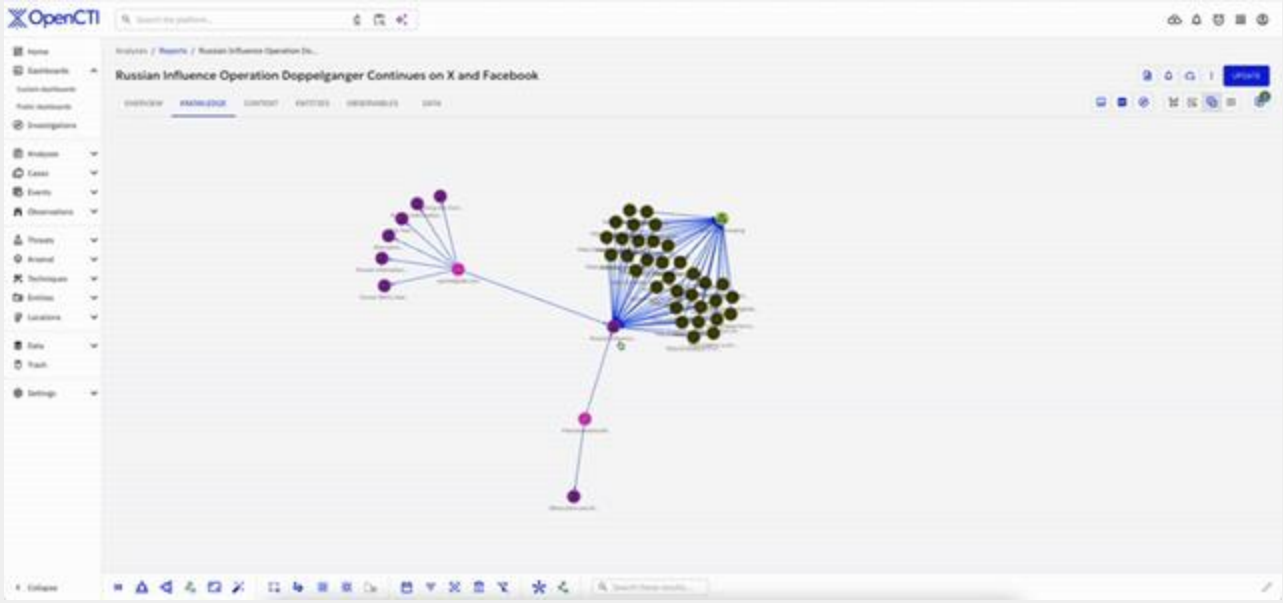


OpenCTI screenshot showing Matrix view of the Russian Influence Operation Doppelganger Continues on X and Facebook Report.

Source: Debunk.org

Correlation view

- **Visualizes cross-domain infrastructure** sharing between cloned media sites (e.g., sputnikglobe.com, tribunalukraine.info) and dozens of fake news portals.
- **Clusters show content replication** — same pro-Kremlin articles appear on multiple lookalike domains within hours.
- **Strong connection** between **sputnikglobe.com** and **tribunalukraine.info,** both serving as primary content sources for wider distribution.



OpenCTI GIF showing Correlation view of the Russian Influence Operation Doppelganger Continues on X and Facebook Report.

Source: Debunk.org

Entities

Campaign entities:
(*Entities are the core objects in OpenCTI that describe the actors, methods, content, and targets involved in an operation*)

- **Attack Patterns (TTPs):** T0002 Facilitate State Propaganda, T0023 Distort Facts, T0048 Amplify Wedge Issues.
- **Narratives:** “Ukraine is neo-Nazi”, “EU sanctions harm Europe”, “Western governments lie to their citizens”.

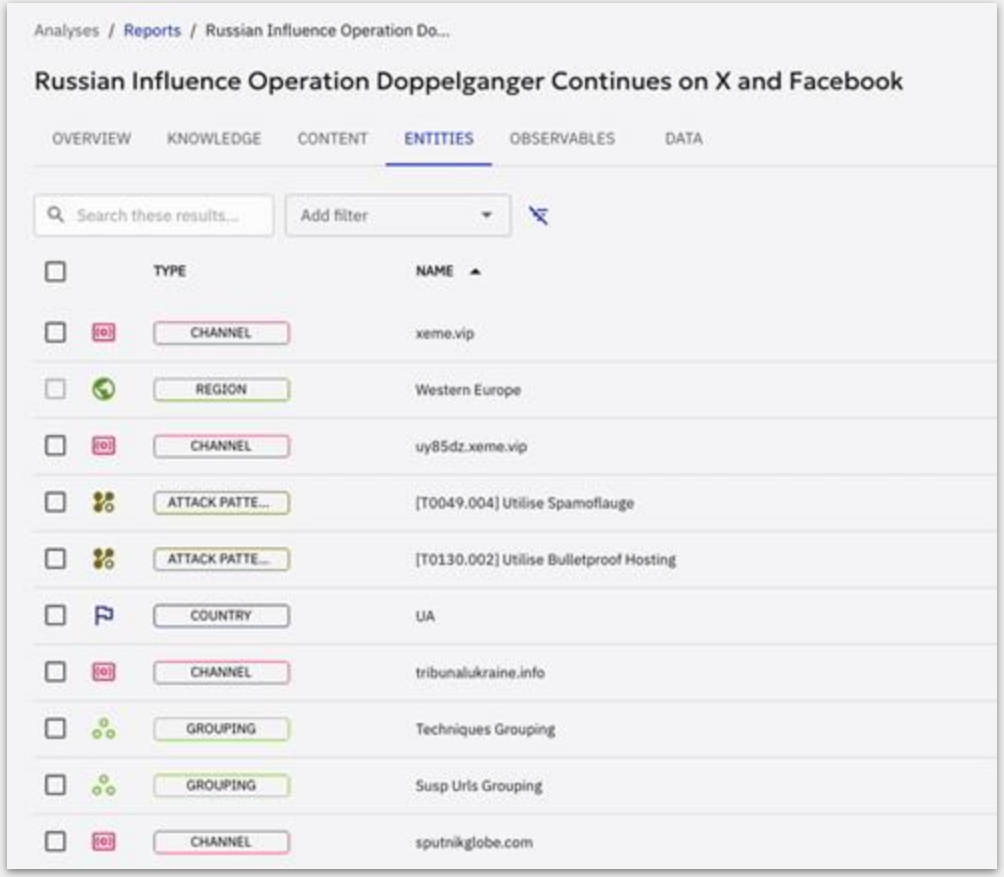
Regions targeted:

- Europe and North America

Key amplification channels:

- facebook.com/worldnewsintel
- x.com/europe_trends.

Source: Debunk.org



OpenCTI GIF entities from the Russian Influence Operation Doppelganger Continues on X and Facebook Report.

Observables (URLs)

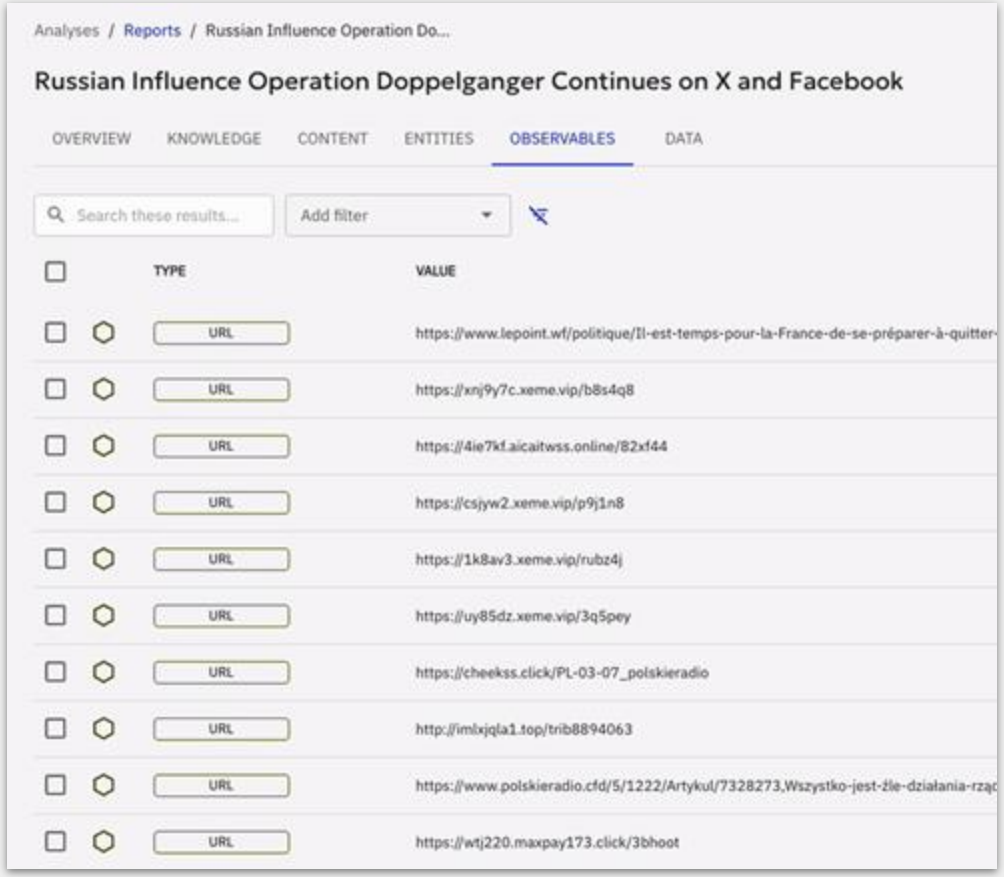
Observables are the **specific**, measurable pieces of **data** — such as **URLs**, **domains**, social media **posts** — that serve as **evidence** for these entities.

Example Doppelgänger domains from report:

- leparisien.ltd – mimics French news site, promotes “Ukraine refugee crisis” disinfo.
- theguardian.today – clones The Guardian, pushes “EU sanctions failing” narratives.
- bild.ltd – mimics German tabloid Bild, spreads “Ukraine is corrupt” claims.

Domains hosted on infrastructure linked to Russian operators, with content seeded on X and Facebook for reach.

Articles often **copy original layouts** but **replace text** with pro-Kremlin framing.



OpenCTI GIF observables from the Russian Influence Operation Doppelganger Continues on X and Facebook Report.

Source: Debunk.org

Case Study Takeaways

Persistent & Adaptive

Russian state-linked IO sustaining activity since 2022, **evolving tactics to evade detection and maintain reach.**

Infrastructure Redundancy

Multiple cloned domains (e.g., leparisien.ltd, theguardian.today, bild.ltd) ensure **rapid content replacement after takedowns.**

Narrative Consistency

Focused on anti-Ukraine, anti-EU, and sanctions-failure messaging across **multiple languages and regions.**

Cross-Platform Amplification

Coordinated seeding on Facebook & X drives **rapid narrative spread across audiences.**

Structured Intelligence Advantage

OpenCTI's network, correlation, and observable mapping reveal **campaign structure and key amplification nodes.**

1. OPENCTI: WHY IT MATTERS FOR FIMI?

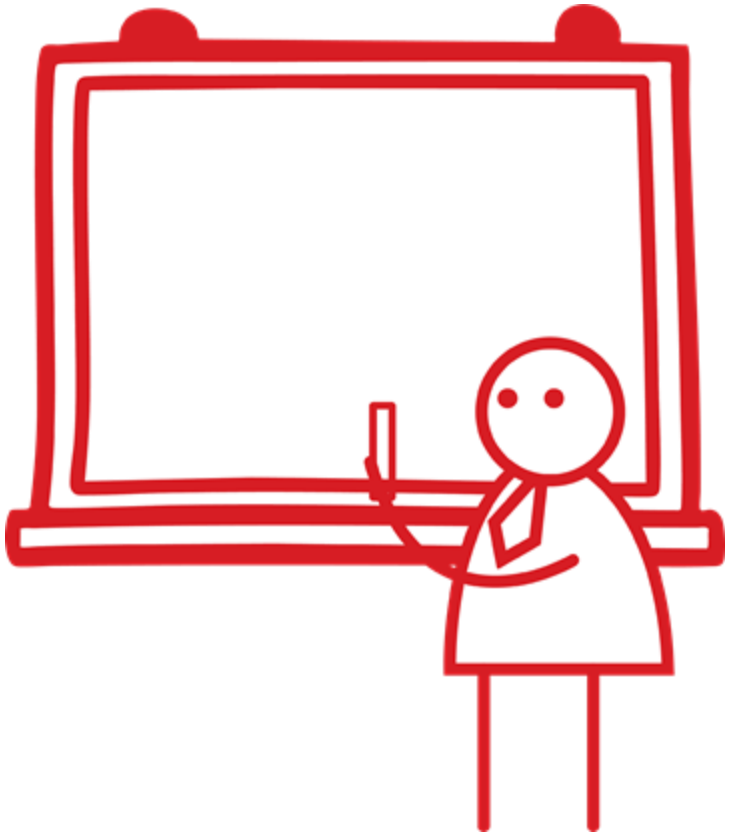
After Completing This Part You Will:

01 Understand **why structured threat intelligence is vital for FIMI**—and how **OpenCTI delivers it.**

02 Describe how **OpenCTI** gathers and standardises all your FIMI signals into **one shared workspace.**

03 **Sketch the automated FIMI lifecycle in OpenCTI**—from initial clue collection through analysis to ongoing monitoring.

04 **Summarise the core benefits OpenCTI brings,** from auto-linking disinformation threads to real-time team collaboration.

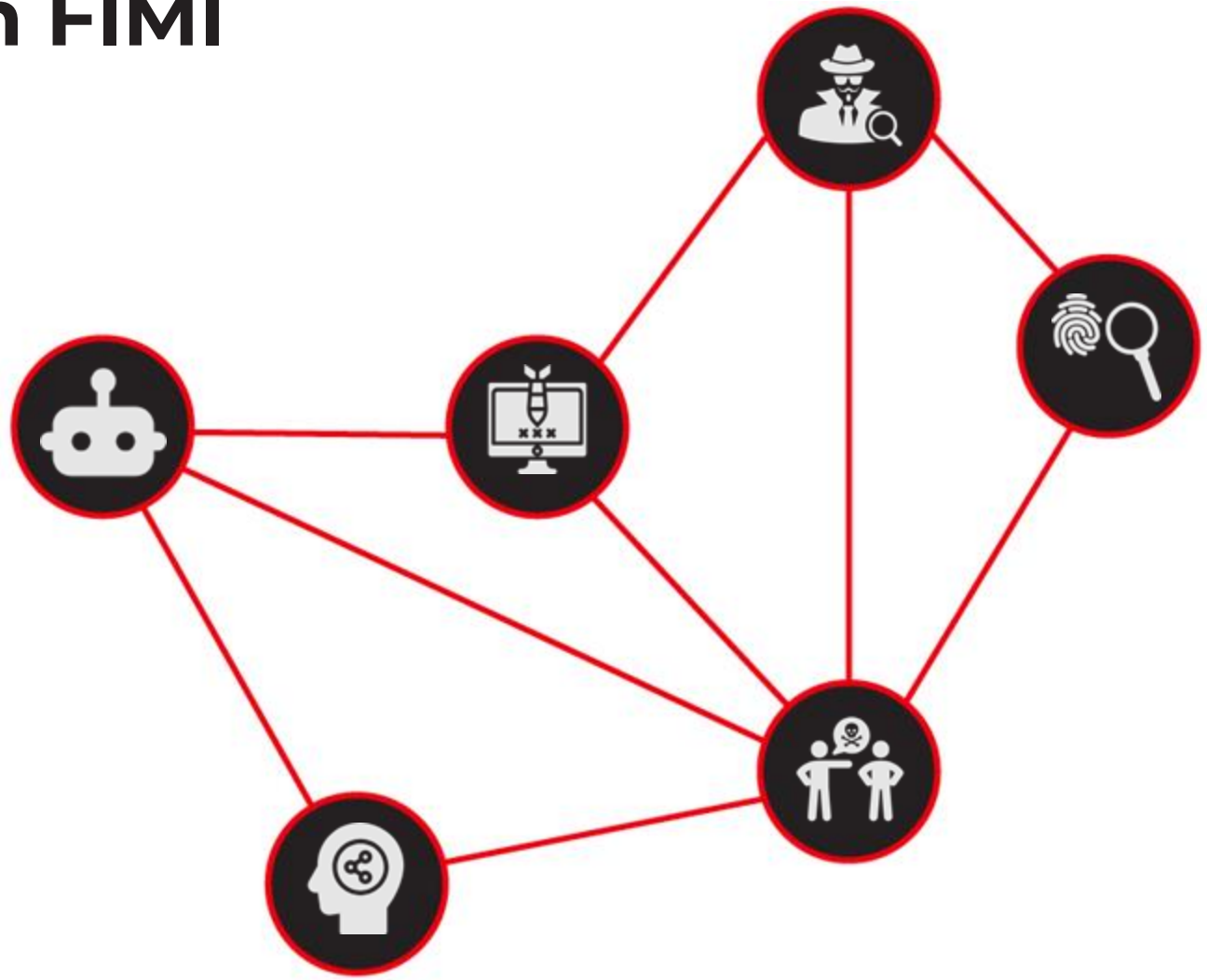


Threat Intelligence: Connecting the Dots in FIMI

In **Foreign Information Manipulation and Interference (FIMI),** threat intelligence means **connecting the dots:**

- Identify who is driving disinformation
- Understand how they operate
- Reveal what they aim to achieve

Goal: Stop them — faster and more effectively.



The FIMI Analyst's Pain Points

Data Overload & Scattered Sources

You're drowning in endless feeds, spreadsheets, Slack channels and inbox alerts, and no single place to see it all.

Manual Cross-Referencing & Inconsistent Terminology

Copy-pasting between mismatched lists takes hours—and when labels differ, a single mislabeled entry can hide a critical link.

Difficulty Maintaining Situational Awareness

As new clues pour in, it's nearly impossible to track the evolving shape of a disinformation operation in real time.

Broken Collect-Analyse-Coordinate Loop

Handoffs stall—what one analyst collects, another analyses, yet no one has the full, up-to-date view for a swift response.

Slow / Siloed Reporting

Findings get trapped in PDFs and inboxes—slowing any follow-up and locking partners out of data they could reuse.

Handcrafted Investigations, Meet Assembly-Line Intelligence

Industrial-scale analysis
OpenCTI moves us from gut-feel, one-off digging to scalable, automated analysis—capable of ingesting and normalising large batches of FIMI signals in minutes.

Built for teams
Full-scale FIMI investigations need collectors, analysts, and responders working in one shared graph—no one can do it all alone.

Source: Gemini

OpenCTI: from FIMI Chaos Into Clarity

Freely Available & Community-Driven

An open-source (cyber) threat-intelligence platform you can extend with a vibrant ecosystem of community-built connectors and plug-ins.

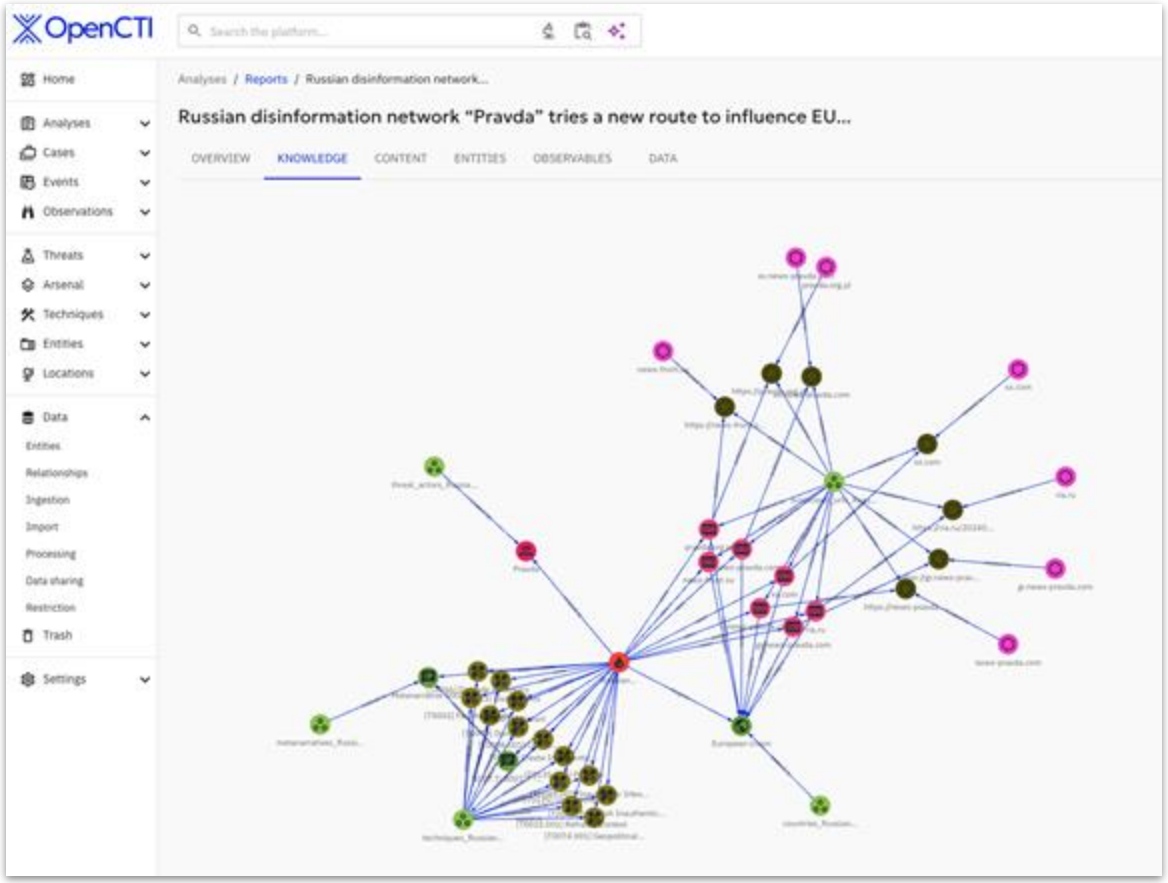
Where Disorder Becomes Intelligence

Designed by CTI experts to normalise and centralise dozens of disparate feeds—and now fine-tuned for FIMI signals like URLs, social posts, media clips, and tip reports.

