MISP

INTELLIGENCE SHARING

MISP 2.5: everyday analysis

Find, create, review and use a record

CIRCL / Team MISP Project

https://www.misp-project.org/

Reference: 3 November 2026

What you will practise

- Find and interpret an existing record.
- Create an event, attributes and a structured object.
- Review context, recipients and the IDS flag.
- Inspect a correlation, add feedback and export deliberately.

Start with an authorised training instance

- Use the account and URL supplied by your trainer.
- Use only the supplied synthetic documentation values.
- Keep exercise events organisation-only and unpublished.
- Do not enable feeds, sync or external enrichment for this exercise.

Follow one synthetic report

- Team A reports `login-support.example` in a sign-in message.
- Team B has a separate report with the same domain.
- A second example supplies a domain/IP relationship.
- Keep the source, uncertainty and purpose with each record.

Use the data model to preserve meaning

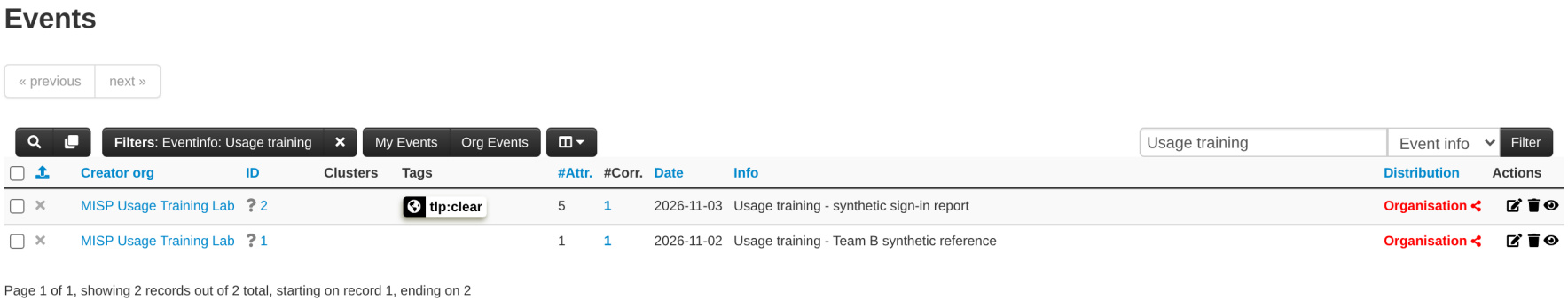
Event: a report and its context

Standalone attribute
`domain:`
`login-support.example`

Object: related attributes
`domain-ip`
`domain + ip: 192.0.2.25`

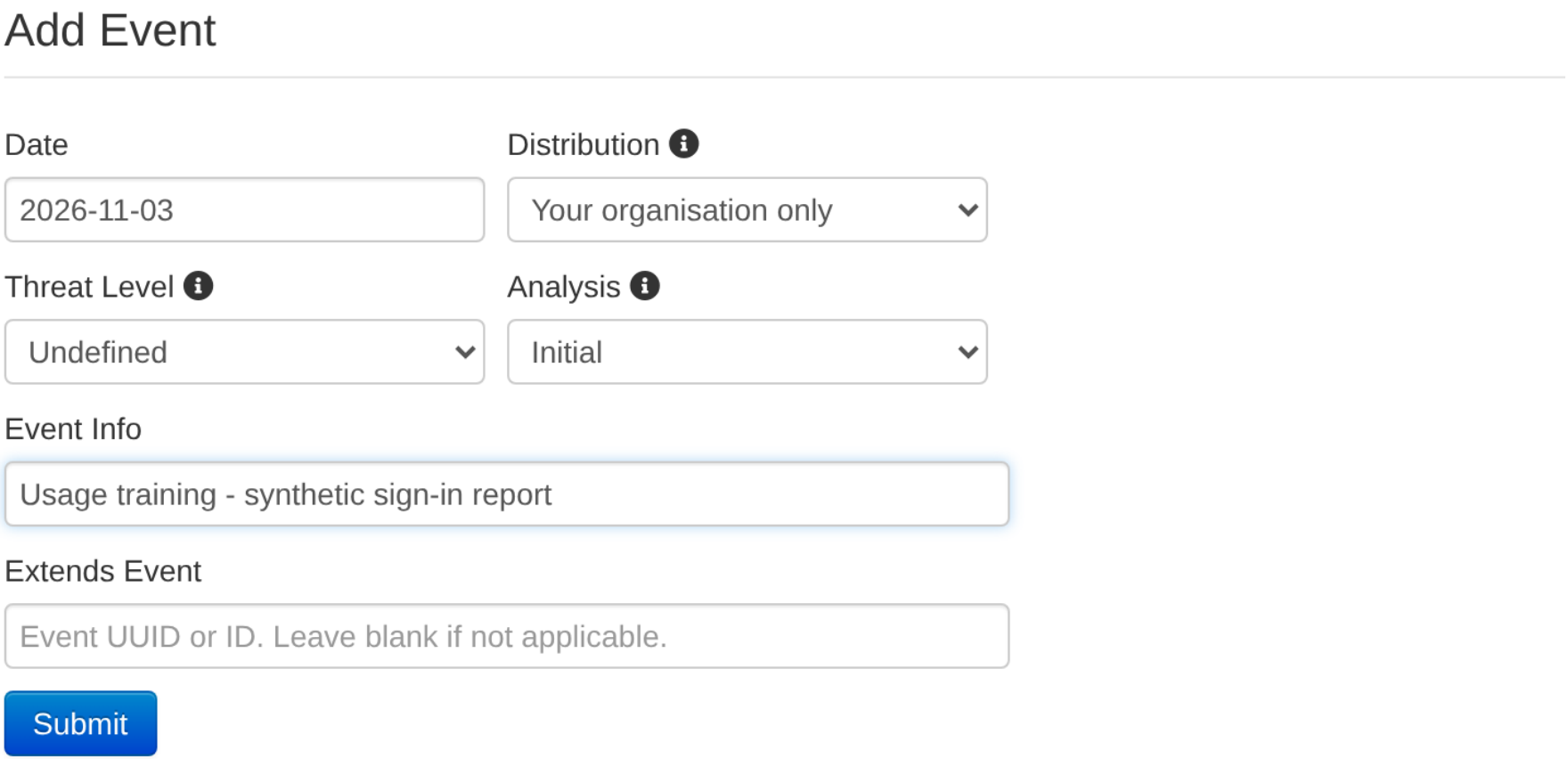
Tags and Galaxy clusters add context; sightings add observation feedback.