Automated Ingestion & Unified Storage

Built-in connectors feed every new signal—whether a post, news alert, spreadsheet, or partner report—directly into your shared workspace as uniform, clickable entries.

Source: Debunk.org

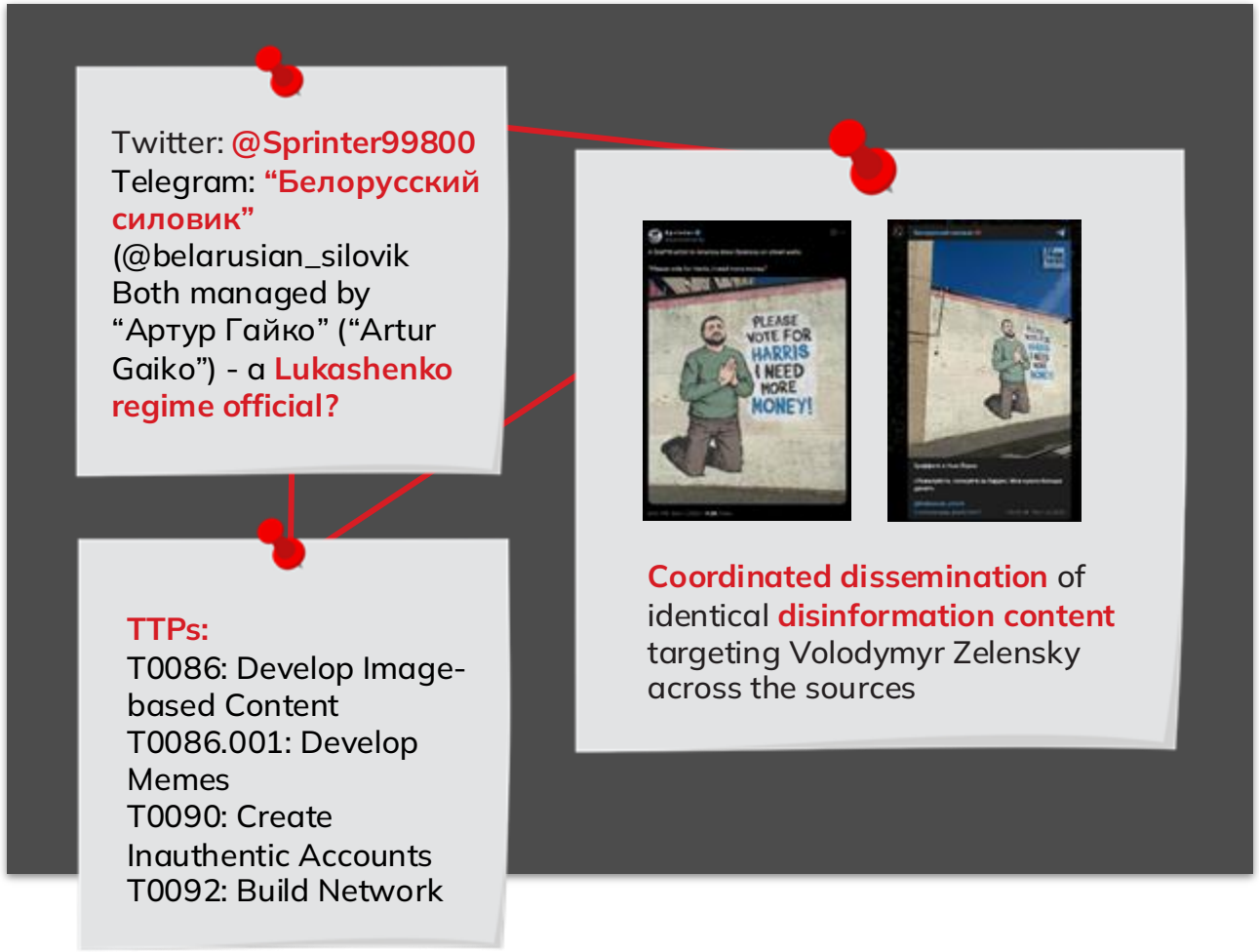


OpenCTI screenshot showing Knowledge Graph of the Russian disinformation network "Pravda" tries a new route to influence EU public opinions few days ahead of the vote Report.

OpenCTI: Your Digital Evidence Board For FIMI

Think of OpenCTI as a digital ‘evidence board’ in a detective’s war room.

OpenCTI is that same board reimagined as a searchable, auto-linking digital graph—letting you see **how every piece of disinformation or FIMI artifact connects to the bigger picture** with just a few clicks.



Source: Debunk.org

How OpenCTI Supports FIMI Investigations

Collect & Centralise Clues
Bring URLs, social-media posts, media clips, and tip reports into one shared workspace.

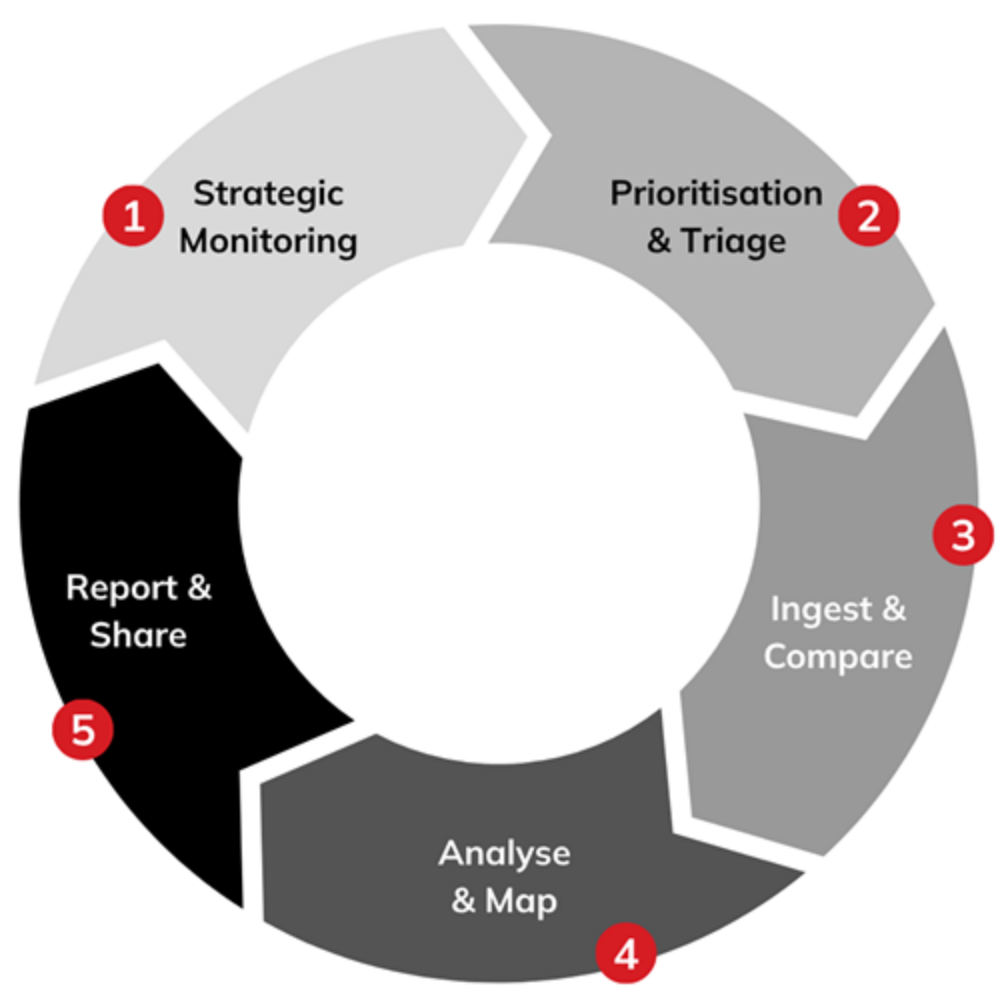
Normalise & Connect
Convert each piece of data into a standard format and track its connections to actors, content, and platforms.

Visualise the Big Picture
Map narrative chains and actor networks instantly in an interactive graph.

Collaborate & Act Fast
Share live dashboards, assign tags/notes, and coordinate responses in real time.

Source: Debunk.org

The FIMI Investigation Cycle



A FIMI investigation ***isn't linear***—**it's a loop.** We set monitoring priorities, triage potential incidents, and then hand the best leads into **OpenCTI for deeper *analysis, mapping and reporting.*** Those insights flow right back to sharpen the next monitoring round.

Strategic Monitoring: Set the Radar

Source: EEAS

Monitoring is done outside OpenCTI.

Current social-media and web monitoring tools don't connect directly to OpenCTI, so teams run their own stacks—dashboards, scrapers, LLM filters—and then import only the leads they consider worth keeping (sometimes just an analysis note; high-value cases may include URLs or full evidence bundles).

Prioritisation & Triage: Read the Radar Blips

Source: EEAS

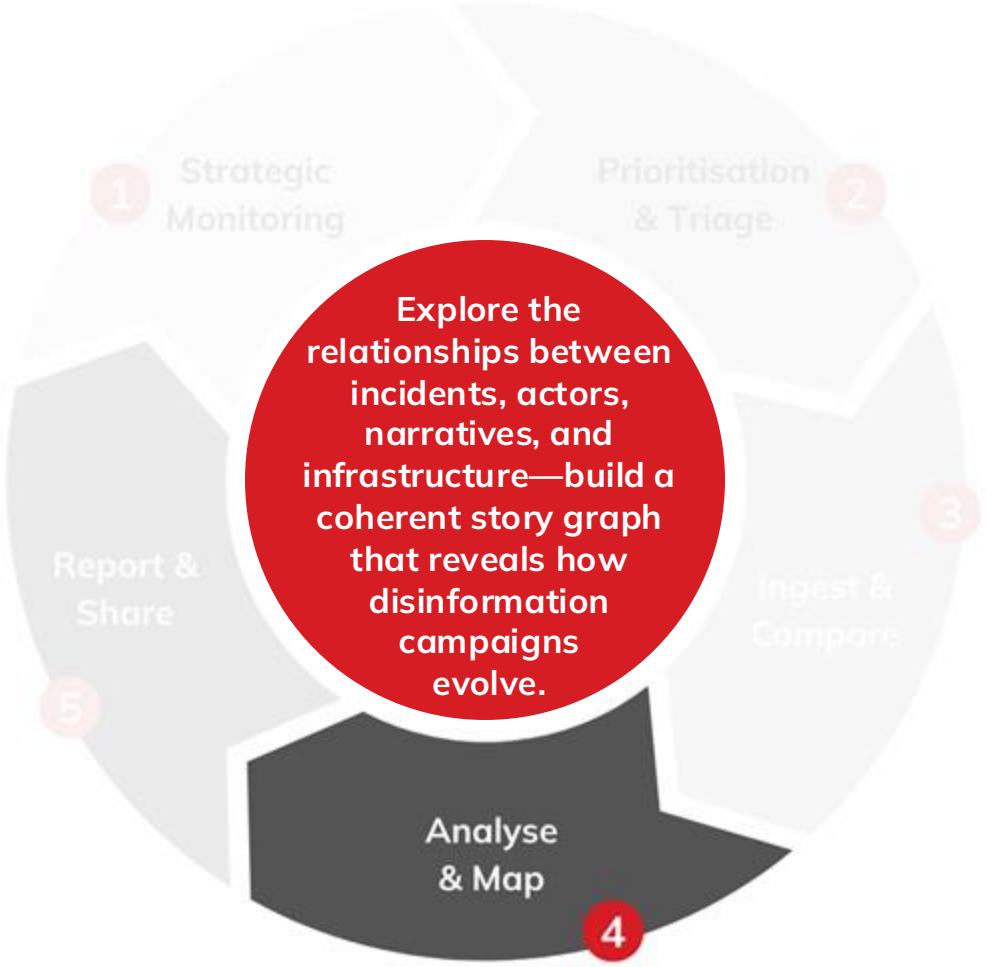
Triage happens upstream of OpenCTI.
Teams score and cluster leads in external dashboards, scrapers, or LLM sheets—then record *only priority items* in OpenCTI (sometimes just an analysis note + key indicators; high-value cases may add URLs or evidence bundles).

Ingest & Compare: Drop to Discover

Variable ingestion workflows.

Some teams import only the final analysis summary and selected indicators into OpenCTI, whilst others log just URLs, domains, or account handles. A few pilot projects attach Hunchly/CSV archives for deeper parsing. OpenCTI would then auto-normalise each imported item, enrich it with metadata and auto-link to matching cases.

Analyse & Map: Connecting the Dots



Interactive, collaborative graph work.

Teams use OpenCTI's graph and timeline views to pivot from domains to campaigns, tag narrative themes, and assign confidence levels. Some add notes or comments node-by-node; others trial LLM-assisted tagging of TTPs. Because the graph updates in real time, teams stay aligned—but very large networks can get messy unless you apply custom filters or predefined views.

Report & Share: Seal the Cycle

Export & loop-back workflows.

OpenCTI lets you export dashboard configurations (JSON), entity data as STIX bundles or CSV/JSON/PDF files for partners. Most teams still write narrative reports offline, then codify the key findings (observables, TTPs, confidence) in CTI afterward. Feeding fresh watch-lists back into monitoring remains a manual step.

Key takeaways

OpenCTI is an open-source platform that **structures, connects, and visualises disinformation data like a digital evidence board.**

It solves core FIMI analyst challenges: fragmented data, manual cross-referencing, inconsistent terminology, and poor situational awareness.

Empowers analysts to shift from reactive work to **strategic, pattern-based investigation.**

Exercise 1.1

Type of the exercise:

Single choice

Please select your type of the exercise from these options:

- True - false
- Single choice
- Multiple choice
- Sort the cards into categories
- Drag-drop
- Scenario
- Match the sentence
- Pick one or many
- Fill in the missing word
- Rank the options

Exercise 1.1

Question 1:

What does OpenCTI primarily help analysts do?

Please highlight the correct answer:

A. Encrypt data
B. Monitor server health
C. Structure, analyse, and visualise intelligence data✓

Exercise 1.1

Please explain why this is the correct answer:

Correct Answer: C – Structure, analyse, and visualise intelligence data

Why it's correct:
OpenCTI is designed to help analysts organize threat intelligence using structured formats (like STIX), analyze relationships between threat elements (e.g., actors, observables, campaigns), and visualize these links through graphs, timelines, and dashboards. It's a powerful tool for turning scattered data into meaningful intelligence.

Please explain why other options are incorrect:

A – Encrypt data

Why it's incorrect:
OpenCTI is not an encryption tool. It stores and processes structured intelligence but does not encrypt communications or secure data transmission — that's the job of cryptographic tools.

B – Monitor server health

Why it's incorrect:
Server health monitoring is related to IT operations tools like Nagios, Zabbix, or Prometheus. OpenCTI is a threat intelligence platform, not a system monitoring solution.

Exercise 1.2

Type of the exercise:

Single choice

Please select your type of the exercise from these options:

- True - false
- Single choice
- Multiple choice
- Sort the cards into categories
- Drag-drop
- Scenario
- Match the sentence
- Pick one or many
- Fill in the missing word
- Rank the options

Exercise 1.2

Question 1:

The “digital evidence board” metaphor emphasises that OpenCTI…

Please highlight the correct answer:

A. Prints physical reports for wall displays
B. Auto-links imported clues into a graph you can explore✓
C. Hides relationships until manually added
D. Works only for cyber-malware cases

Exercise 1.2

Please explain why this is the correct answer:

The detective-board metaphor conjures an image of a corkboard covered with photos, clippings, and red string that physically links related clues. In OpenCTI, that string is replaced by the **platform's graph engine,** which automatically connects every imported **URL, account, hashtag, or domain into a network of relationships the moment data is ingested.** That instant, behind-the-scenes linking—and the ability to click through the resulting graph to follow a trail—**is exactly what Option B describes.**

Please explain why other options are incorrect:

The other choices mention **printing, hiding relationships, or limiting use-cases,** none of which capture this core "auto-linking evidence board" functionality.

Exercise 1.3

Type of the exercise:

Fill in the missing word

Please select your type of the exercise from these options:

- True - false
- Single choice
- Multiple choice
- Sort the cards into categories
- Drag-drop
- Scenario
- Match the sentence
- Pick one or many
- Fill in the missing word
- Rank the options

Exercise 1.3

Question 1:

OpenCTI excels as a living _____ base—analysts use its graph to spot links and trends.

Please highlight the correct answer:

A. Threat

B. Knowledge✓

Exercise 1.3

Please explain why this is the correct answer:

OpenCTI acts as a centralized knowledge repository—every incident, actor, and indicator lives in one searchable graph. By surfacing links and patterns automatically, **it helps analysts spot emerging trends and relationships that might otherwise be buried across disconnected notes or spreadsheets.** This shared context means teams can draft more accurate, comprehensive reports—**grounded in the full history of what's happened**—rather than reinventing the wheel with each new investigation.

Please explain why other options are incorrect:

Exercise 1.4

Type of the exercise:

Single choice

Please select your type of the exercise from these options:

- True - false
- Single choice
- Multiple choice
- Sort the cards into categories
- Drag-drop
- Scenario
- Match the sentence
- Pick one or many
- Fill in the missing word
- Rank the options

Exercise 1.4

Question 1:

In the FIMI analysis Cycle phase Analyse & Map, analysts primarily use the graph view to:

Please highlight the correct answer:

A. Define keywords for monitoring
B. Compare alerts to previous cases
C. Trace connections between domains, actors, and campaigns ✓
D. Export data bundles

Exercise 1.4

Please explain why this is the correct answer:

In Phase 4: Analyse & Map, **the core activity is spinning up the live graph to trace connections**—**clicking from one domain or observable to linked actor profiles, campaigns, or infrastructure** and following narrative threads through the network. Analysts lean on that graph view and its timeline pane to explore how disinformation elements relate and evolve.

Please explain why other options are incorrect:

A. Define keywords for monitoring

That's a Phase 1 task—s**etting your watchlist**—rather than mapping connections.

B. Compare alerts to previous cases

Matching happens in Phase 3 (Ingest & Compare), not in the detailed graph exploration step.

D. Export data bundles

Exporting STIX/CSV/PDF is a Phase 5 activity (Report & Share), not part of the Analyse & Map phase.

Exercise 1.5

Type of the exercise:

Drag-drop

Please select your type of the exercise from these options:

- True - false
- Single choice
- Multiple choice
- Sort the cards into categories
- Drag-drop
- Scenario
- Match the sentence
- Pick one or many
- Fill in the missing word
- Rank the options

Exercise 1.5

Question 1:

Put these FIMI analysis cycle phases in the correct order (1 = first, 5 = last):

- Analyse & Map
- Strategic Monitoring
- Report & Share
- Prioritisation & Triage
- Ingest & Compare

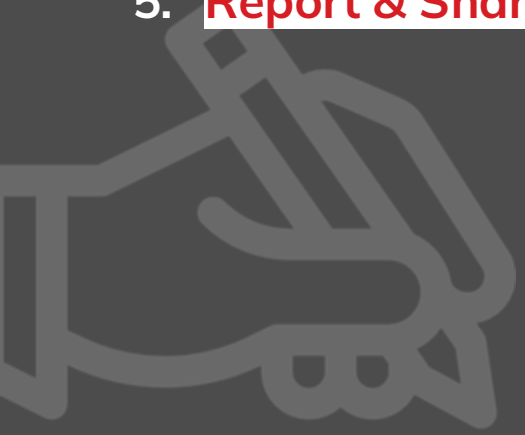
Please highlight the correct answer:

1. Strategic Monitoring
2. Prioritisation & Triage
3. Ingest & Compare
4. Analyse & Map
5. Report & Share

Exercise 1.5

Please explain why this is the correct answer:

1. **Strategic Monitoring:** define your watchlist and configure external collection.
2. **Prioritisation & Triage:** filter, de-duplicate, and rank alerts to pick top leads.
3. **Ingest & Compare:** import leads into OpenCTI, enrich them, and link to past intel.
4. **Analyse & Map:** explore the graph to trace and tag key connections.
5. **Report & Share:** export insights and update your monitoring setup.



2. MODELING FIMI IN STIX 2.1 & DISARM FRAMEWORK

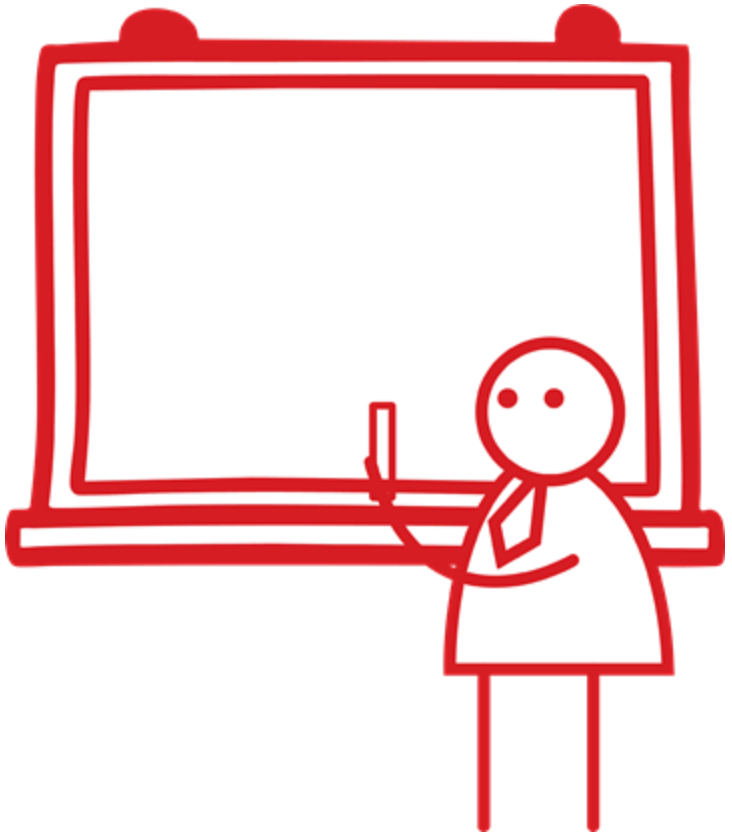
After Completing This Part You Will:

01 Understand what **STIX** is and **how it models disinformation threats.**

02 Recognize **how OpenCTI leverages STIX** to visually organize and analyze disinformation campaigns.

03 Explore how the **DISARM framework** enhances threat behavior classification within **STIX and OpenCTI.**

04 Practice **mapping disinformation elements to STIX objects** using a real or fictional example.



What is STIX 2.1?

STIX™ is a standardized format for **encoding and sharing threat intelligence.** Originally developed for cyber threat intelligence, but adaptable for FIMI incidents.

Breaks complex incidents into structured elements (e.g., actors, campaigns, observables).

Designed to be both **machine-readable** and **human-readable**.

Compatible with various programming languages for **integration** and **automation.**

Source: Gemini

STIX 2.1 Objects used for FIMI

ATTACK PATTERN

Provides a structured way to understand **how** threat actors **spread disinformation**.

COURSE OF ACTION

A **recommendation** to a consumer on the actions that they might take in response to the intelligence.

DOMAIN NAME

Name of the **domain used** in FIMI **campaign**.

INCIDENT

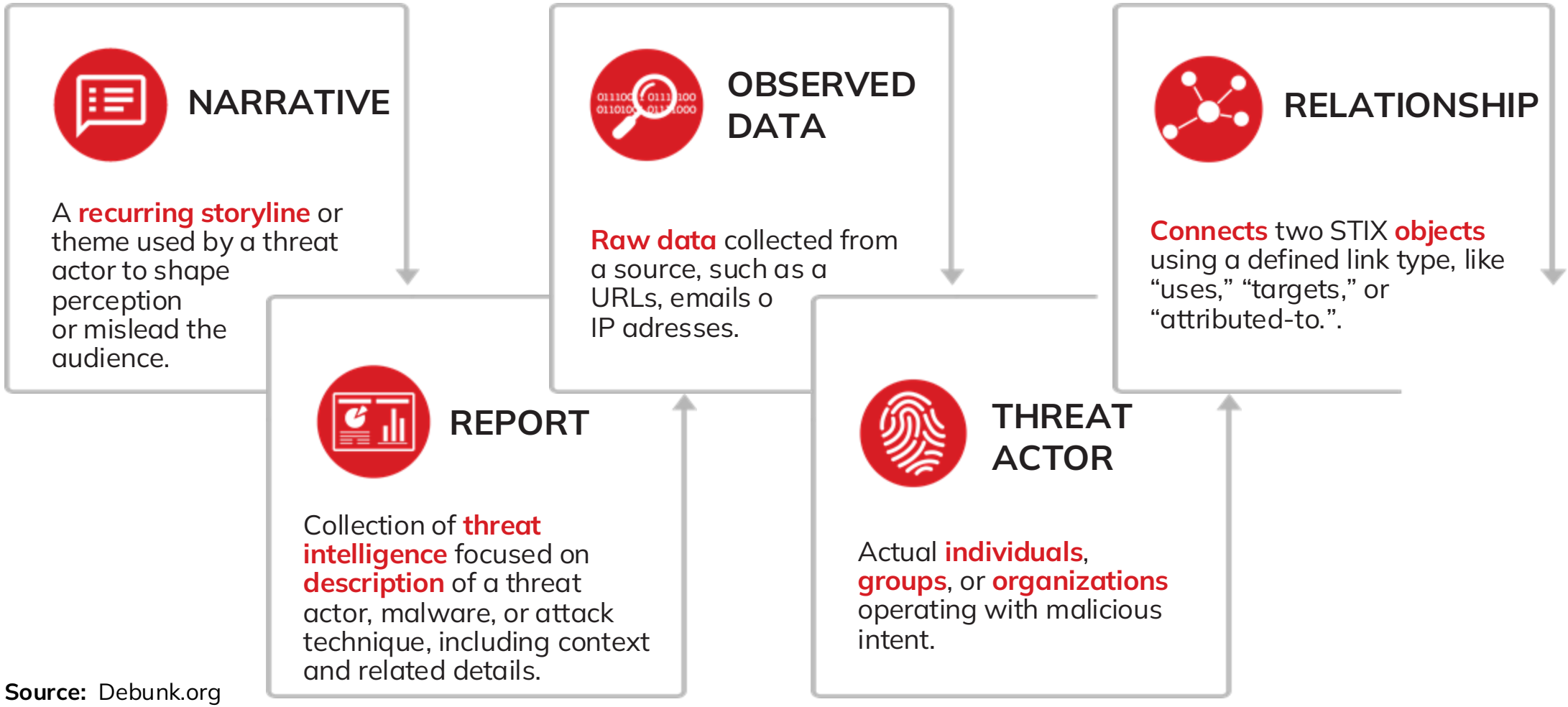
A specific instance of an **event** or a set of related events **negatively affecting** a **target**.

INDICATOR

A technical **sign** (e.g., keyword, hashtag, or domain) **used** to **detect malicious** or **deceptive activity.**

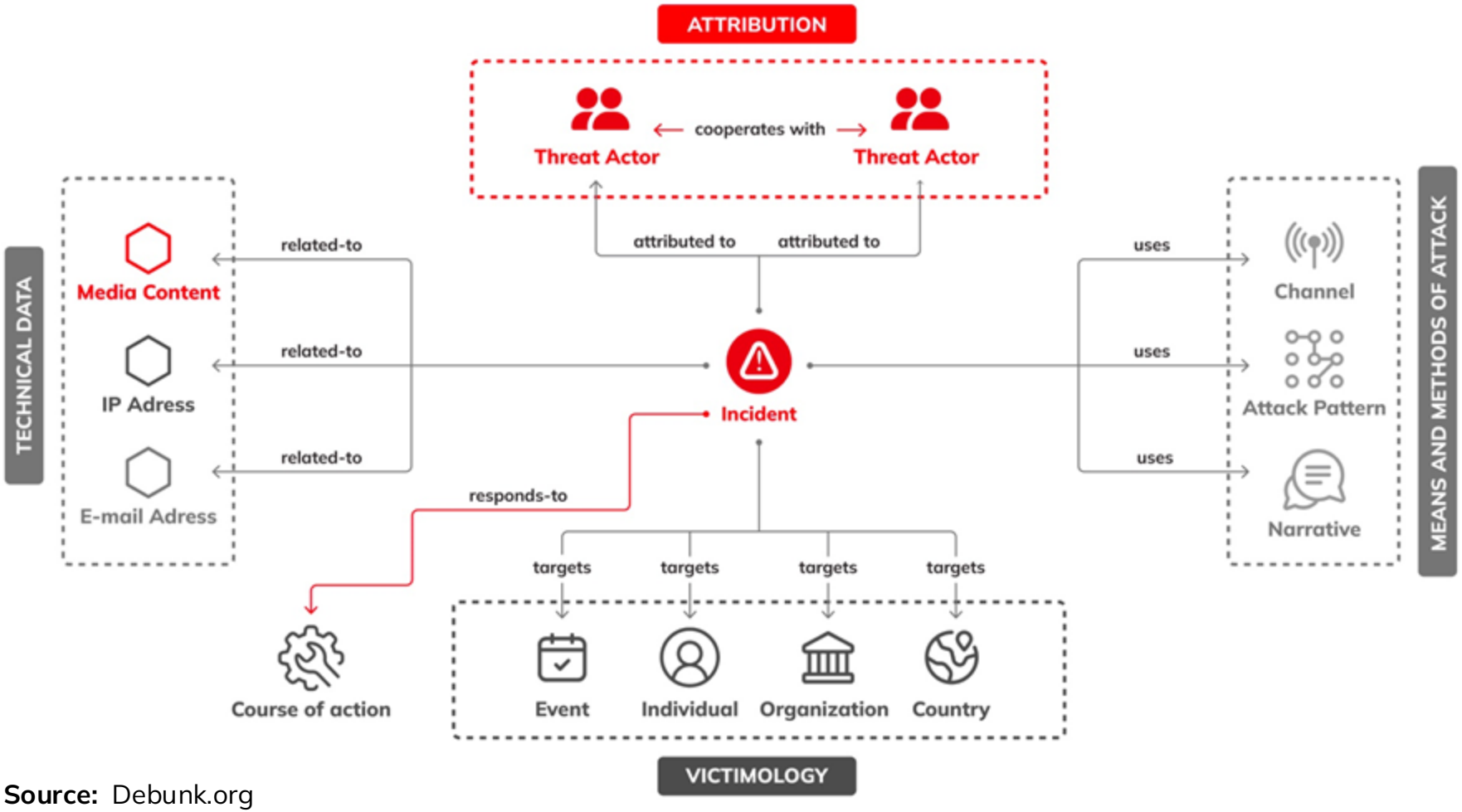
Source: Debunk.org

STIX 2.1 Objects used for FIMI



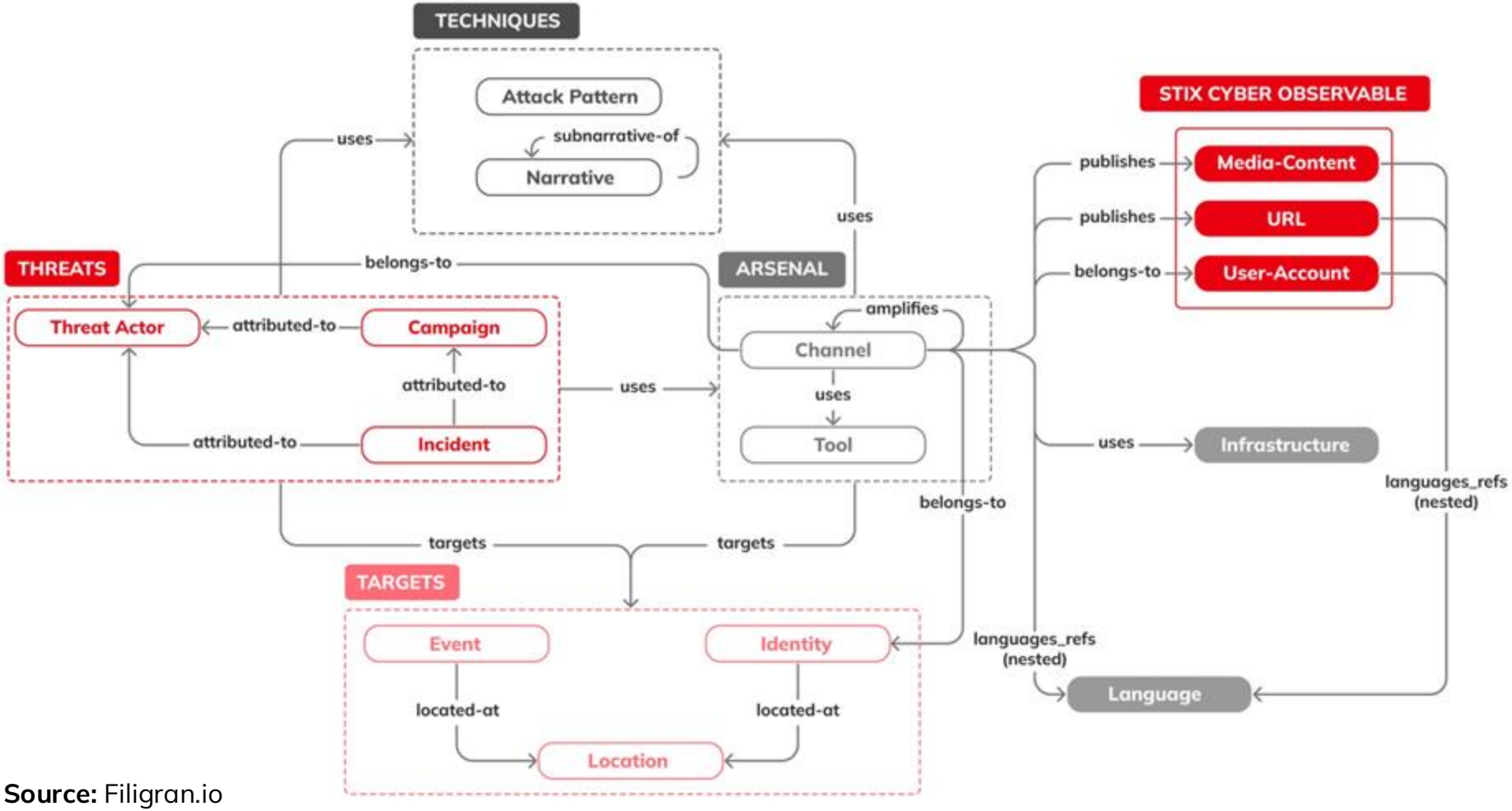
Source: Debunk.org

Observables, Entities, Relationships



Source: Debunk.org

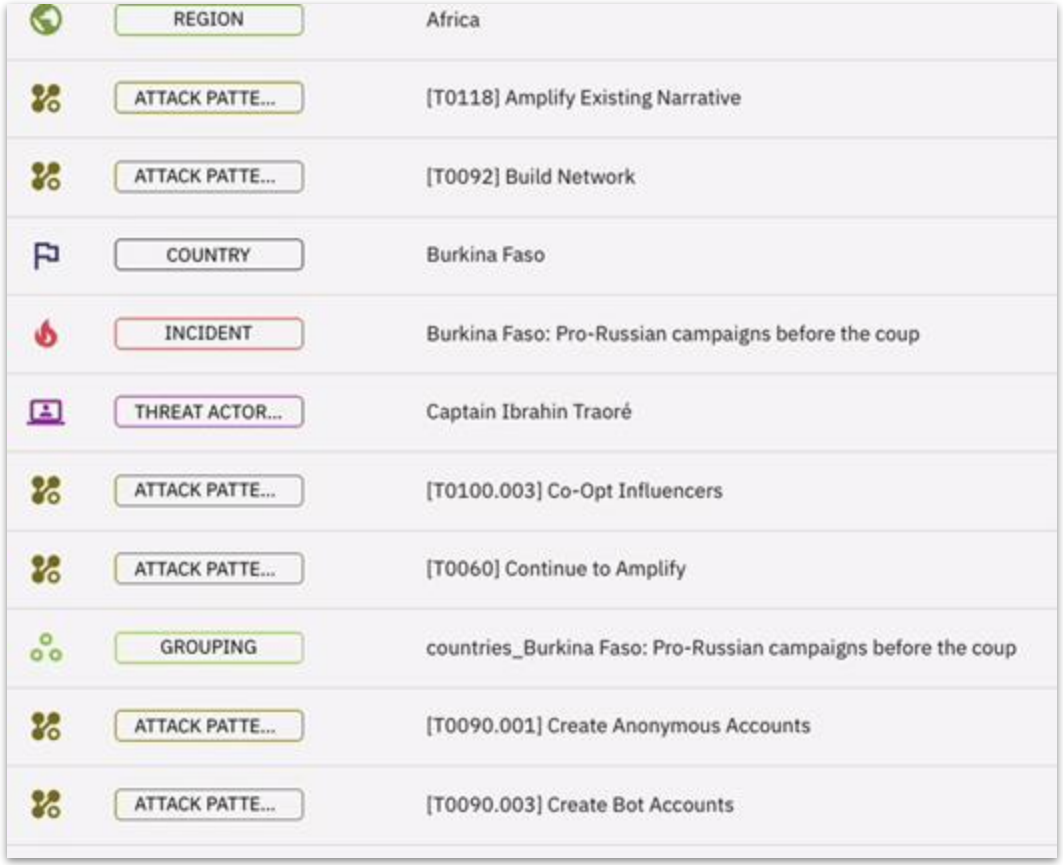
Observables, Entities, Relationships



Source: Filigran.io

Modeling Disinformation as a Structured Threat

- Disinformation can be treated like a threat, just like in cybersecurity — it has **patterns, actors, and tools that can be mapped.**
- **STIX 2.1** allows encoding of key elements: **actors, campaigns, narratives, observables**, and **targeted entities**.
- Enables **standardized**, machine-readable representation of influence operations.
- Facilitates **data sharing**, trend analysis, and cross-platform correlation.



OpenCTI screenshot showing disinformation-related entities encoded in STIX 2.1 format — including attack patterns (tactics), narratives, and dissemination channels.

Source: Debunk.org

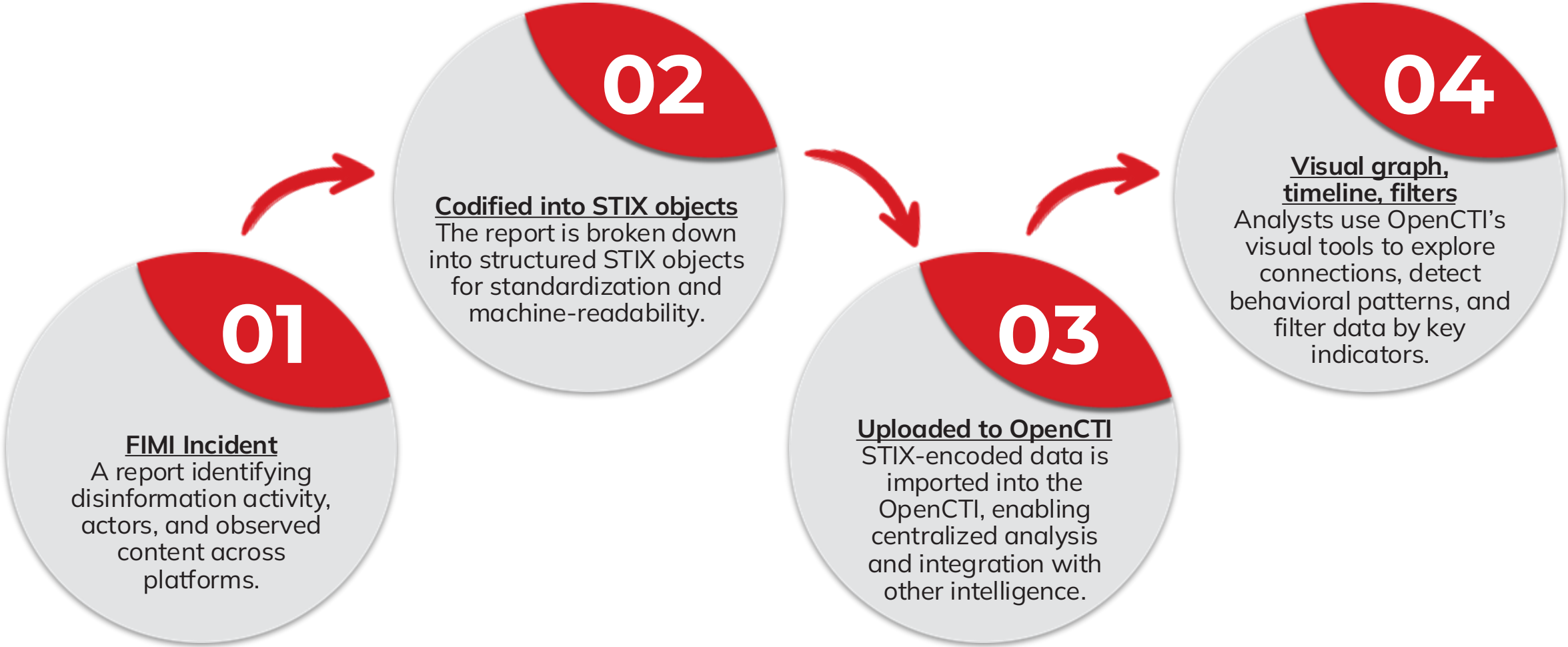
Modeling Disinformation as a Structured Threat

Click the following link or scan the **QR code:**

https://www.dropbox.com/scl/fi/ts9iwknx3xgrfepqpmdtj/modeling-diisnfo-as-str-threrat.mp4?rlkey=0qc6ab1tzc5e4xsj4xby8cv01&st=yjwozmx2&dl=0

Source: Debunk.org

STIX + OpenCTI = Disinfo Intelligence Workflow



Source: Debunk.org

What is DISARM Framework?

DISARM (Disinformation Analysis and Risk Management) is an open-source framework to describe disinfo TTPs.

TTPs = **Tactics, Techniques, and Procedures:** Specific methods threat actors use to plan, deliver, and amplify influence operations.

It **standardizes** how behaviors are described and categorized across campaigns.

The newest version of the **Framework** is available on the official DISARM Foundation Website.