Find before you create



Use Event info and Filter to find the synthetic reports; check organisation, date and distribution.

Create a limited event



Add Event: set Your organisation only, a clear Event Info and the report date; then Submit.

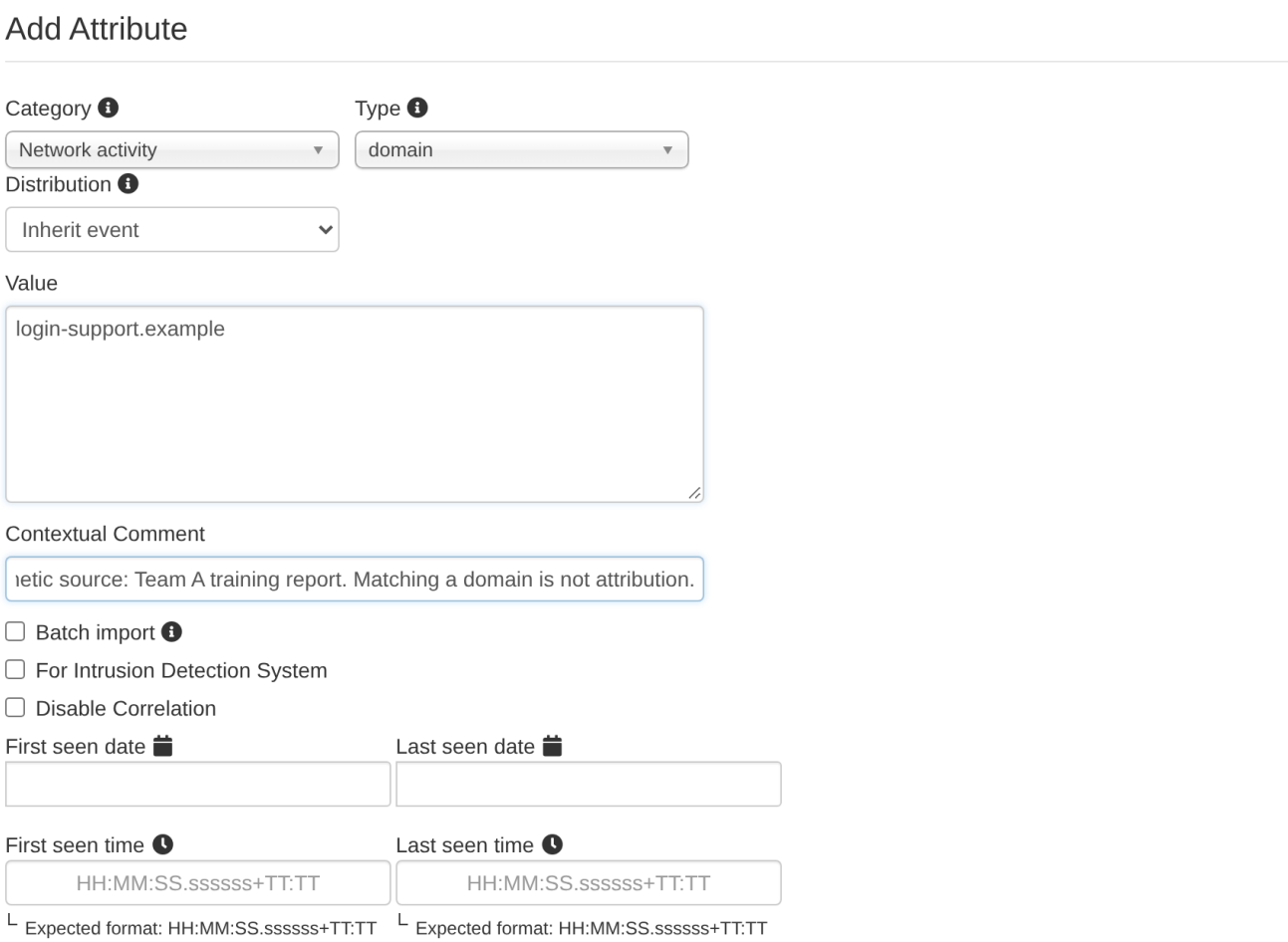
Read the saved event before adding data

Usage training - synthetic sign-in report

Event ID	2
UUID	29f99882-1d01-4f87-be38-aff4ee1f8ea1
Creator org	MISP Usage Training Lab
Creator user	analyst@example.test
Protected Event (experimental)	Event is in unprotected mode. Switch to protected mode
Tags	
Date	2026-11-03
Threat Level	Undefined
Analysis	Initial
Distribution	Your organisation only
Warnings	**Content**: Your event has neither attributes nor objects, whilst this can have legitimate reasons (such as purely creating an event with an event report or galaxy