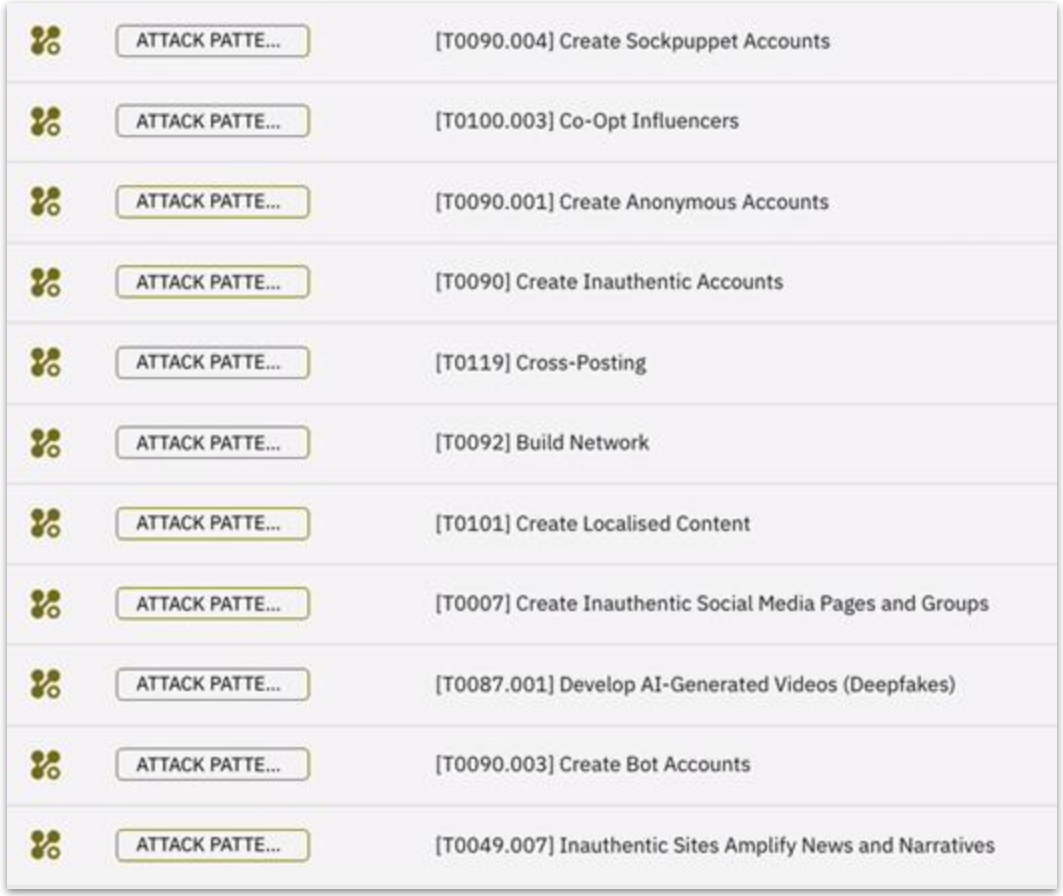
TA14: Develop Narratives	TA06: Develop Content	TA15: Establish Social Assets	TA16: Establish Legitimacy	TA05: Microtarget
T0003: Leverage Existing Narratives	T0015: Create hashtags and search artifacts	T0007: Create Inauthentic Social Media Pages and Groups	T0009: Create fake experts	T0016: Create Clickbait
T0004: Develop Competing Narratives	T0019: Generate information pollution	T0010: Cultivate ignorant agents	T0009.001: Utilize Academic/Pseudoscientific Justifications	T0018: Purchase Targeted Advertisements
T0022: Leverage Conspiracy Theory Narratives	T0019.001: Create fake research	T0013: Create inauthentic websites	T0011: Compromise legitimate accounts	T0101: Create Localized Content
T0022.001: Amplify Existing Conspiracy Theory Narratives	T0019.002: Hijack Hashtags	T0014: Prepare fundraising campaigns	T0097: Create personas	T0102: Leverage Echo Chambers/Filter Bubbles

Some of the TTPs from the DISARM Red Framework

Source: Debunk.org

Why Use DISARM in STIX + OpenCTI?

- **DISARM techniques** can be encoded in **STIX** as **Attack Patterns.**
- Allows **mapping of behavioral patterns** across disinformation campaigns.
- Supports **detection** of repeat methods, coordination indicators, and actor profiles.
- Empowers analysts to classify threats based on **actual behavior,** not just content.



OpenCTI UI showing DISARM TTPs encoded as Attack Patterns

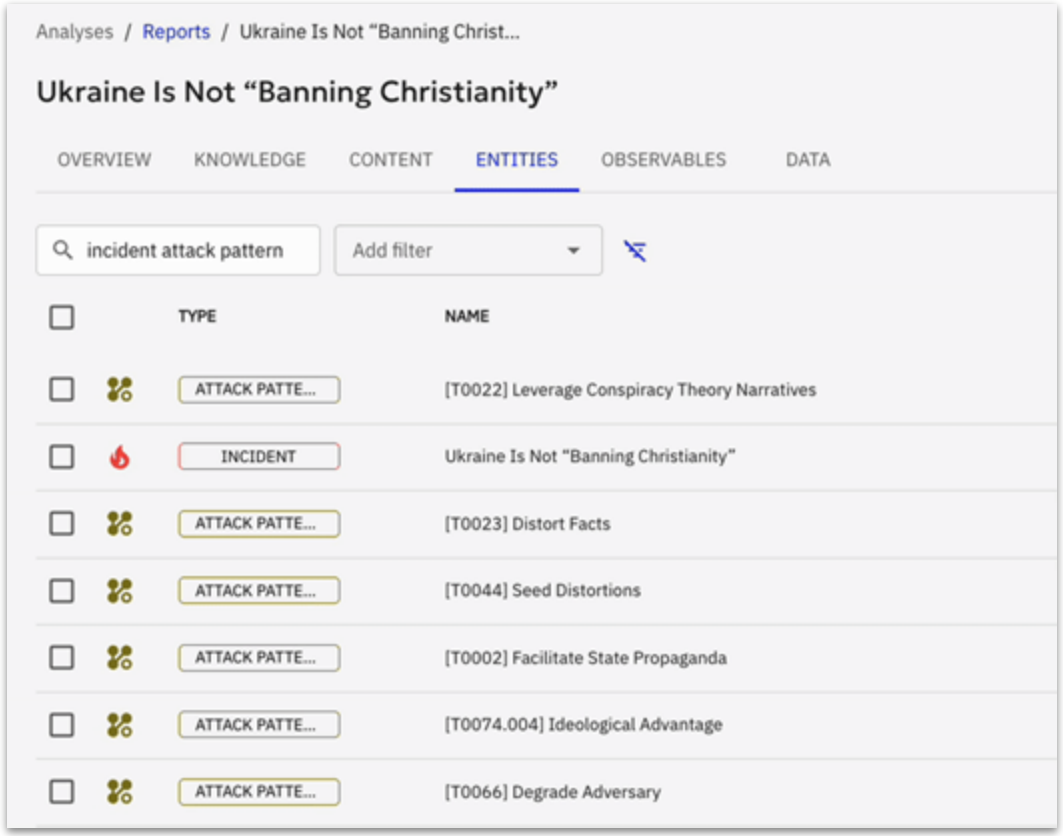
Source: Debunk.org

Case Study: Ukraine Is Not “Banning Christianity”

This operation used **Russian state media** and **Kremlin-aligned social media.**

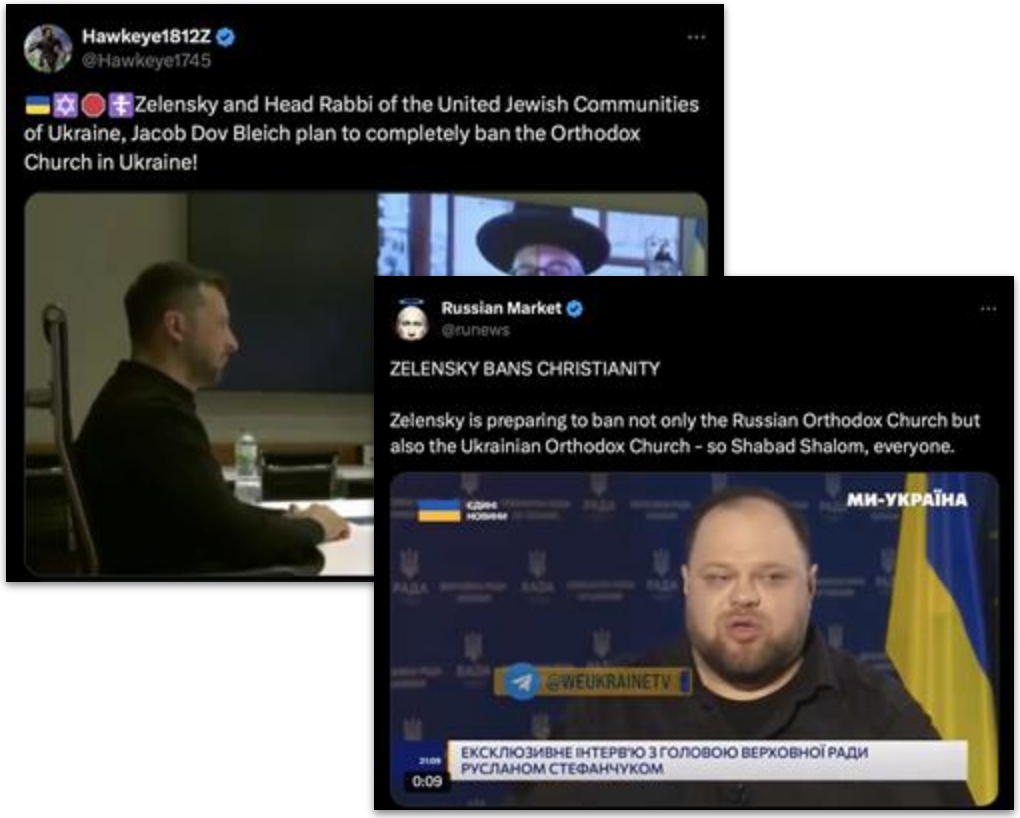
Goal: spread a narrative framing Ukraine’s actions against the Orthodox Church as a ban on Christianity, laced with antisemitic conspiracy theories.

The campaign portrayed Ukraine as **engaging in religious persecution** under alleged Jewish influence, though the number of channels used is unspecified.



Source: disinfowatch.org

Case Study: Ukraine Is Not “Banning Christianity”



Source: disinfowatch.org

Exercise 2.1

Question 1:

Drag-and-Drop Matching

Task: Match the Object to its definition:

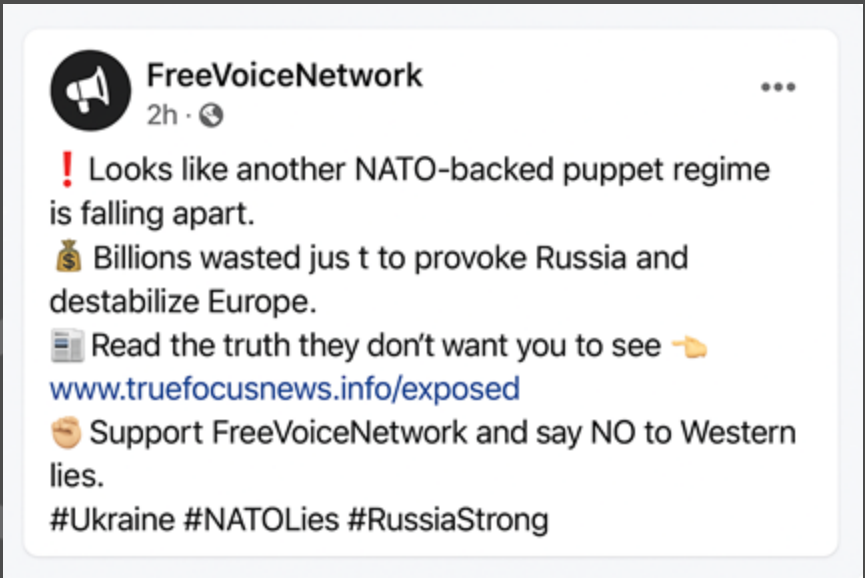
Please highlight the correct answer:

Object	Definition
Incident	Technique or method used
Observable (obsedrved data)	A coordinated disinformation effort
Campaign	Individual(s) or group(s) involved in malicious activity.
TTP	A specific instance of an event or a set of related events negatively affecting a target.
Threat Actor	A URL, username, hashtag

Exercise 2.2

Question 1:

Select the correct **TTP, narrative, actor, observable, threat actor** and t**argeted country** in a given social media post.



Please highlight the correct answer:

- **TTP** → T0023 – **Distort Facts;** T0014 Prepare Fundraising Campaigns; T0086.002 Develop AI-Generated Images (Deepfakes)
- **Observable** → www.facebook.com; **www.truefocusnews.info/exposed;** FreeVoiceNetwork
- **Threat Actor** → NATO; Europe; Russia; **FreeVoiceNetwork;**
- **Targeted Entity** → **NATO; Ukraine; Europe;** Russia; FreeVoiceNetwork;

Key takeaways

STIX 2.1 is a flexible and standardized format that enables structured modeling of disinformation threats — not just cyber ones.

Disinformation campaigns can be encoded as interconnected STIX objects: actors, arratives, channels, TTPs, observables, and victims.

OpenCTI visualizes these STIX objects through knowledge graphs, timelines, correlation views and matrix tools.

The DISARM Framework brings structure to disinfo behaviors, allowing them to be encoded as STIX attack patterns.

Visual tools in OpenCTI help analysts track campaigns, identify repeat tactics, and produce evidence-based insights for response and reporting.

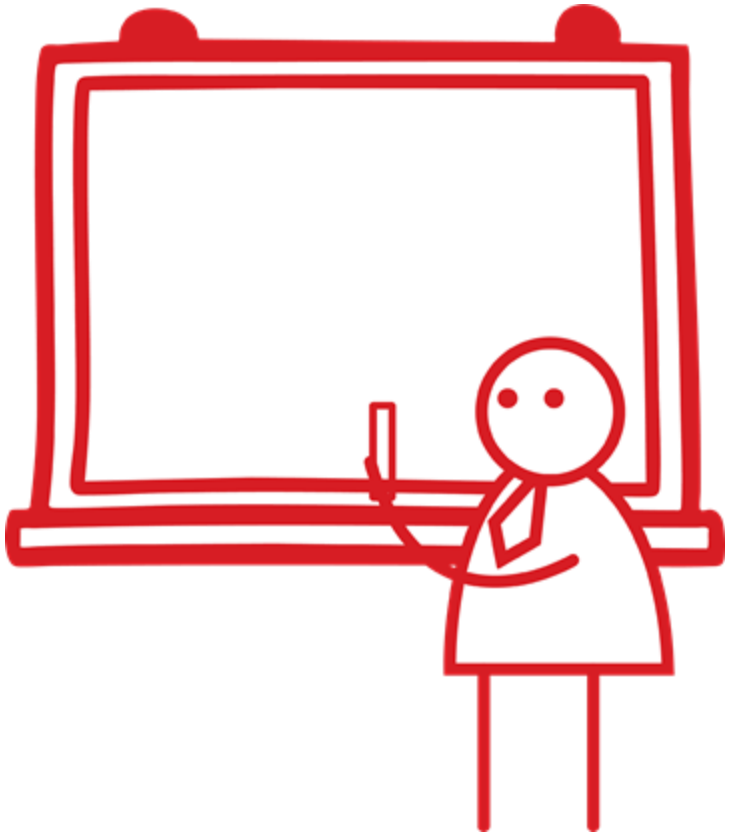
Structured codification improves data sharing, cross-platform detection, and collaborative analysis across organizations.

3. UPLOADING DATA INTO OPENCTI

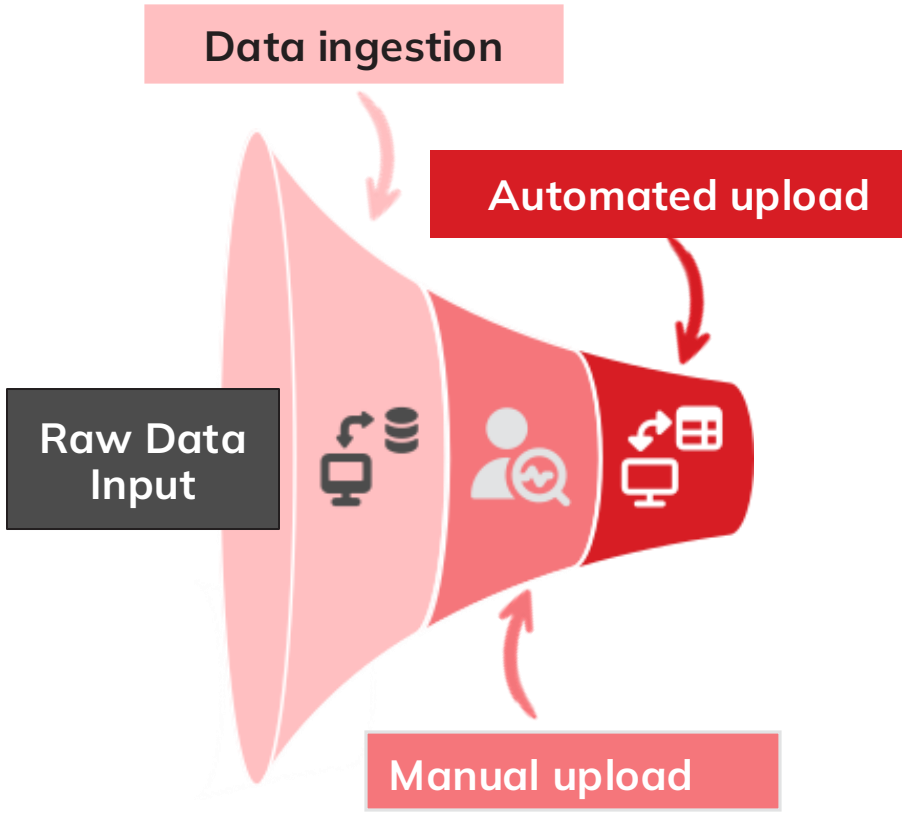
After Completing This Part You Will:

01 Be able to **manually enter data in OpenCTI,** including the creation of basic entities such as **threat actors, campaigns,** and **indicators relevant to disinformation analysis.**

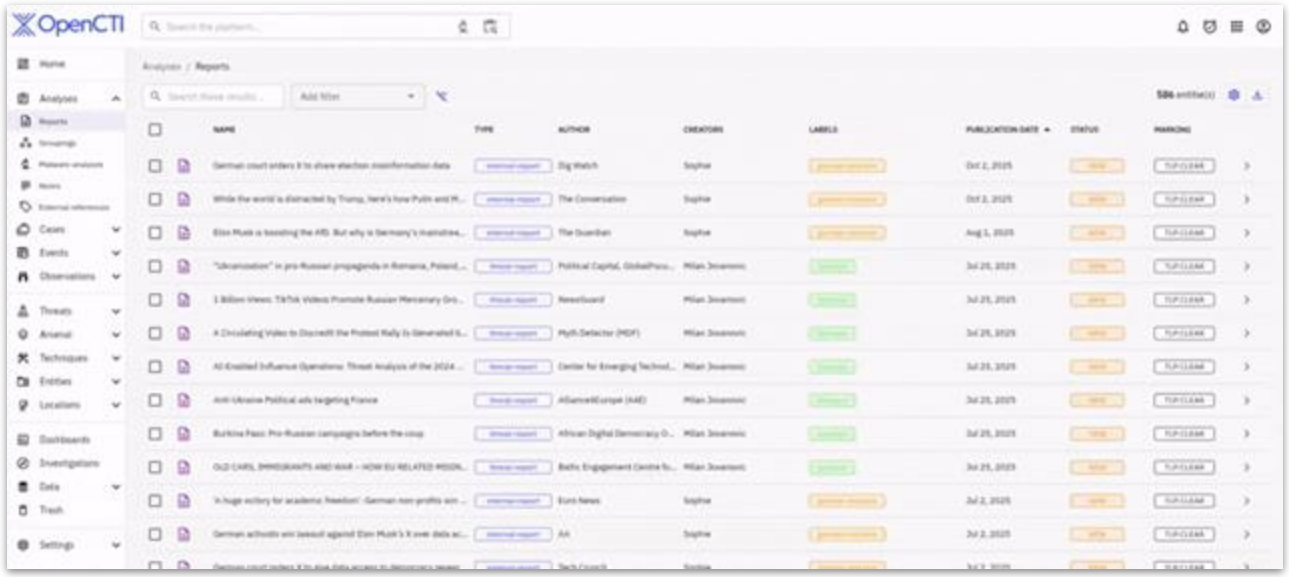
02 Upload structured data in **CSV or JSON format** using standard templates or external tools (e.g., Debunk uploader) to **efficiently ingest multiple observables and entities.**



OpenCTI Knowledge Base For FIMI Investigations



Source: Debunk.org



OpenCTI Threat Actors Overview

From Data to Intelligence: STIX Objects

Threats

Threat actors, Intrusion sets, Campaigns

- Groups or individuals responsible for hostile activity.
- Linked to intrusion sets and campaigns.

Arsenal

Channels, Tools, Vulnerabilities

- Tools, infrastructure, and software used by threat actors.
- May include exploited vulnerabilities.

Locations

Regions, Countries, Cities

- Geographic focus of threat activity.
- Used to identify affected areas.

Techniques

Attack patterns, Narratives, Courses of action

- Includes attack patterns and disinformation narratives.
- Describes operational techniques.

Entities

Events, Organizations, Individuals

- Specific people or organizations involved in disinformation.
- Covers both actors and targets.

Analyses

Reports, Groupings, External references

- Documents and analytical groupings.
- Supports contextual and strategic insights.

STIX Domain Objects Upload Methods

Manual Entry

- Manual Entry allows users to add data directly via the user interface.
- Ideal for quick, small-scale inputs or exploratory work.

CSV Upload

- Use CSV Upload to bulk-ingest structured data using a predefined template.
- A scalable and repeatable method suited for uploading multiple observables or SDOs efficiently.

Connectors

- Connectors automate data ingestion from external sources like threat intel feeds, or even custom tools.
- Once set up, they ensure continuous synchronization and reduce manual overhead.

STIX / JSON

- Ingest STIX 2.1-formatted JSON files directly into OpenCTI.
- Ensures compatibility with other CTI systems and standards.

APIs

- OpenCTI exposes APIs to programmatically send or retrieve data.
- Supports automated workflows and system-to-system integrations.

PyCTI Library

- Use the PyCTI to interact with the platform programmatically.
- It simplifies API calls and helps script bulk uploads, enrichments, or updates.

Understanding TLPs (Traffic Light Protocol)

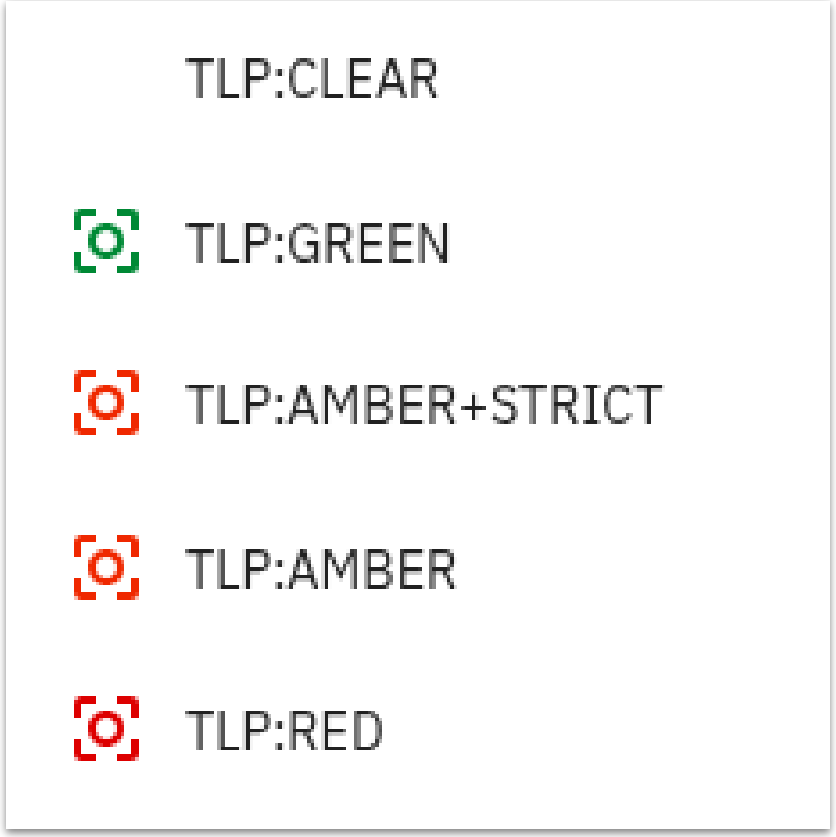
TLP (Traffic Light Protocol) is a system used to classify and control the sharing of sensitive threat intelligence data.

Levels and Meanings:

- **TLP:CLEAR** - fully public, can be shared without restriction.
- **TLP:GREEN** - shareable within your community or sector, but not publicly.
- **TLP:AMBER+STRICT** - internal only, no sharing with partners or affiliates.
- **TLP:AMBER** - share within your organization or trusted partners.
- **TLP:RED** - for the recipient only, no further distribution.

How It's Used in OpenCTI:

- Every uploaded document or entity can be **tagged with a TLP level**.
- Controls who can see and share intelligence within or outside OpenCTI.



OpenCTI TLPs

Source: Debunk.org

Connectors in OpenCTI

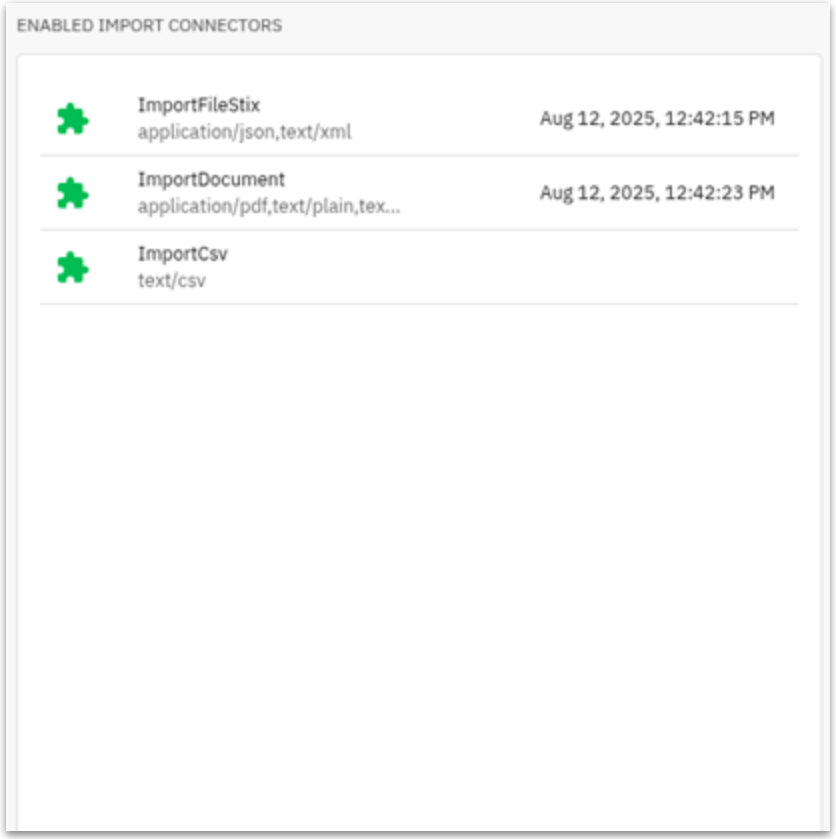
Connectors in OpenCTI serve as dynamic gateways to import data from diverse sources.

Each connector is built to **handle specific data types** and **structures**, offering flexible configuration based on your needs.

Once initialized, connectors operate in real-time, continuously importing fresh intelligence.

The Connector Ecosystem spans threat feeds, databases, and enrichment tools, categorized as:

- **Import Connectors** (data ingestion)
- **Enrichment Connectors** (contextual updates)
- **Stream Consumers** (live feeds)



OpenCTI Enabled Import Connectors

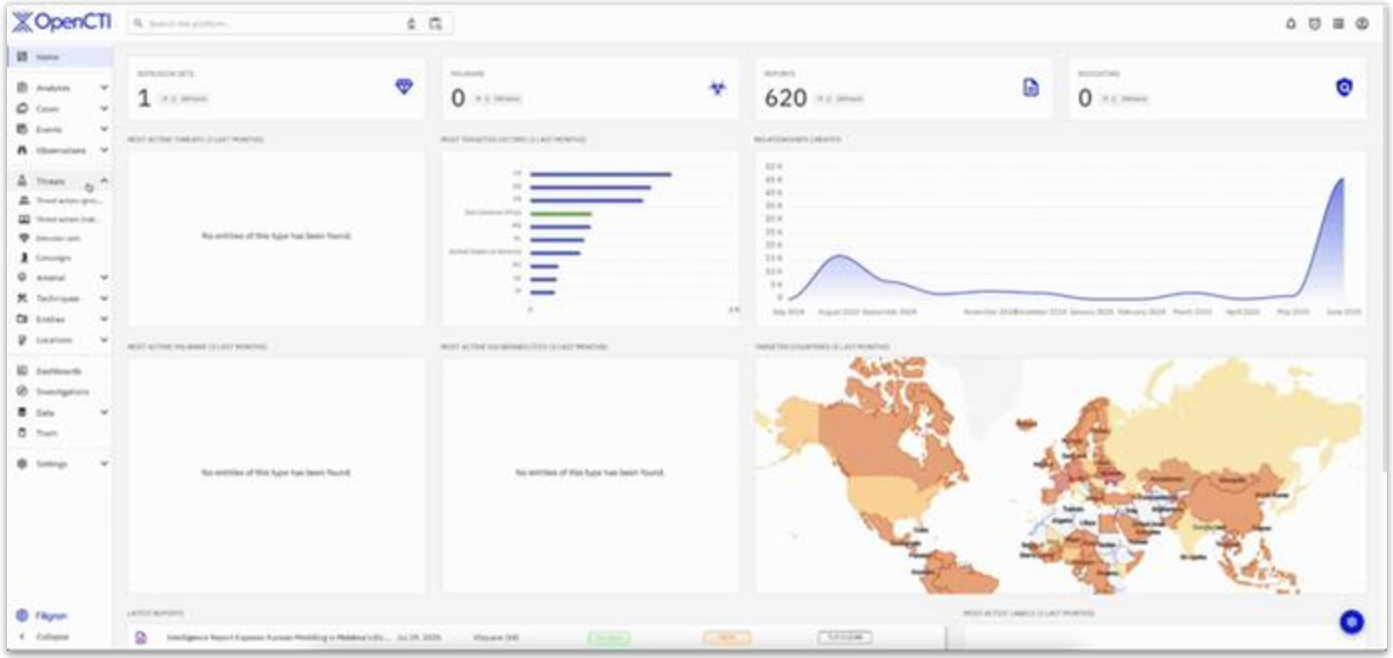
Source: Debunk.org

Manual Upload

Home -> Threats -> Threat Actors

Fill in fields: Name, Type, Description ...

Save via the User Interface



Source: Debunk.org

Manual Upload

Click the following link or scan the QR code:

https://www.dropbox.com/scl/fi/5swmnohyo2ubvgwrzn02l/manual-upload.mp4?rlkey=bibwffdl3le8k8srshkwxnlp3&st=jqv329t4&dl=0

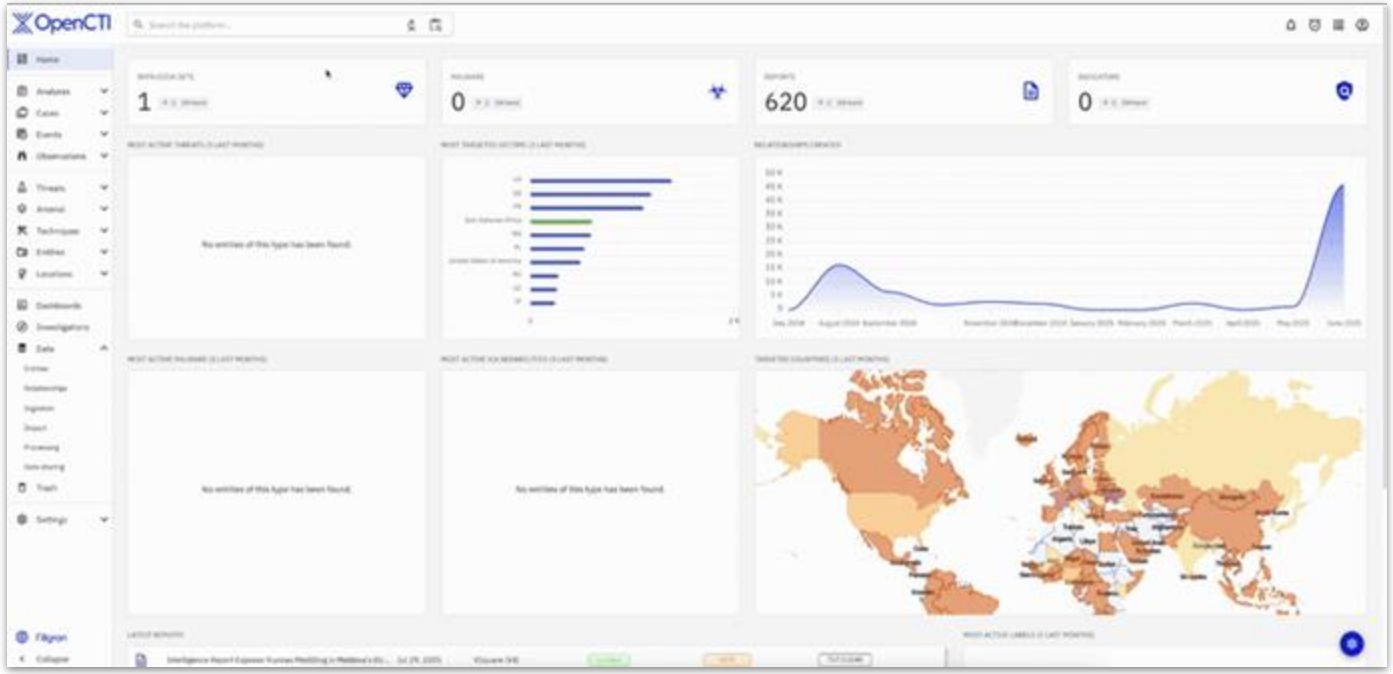
Source: Debunk.org

Upload - CSV Mapper

Fill CSV with the appropriate headers and rows

Data → Import → Uploaded files → CSV

Save via the User Interface



Source: Debunk.org

Upload - CSV Mapper

Click the following link or scan the QR code:

https://www.dropbox.com/scl/fi/gn9bfacnv96jenpujz3c9/csv-upload.mp4?rlkey=n0d4b7qguo7mfbzwz9qr69va2&st=4q4hs7yt&dl=0

Source: Debunk.org

Upload - JSON Mapper

Create data in STIX 2.1 JSON format

Data → Import → Uploaded files → JSON

Save via the User Interface

Source: Debunk.org

Upload - JSON Mapper

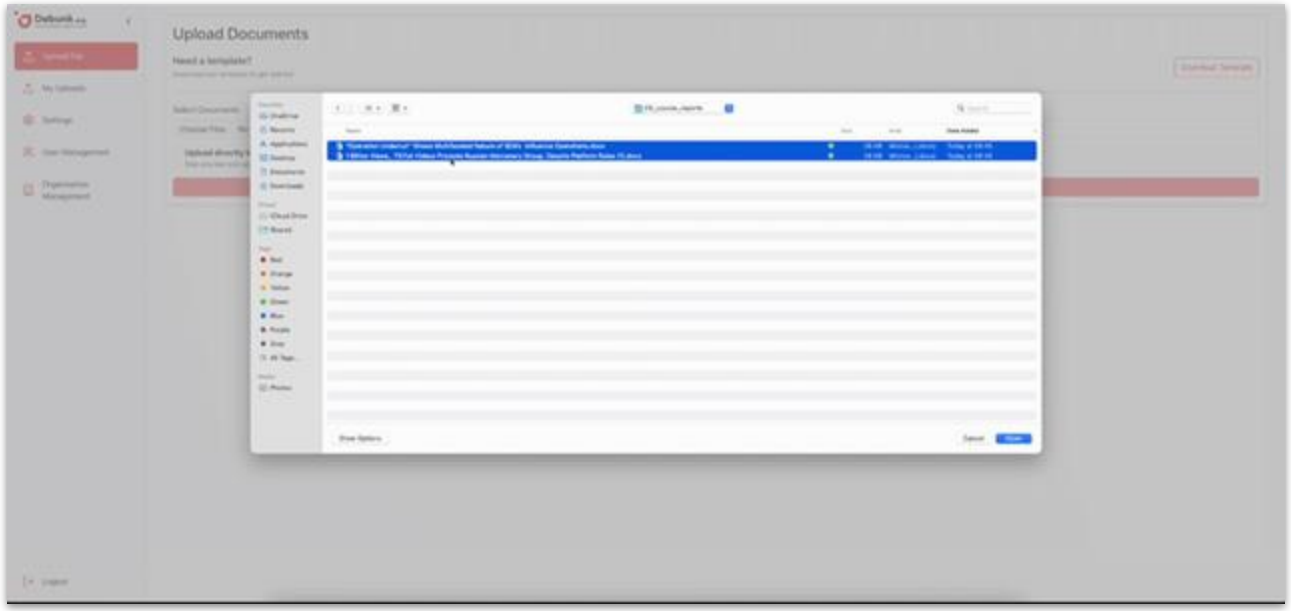
Click the following link or scan the QR code:

https://www.dropbox.com/scl/fi/wk44coijr60fubwegyduq/json-mapper.mp4?rlkey=qpnbesdxwgdjy1g91ij1ucvce&st=gpe8u81e&dl=0

Source: Debunk.org

Automated Upload - Debunk Uploader

- You can use **Debunk.org scam investigation report template** to speed up documentation and ensure consistency.
- **Request access** to the Debunk.org platform and template via: *info@debunk.org*
- We update the template regularly — including **new policy labels, evidence fields,** and **automation helpers.** Make sure you're using the latest version before submitting.



Source: Debunk.org

Automated Upload - Debunk Uploader

Click the following link or scan the QR code:

https://www.dropbox.com/scl/fi/czhgj7o2jusjhkmwyzpna/automatic-upload-debunk-app.mp4?rlkey=34aw8kv8h9xzsvgznzjf1od4f&st=61jjsbqz&dl=0

Source: Debunk.org

When to Use Which

Manual upload:

Granular control: You can carefully define each entity and relationship

Low barrier to entry: No technical formatting or preprocessing needed

Immediate feedback: You see data as it's added and can correct mistakes on the fly

Useful for: Small-scale or exploratory analysis, Single cases or investigations

Automated upload:

Scalable and efficient: Bulk-upload hundreds of observables/entities at once

Repeatable: Ideal for recurring ingestion (e.g., OSINT, threat intel feeds)

Supports STIX 2.1 standards: Useful for sharing data across systems

Useful for: Large-scale or systematic analysis, Multi-case investigations

Key Takeaways

OpenCTI allows two primary data upload methods:

1. **Manual** upload for precise, small-scale entry;
2. **Automated** upload for scalable, repeatable ingestion.

You can ingest multiple entity types, including: Threat actors, Campaigns, Indicators, Narratives, Tools, Reports, and more.

Manual entry provides control and visibility, ideal for exploration and individual investigations.

Automated ingestion (CSV/JSON/API) is best for high-volume, ongoing, or integrated workflows (e.g. Debunk Uploader).

Choosing the right upload method depends on scale, frequency, and technical context.

4. ANALYSIS AND VISUALISATION

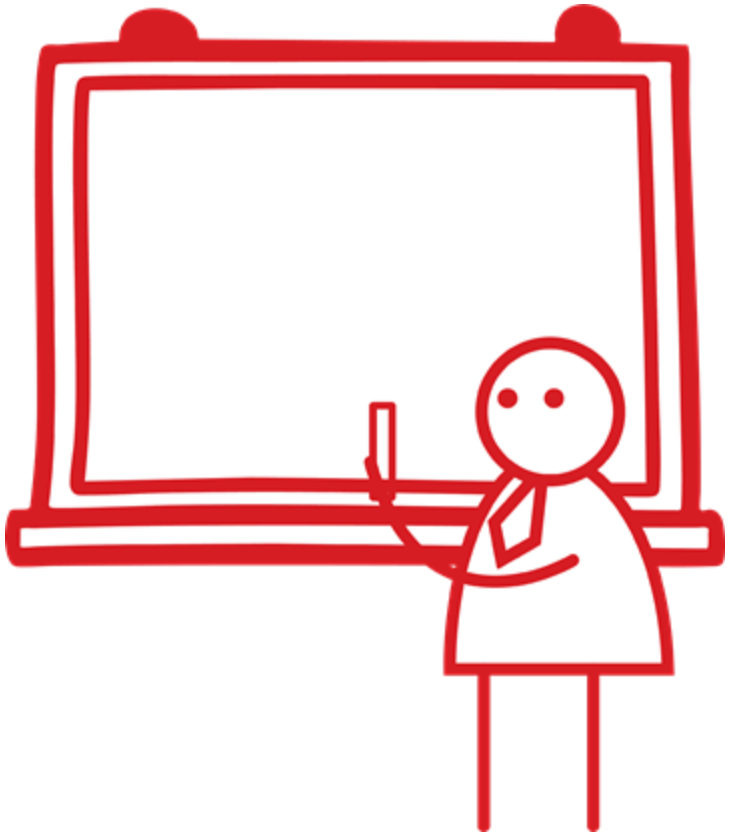
After Completing This Part You Will:

01 Navigate and customise **OpenCTI visualisation** tools to explore FIMI datasets.

02 **Identify and map relationships** between campaigns, threat actors, narratives, and channels.

03 Detect **patterns, clusters,** and **coordination** by analysing network structures and connections.

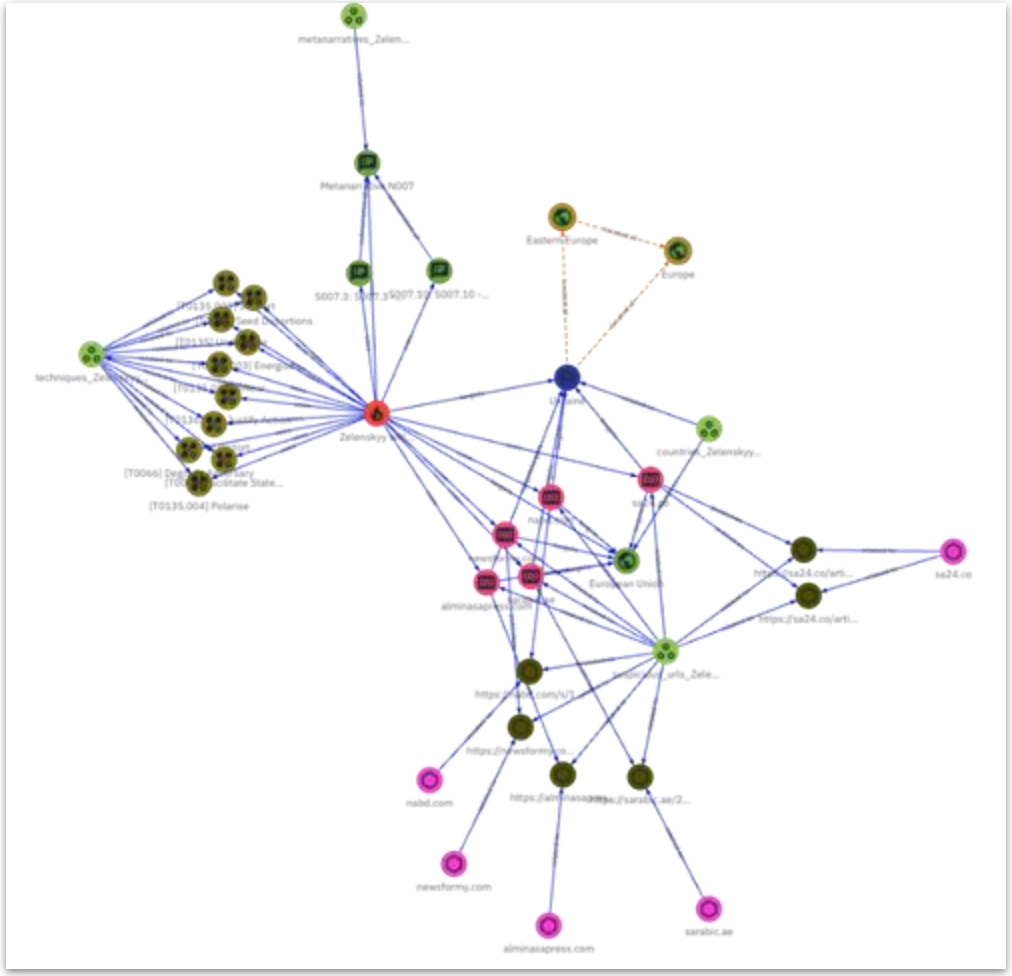
04 Apply filtering and pivoting techniques to focus on specific **incidents, entities,** or **time periods.**



Source: Debunk.org

Knowledge Graph

- Interactive graph connects STIX objects like: **Threat actors → Campaigns → Narratives → Observables → Channels**
- Helps spot c**oordinated operations** and repeated techniques.
- Enables **exploration of relationships** at different levels of granularity.



Source: Debunk.org

Knowledge Graph

Click the following link or scan the QR code:

https://www.dropbox.com/scl/fi/dr3ryfemrrzn9jw5w64nq/knowledge-graph.mp4?rlkey=rpnfwg8i37w0acvpgmfbp66jm&st=f8mfafyu&dl=0

Source: Debunk.org

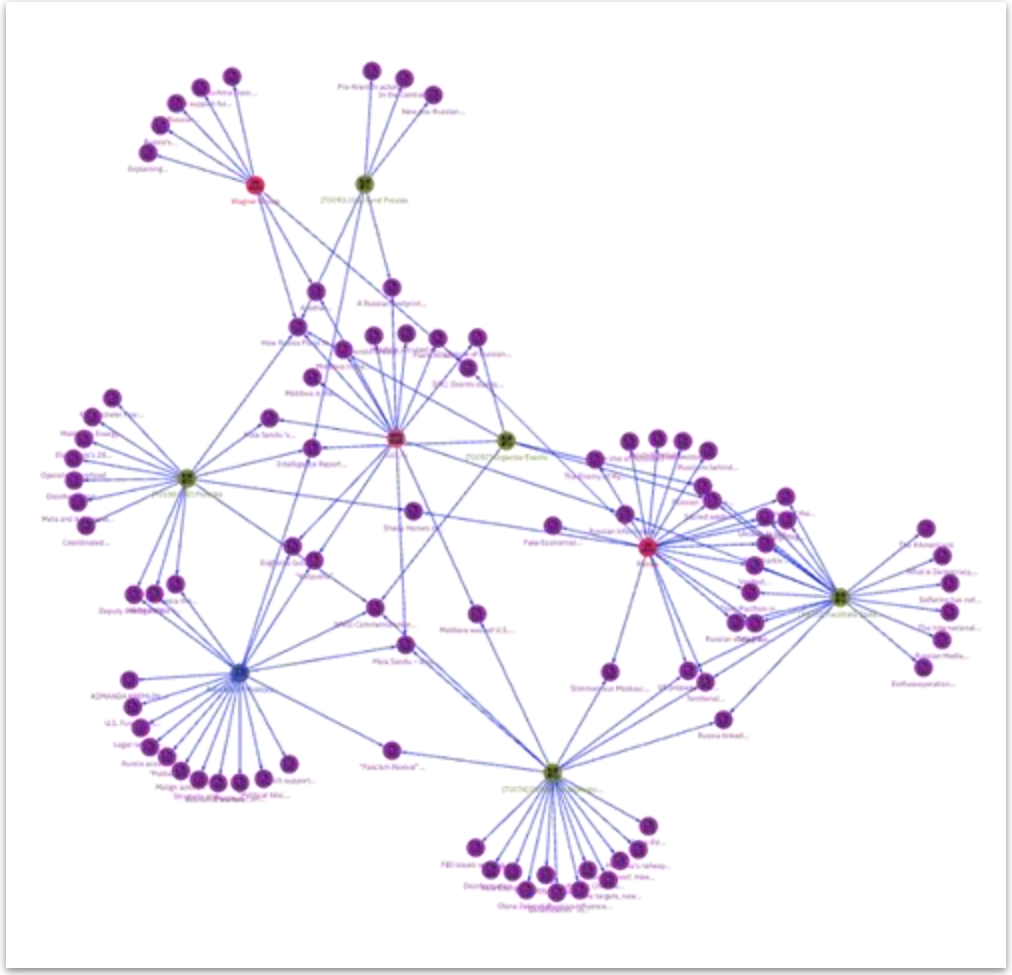
Timeline view

Timeline view from OpenCTI, based on the report “Anti-Ukraine Political ads targeting France”, published by Alliance4Europe

Source: Debunk.org

Correlation Graph

- Highlights **shared elements** (e.g., observables, actors, channels) across multiple incidents or campaigns.
- Helps detect **possible coordination**, reuse of infrastructure, or cross-campaign influence tactics.
- Reveals **relationships that may not be obvious** in isolated reports or timelines.
- Supports **attribution, prioritization,** and **threat clustering** for deeper investigations.



Source: Debunk.org

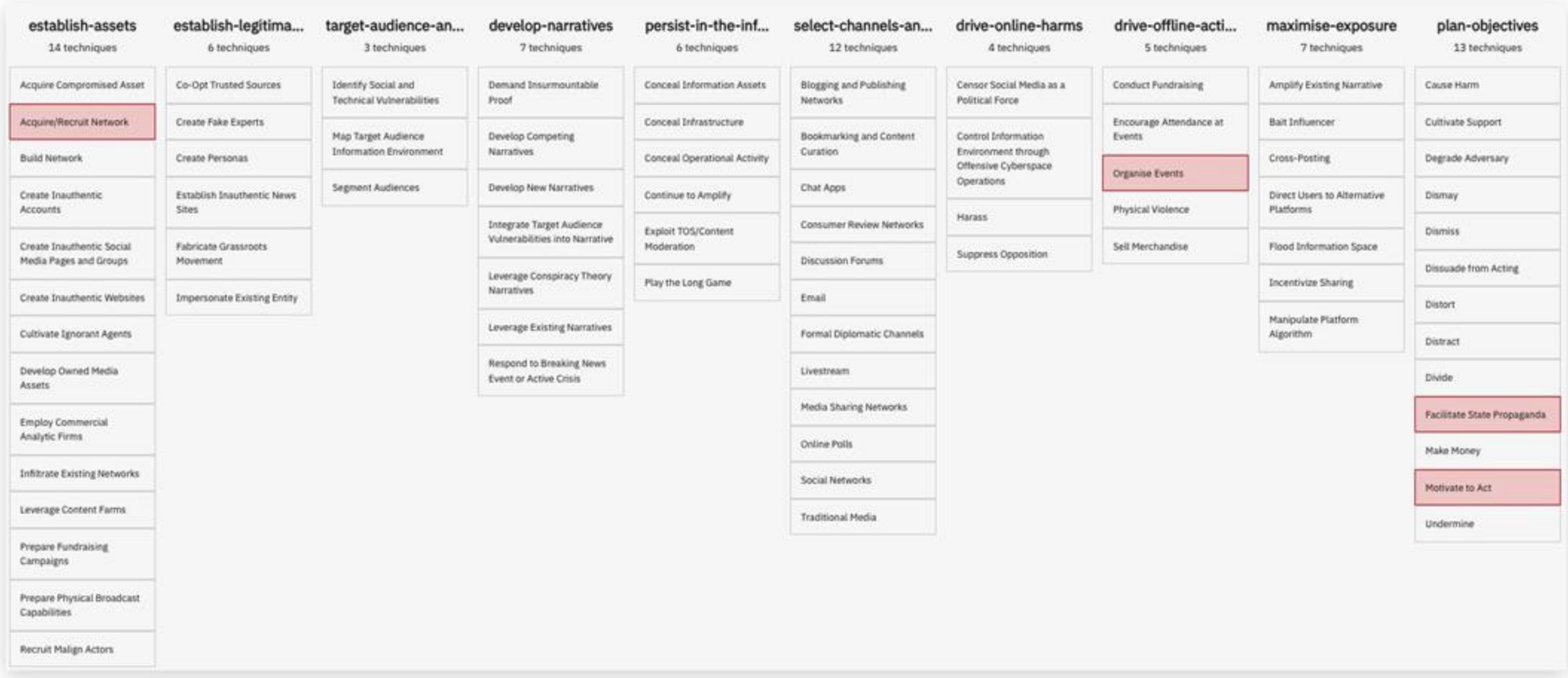
Correlation Graph

Click the following link or scan the QR code:

https://www.dropbox.com/scl/fi/29colocfminhe6dtnxq50/correlation-final.mp4?rlkey=d2oc8ih0zxxwptt86vf3mibyq&st=nug0go1x&dl=0

Source: Debunk.org

Matrix Graph



Matrix Graph based on the report "How Russia Plans to Take Back Moldova", published by Vsquare in 2023.

Source: Debunk.org

Matrix Graph

Click the following link or scan the QR code:

https://www.dropbox.com/scl/fi/ss0rhkkmn6sdgn941qzqn/matrix-view.mp4?rlkey=iblmv8nf8dwzyq70iadzchmzw&st=q6056mny&dl=0

Source: Debunk.org

Exercise 1.1

Type of the exercise:

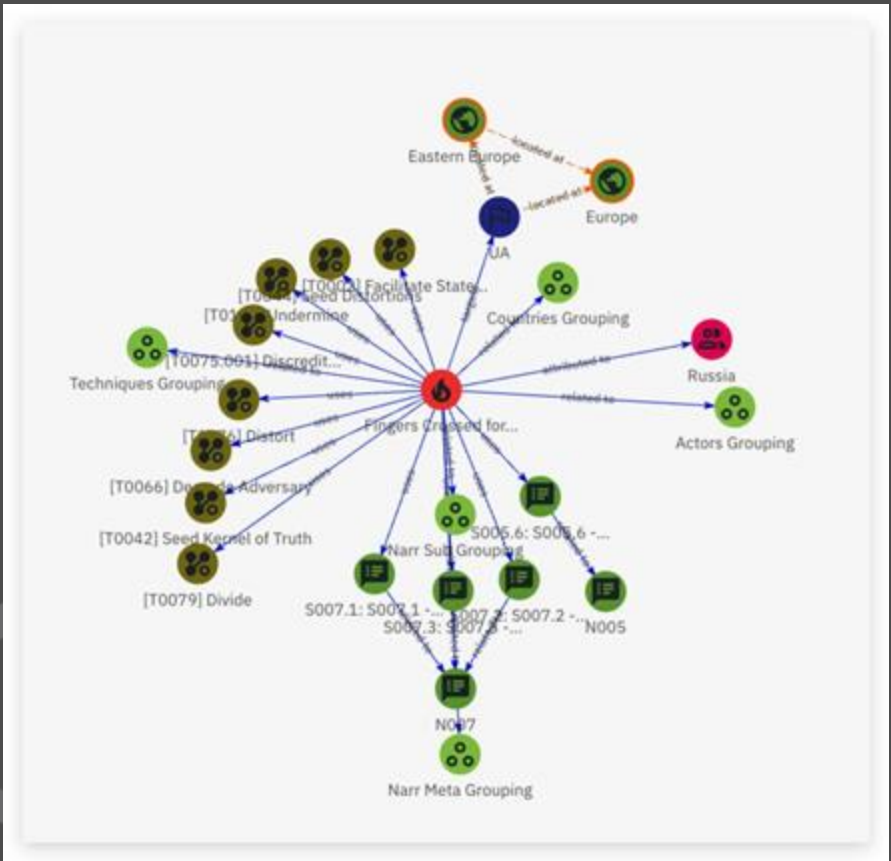
Scenario / Multiple Choice

Please select your type of the exercise from these options:

- True - false
- Single choice
- Multiple choice
- Sort the cards into categories
- Drag-drop
- Scenario
- Match the sentence
- Pick one or many
- Fill in the missing word
- Rank the options

Exercise 1.1

Question 1:



Please highlight the correct answer:

Question 1:

Which country is directly targeted in the showcased incident?

A) Russia

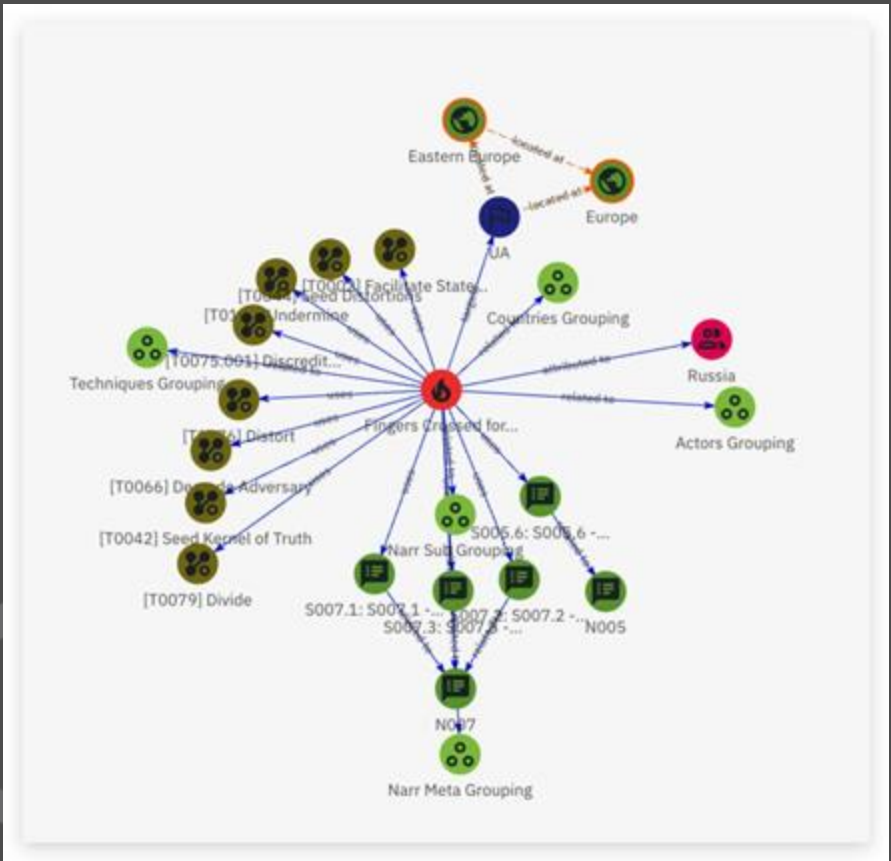
B) Ukraine

C) Eastern Europe

D) Europe

Exercise 1.1

Question 1:



Please highlight the correct answer:

Question 2:

Which threat actor is linked to this incident?

A) NATO

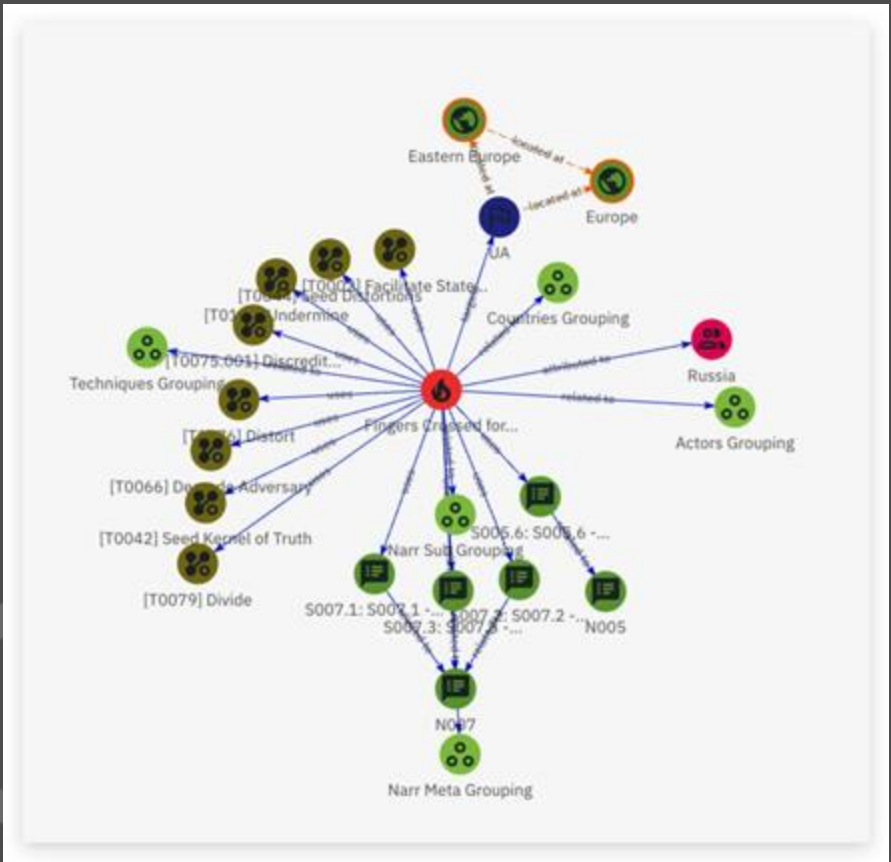
B) Russia

C) EU

D) Eastern Europe

Exercise 1.1

Question 1:



Please highlight the correct answer:

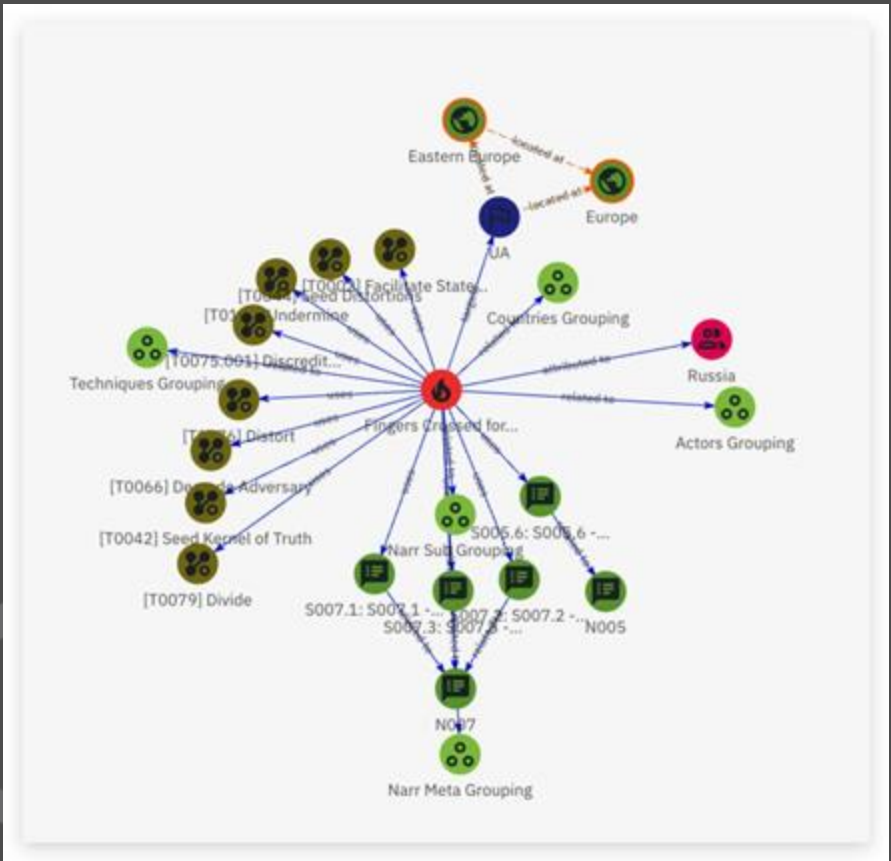
Question 3:

How many DISARM techniques are associated with this incident?

A) 5
B) 7
C) 8
D) 10

Exercise 1.1

Question 1:



Please highlight the correct answer:

Question 4:

How many narratives and meta narratives are associated with this incident?

A) 5 narratives, 2 meta narratives

B) 4 narratives, 2 meta narratives

C) 2 narratives, 4 meta narratives

D) 6 narratives, 1 meta narrative

Key takeaways

Interactive Graph Views allows analysts to explore complex disinfo networks and relationships at various levels of detail.

Timeline View helps detect when content appeared, showing peaks in activity and campaign build-up around real-world events.

Correlation Graphs reveal shared elements across multiple campaigns — helping analysts identify coordination or reused infrastructure.

Matrix View, powered by the DISARM framework, maps actors to disinformation techniques (TTPs), exposing behavioral patterns and strategic intent.

All views together support **strategic threat profiling, cross-case analysis, and evidence-based attribution** — turning raw content into structured intelligence.

5. DASHBOARDS FOR DISINFORMATION TRENDS

After Completing This Part You Will:

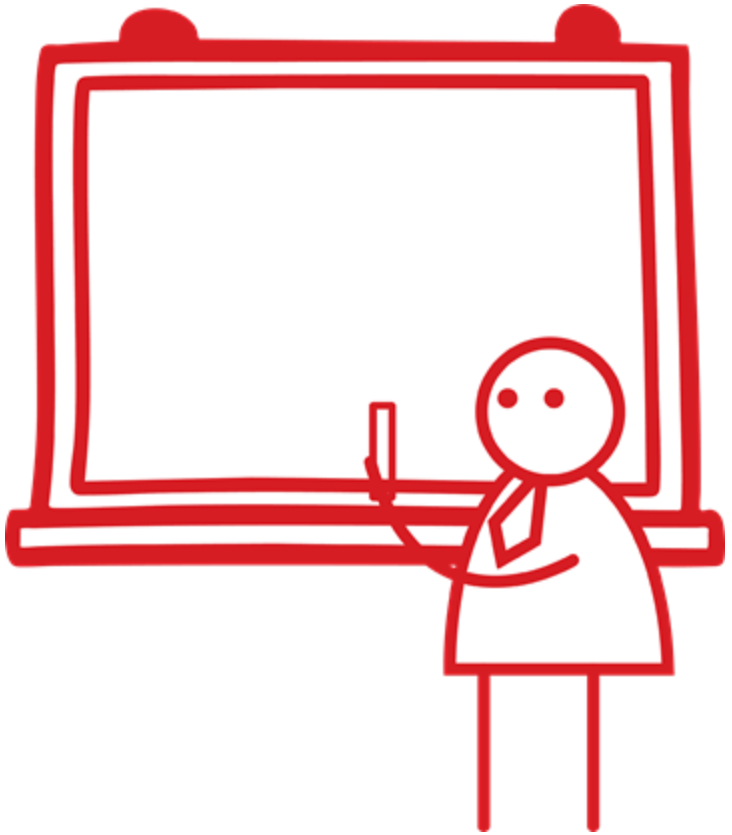
01 **Visualize** patterns and trends in real time.

02 **Summarize** large volumes of structured data into actionable insights.

03 **Identify** top narratives, actors, platforms, and targets.

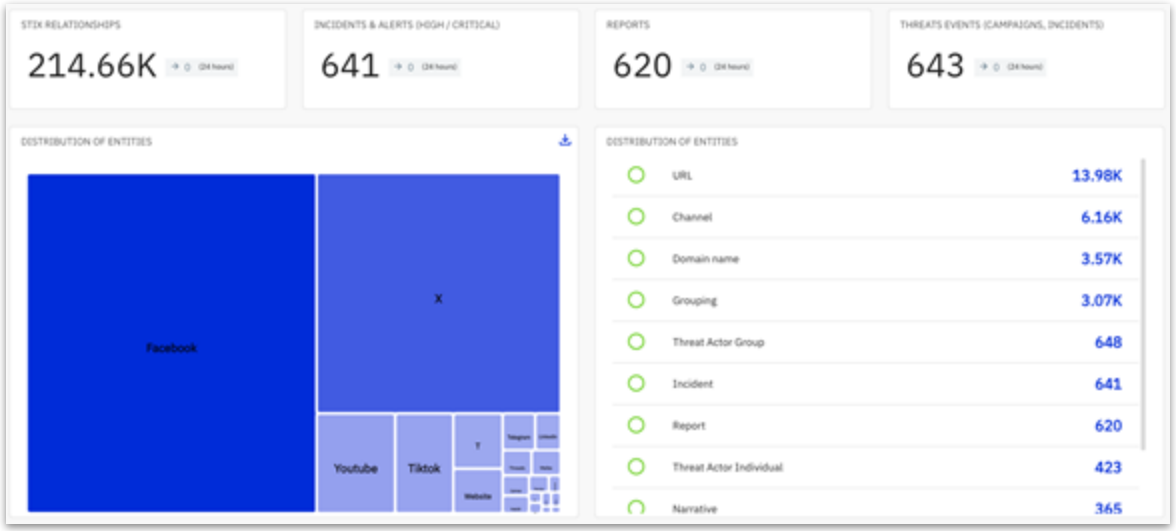
04 **Monitor** disinfo operations across regions or timeframes.

05 **Share** findings with non-technical stakeholders through intuitive visuals.



Dashboard Basics in OpenCTI

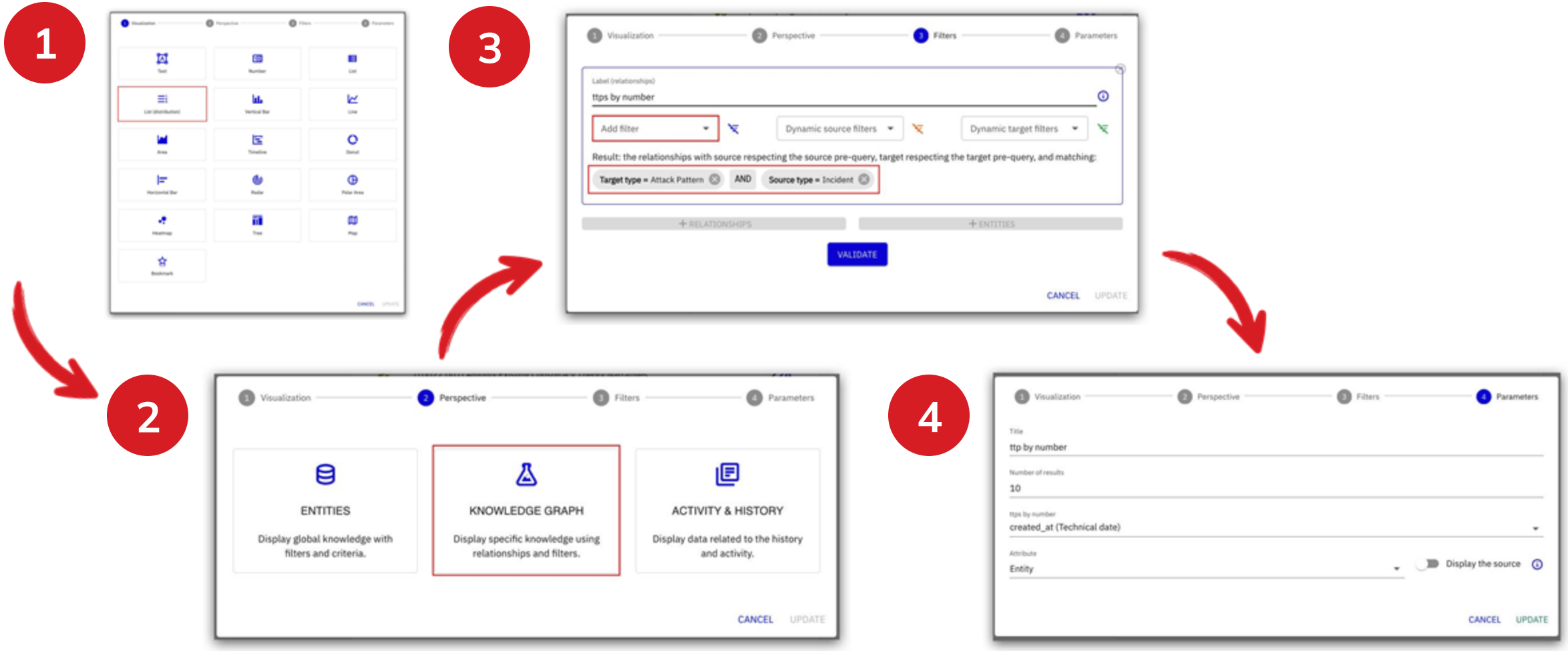
- Access via the **left-hand OpenCTI menu** under **“Dashboards”.**
- **Core widgets** include: pie charts, bar charts, time series, tables.
- Use **filters** to customize by tag, time range, or entity type.
- **Export options:** PNG, PDF, JSON for sharing insights externally.



The screenshot shows an OpenCTI dashboard with key metrics (STIX relationships, incidents, reports, threat events) and entity distributions.

Source: Debunk.org

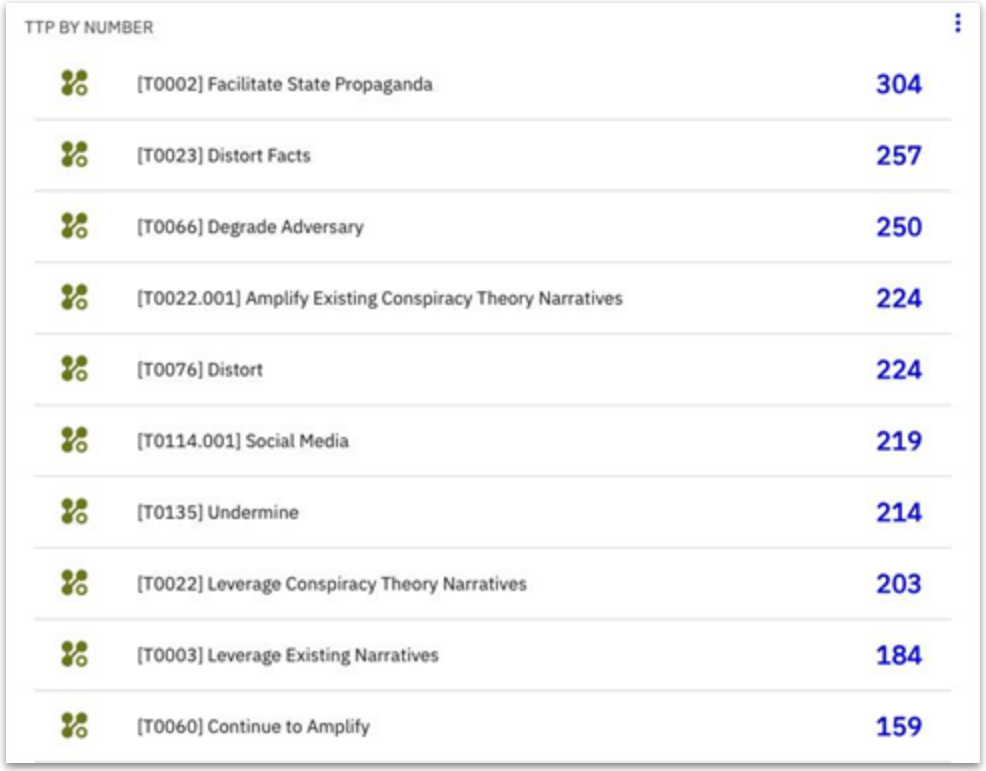
Creating Widgets - DISARM TTPs Overview



Source: Debunk.org

Creating Widgets - TTPs Overview

- Displays the **most frequently** observed **TTPs** across all incidents in the dataset.
- Each item is tagged with its DISARM ID, enabling **consistent** reporting and analysis.
- Useful for spotting **dominant** operational **patterns** in FIMI campaigns.
- Can **inform** strategic mitigation **efforts** and **drive** targeted **counter-disinfo** responses.

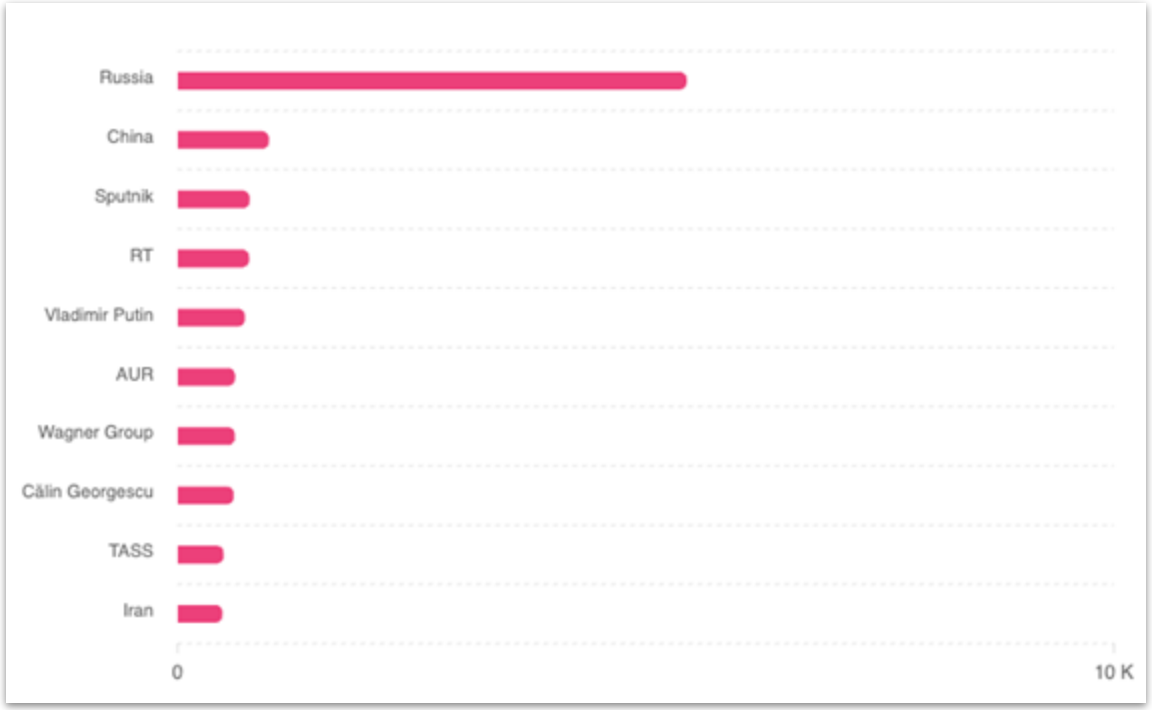


The screenshot shows the most frequently used DISARM TTPs across all reports in the dataset,

Source: Debunk.org

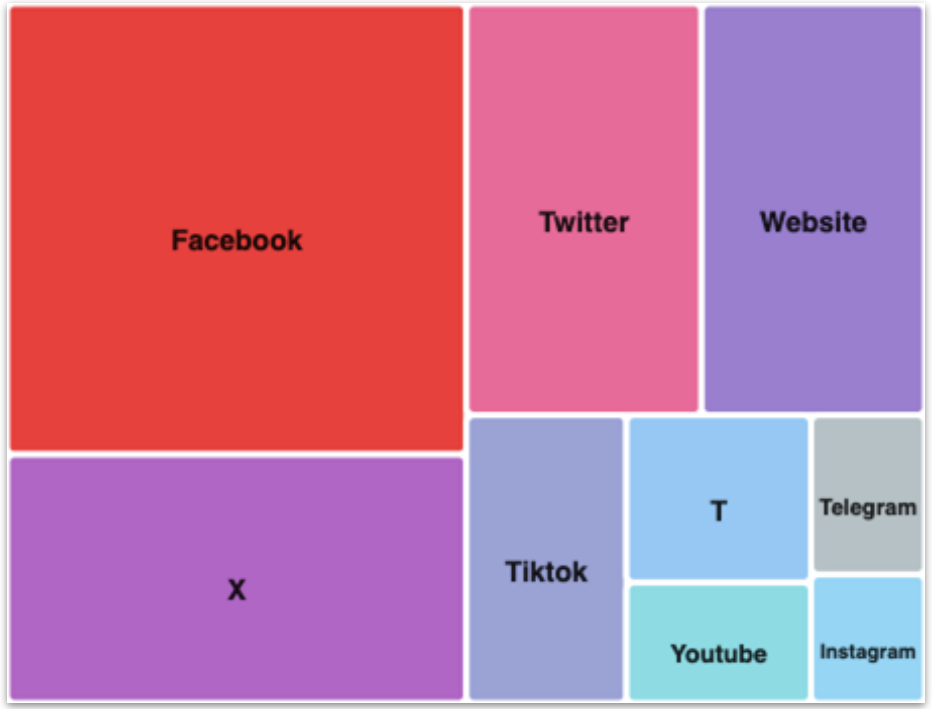
Other useful widgets

TOP 10 ACTIVE THREAT ACTORS



Widget displaying the top 10 most active threat actors in our dataset.

MOST USED CHANNELS

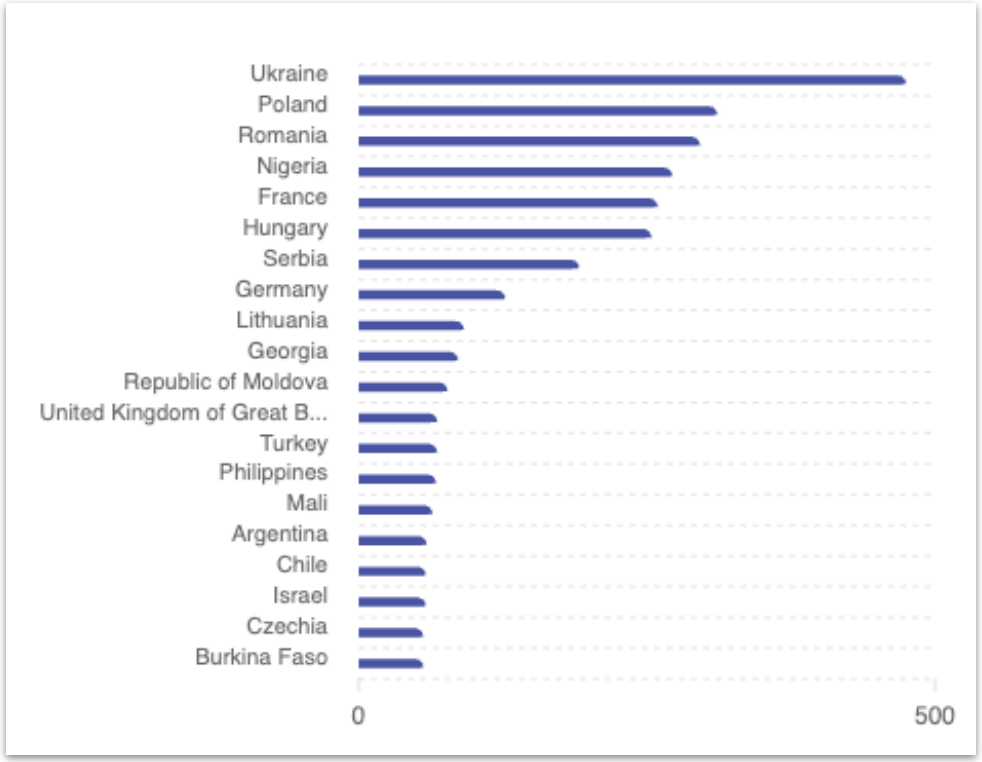


A treemap widgets showing the most used channels in our dataset.

Source: Debunk.org

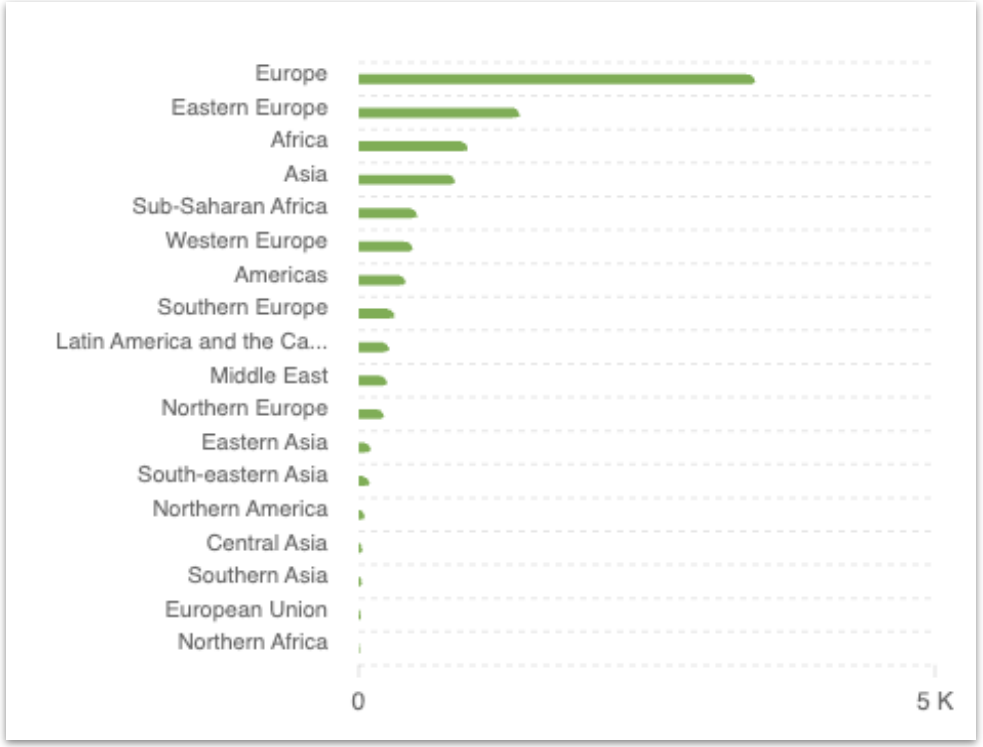
Other useful widgets

MOST TARGETED COUNTRIES



Widget displaying most targeted countries in our dataset.

MOST TARGETED REGIONS

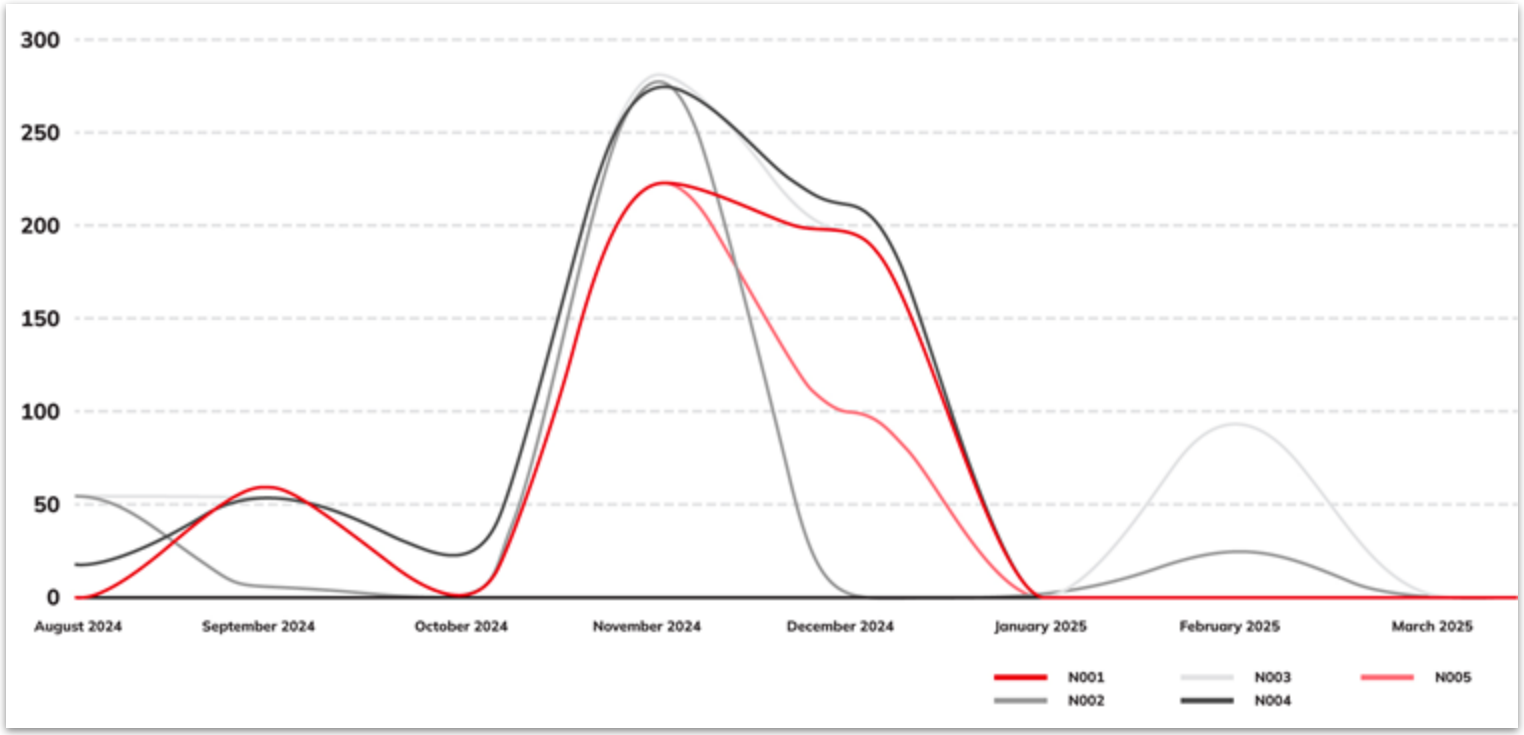


Widget displaying the most targeted regions in our dataset.

Source: Debunk.org

Other useful widgets

NARRATIVES OVER TIME



The chart shows 5 different narratives tracked over time.

N001
Country's government fails to uphold democratic standards and the rule of law

N002
Status of the country is recognised and/or respected by other countries

N003
Relations of an entity with the West are not constructive/beneficial

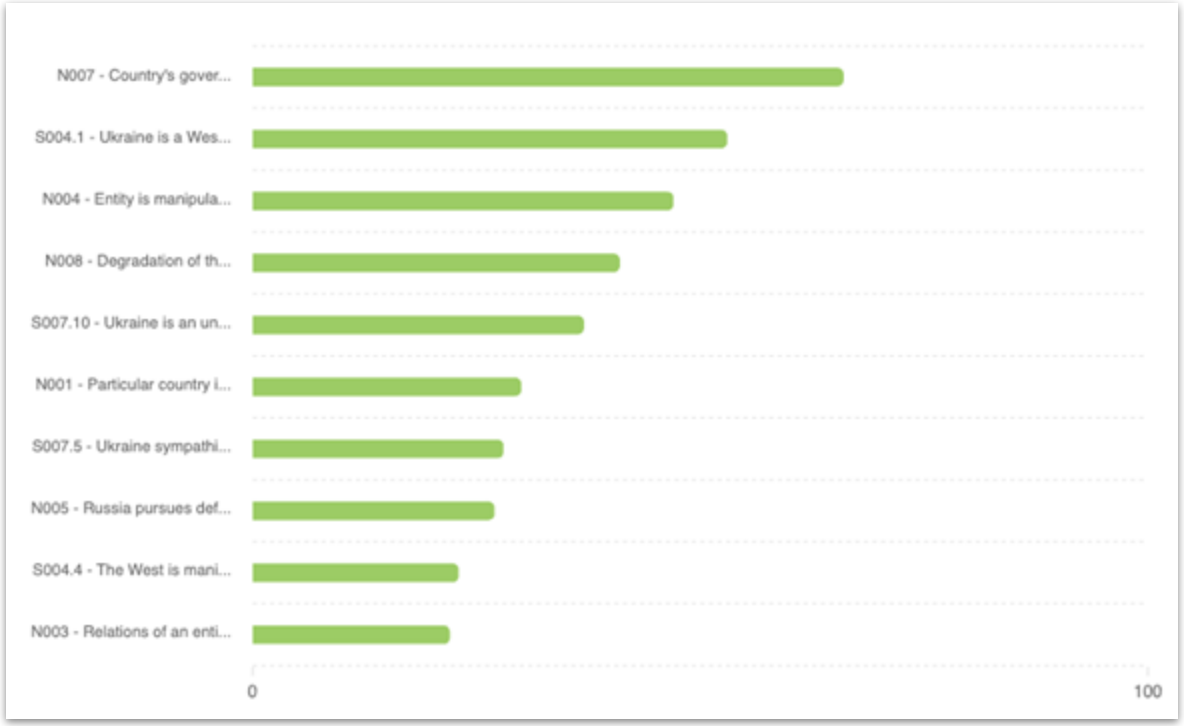
N004
Entity is manipulated by more powerful international system players

N005
Russia pursues defensive military agenda

Source: Debunk.org

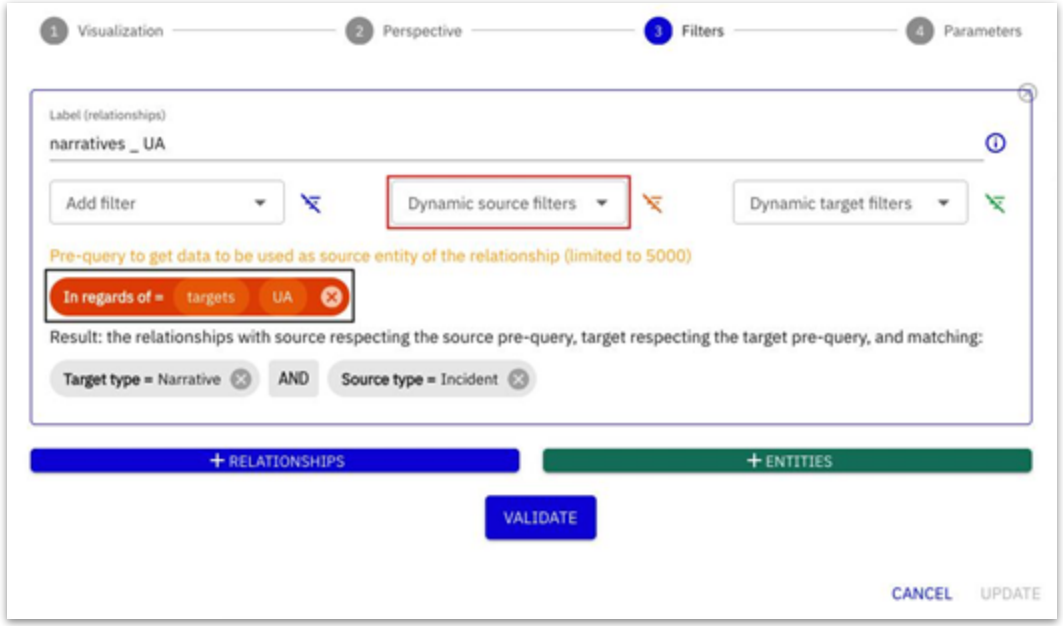
Target-related widgets

NARRATIVES TARGETING UKRAINE



Widget displaying narratives targeting Ukraine.

FILTERING SYSTEM

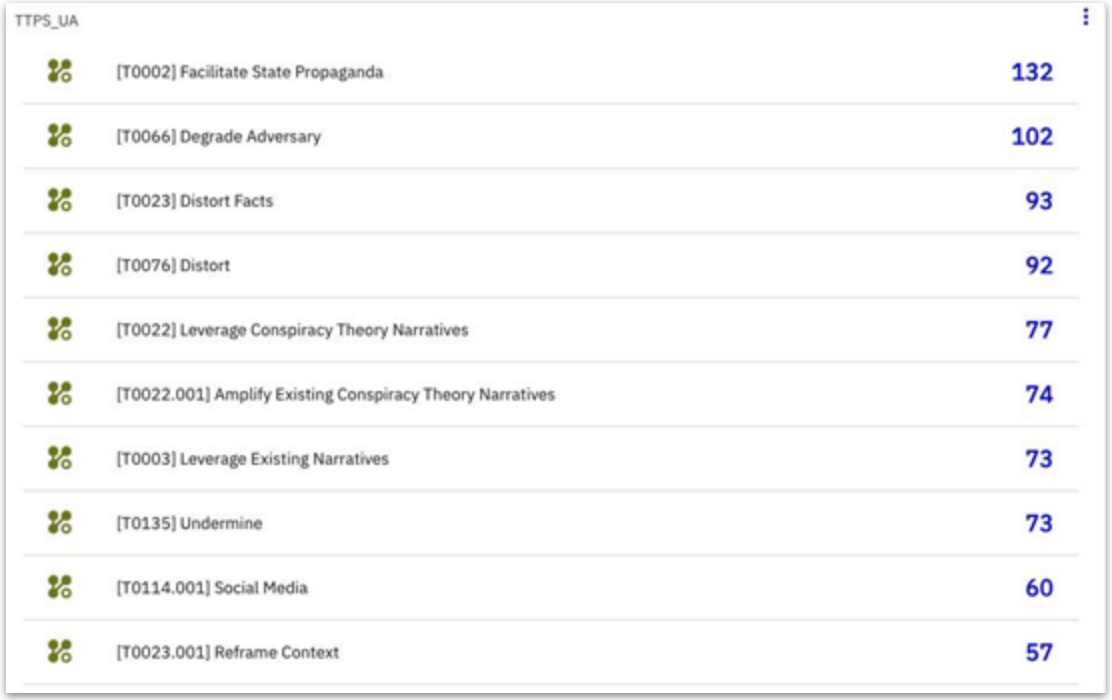


A screenshot displaying filtering system used to get the previous widget.

Source: Debunk.org

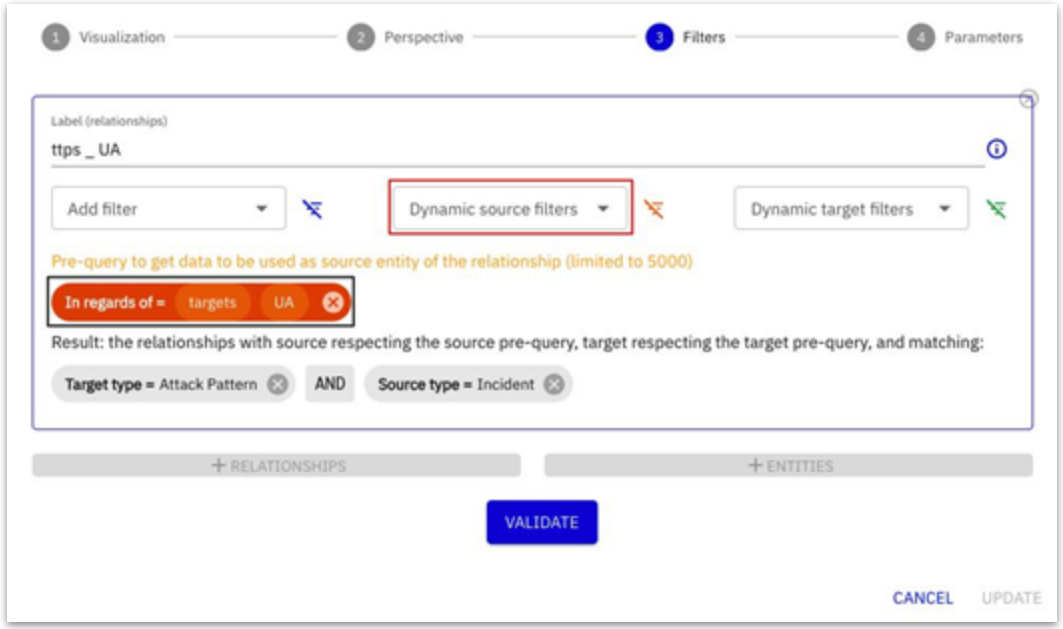
Target-related widgets

TTPs USED IN CAMPAIGNS TARGETING UKRAINE



Widget displaying TTPs used in reports targeting Ukraine.

FILTERING SYSTEM



A screenshot displaying filtering system used to get the previous widget.

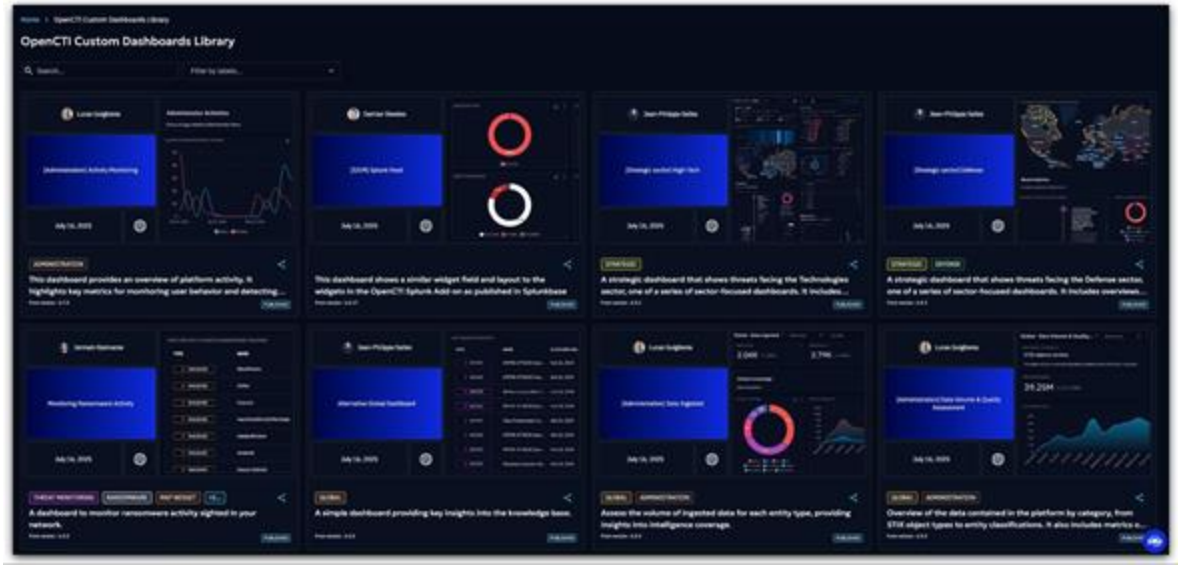
Source: Debunk.org

XTM Hub

- XTM Hub is a central forum to access **resources, share tradecraft,** and **optimize the use of Filigran's products** — fostering collaboration and empowering the community. (Filigran is the company behind OpenCTI and other threat intelligence and risk management tools.)

- OpenCTI **Custom Dashboards Library** **-** range of custom dashboards shared by community, enables users to **download** and **reuse existing templates,** saving time for creating from scratch.

- In the **Dashboards menu** in the OpenCTI, users can import **directly from XTM Hub** or **import downloaded dashboards** and **widgets in .json format.**



A screnshot of Filigran's XTM Hub.

Source: Filigran.io

Key Takeaways

Dashboards provide real-time **visual intelligence** for FIMI investigations

Widgets can display **trends** by actor, campaign, TTP, narrative, or platform

Filtering enhances precision—**focus on specific** timeframes, languages, or regions

Export options (PNG, JSON, PDF) allow for internal reporting or external sharing

A well-structured dashboard **empowers** both analysts and decision-makers.

QUIZ/TEST

Quiz/test for ‘OpenCTI: Why it matters for FIMI?’ section

Q1 – True/False
One key benefit of OpenCTI is replacing one-off, siloed investigations with a central, team-accessible knowledge base.

True Not True

Q2 – Single Choice
Which phrase best describes OpenCTI’s role in FIMI investigations?
a) A replacement for monitoring tools
b) A central hub for structured intelligence and collaboration
c) A social media analytics platform
d) A fact-checking news database

Q3 – Multiple Choice
Which of these tasks are part of Analyse & Map in OpenCTI?
a) Tracing relationships between actors, campaigns, and narratives
b) Adding confidence levels and thematic tags
c) Setting up keyword lists for monitoring
d) Exporting STIX or CSVs for partners

Q4 – True/False
In the FIMI cycle, Strategic Monitoring is usually done directly inside OpenCTI.

True **Not True**

Quiz/test for ‘Modeling FIMI IN STIX 2.1 and DISARM Framework’ section

Q1 – True/False
STIX 2.1 can be used to model both cyber threats and influence operations such as disinformation campaigns.

True **Not True**

Q2 – Single Choice
Which STIX object is most appropriate for representing a disinformation campaign?
a) Identity
b) Campaign
c) Location
d) Note

Q3 – Multiple Choice
Which of the following are valid STIX relationship types for linking a Threat Actor to a Campaign?
a) attributed-to
b) targets
c) related-to
d) authored-by

Q4 – Single Choice
In the DISARM framework, a Technique is:
a) A high-level strategic goal of an influence operation
b) A specific method or action used to achieve a tactic
c) The metadata describing a STIX object
d) A set of unrelated disinformation examples

Quiz/test for ‘Uploading Data Into OpenCTI’ Section

Q1 – Single Choice
Which of the following is NOT one of the supported STIX Domain Objects in OpenCTI?
A. Threat Actors
B. Narratives
C. Cryptocurrency Wallets
D. Campaigns

Q2 – True / False
The Debunk Uploader is incompatible with STIX 2.1 or DISARM templates.

True **Not True** (The Debunk Uploader is specifically designed to support STIX 2.1 and DISARM-compatible formats.)

Q3 – True / False
OpenCTI only allows uploading indicators like URLs or hashes — not context like actors or campaigns.

True **Not True** (OpenCTI supports full STIX context like actors, campaigns, and tools.)

Q4 – True / False
CSV uploads require clearly labeled columns and rely on the ImportCSV connector to ingest data.

True Not True

Quiz/test for ‘Analysis and Visualisation’ section

Q1 – True/False
The correlation view in OpenCTI is used to find and visualise relationships between entities in a dataset.

True Not True

Q2 – Single Choice
Which visualisation tool in OpenCTI allows you to see chronological sequencing of incidents, narratives, and observables?
a) Correlation view
b) Timeline view
c) Report view
d) Activity log

Q3 – Multiple Choice
Which of the following actions are possible in OpenCTI visualisation tools?
a) Apply filters by date
b) Pivot from one entity to related entities
c) Automatically block malicious domains
d) Export graphs

Q4 – True/False
The knowledge graph can only display relationships if both entities are part of the same campaign.

True **Not True**

Quiz/test for ‘Dashboards for Disinformation Trends’ section

Q1 – True/False
Dashboards in OpenCTI can be customised with filters to focus on specific entities, campaigns, or time periods.
True Not True

Q2 – Single Choice
Which widget type is best suited to track the frequency of a narrative over several months?
a) Time series
b) Pie chart
c) Bar chart
d) Table

Q3 – Multiple Choice
Which of the following insights can be obtained from OpenCTI dashboards for FIMI analysis?
a) Top channels spreading a narrative
b) Most active threat actors in a given period
c) Real-time blocking of disinformation
d) Geographic spread of campaigns

Q4 – True/False
Once created, dashboard widgets cannot be edited or deleted.
True **Not True**

THANK YOU

Debunk.org
Disinformation analysis center

This project has received funding from the European Union's Horizon Europe Framework Programme under grant agreement Nº 101132494.

Saufex