clusters), in most cases it's a sign that the event has yet to be fleshed out. **Contextualisation**: Your event has neither tags nor galaxy clusters attached - generally adding context to an event allows for quicker decision making and more accurate filtering, it is highly recommended that you label your events to the best of your ability.
Published	No

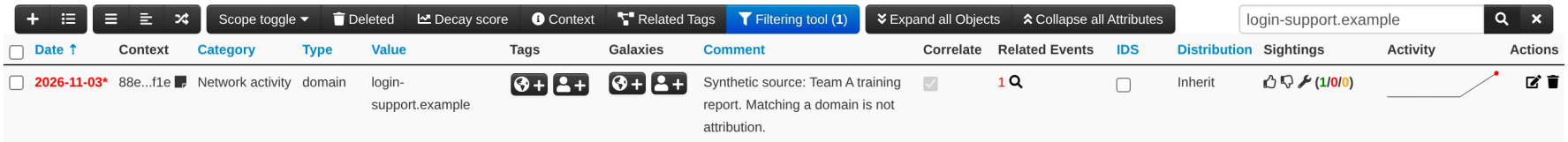
Verify the owning organisation, distribution and Published: No.
Empty-event warnings are expected at this stage.

Add a typed observation



Add Attribute: choose domain, Inherit event and a contextual comment; clear For Intrusion Detection System.

Inspect the saved attributes

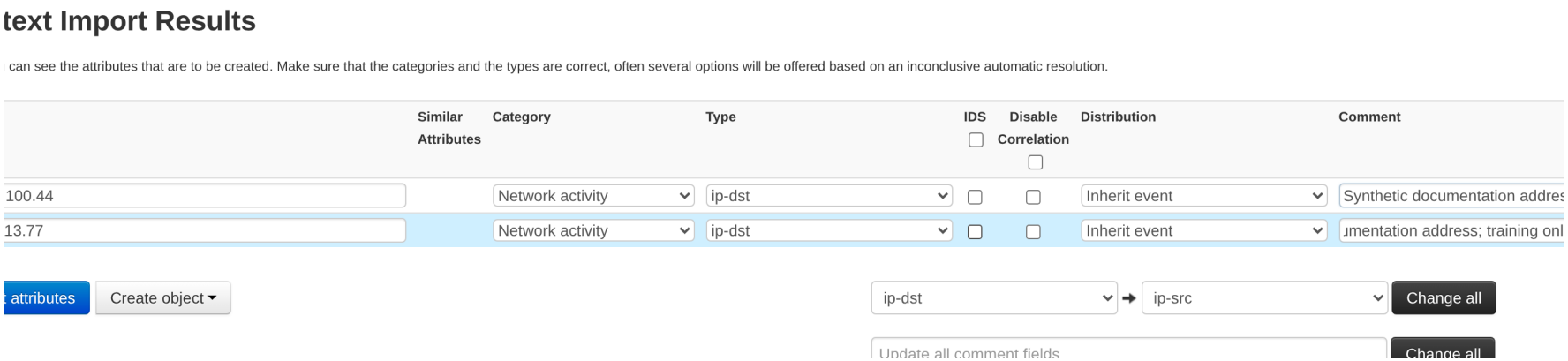


Check Type, Value, Comment, IDS, Distribution and the Related Events column after saving.

Type, category and IDS have different purposes

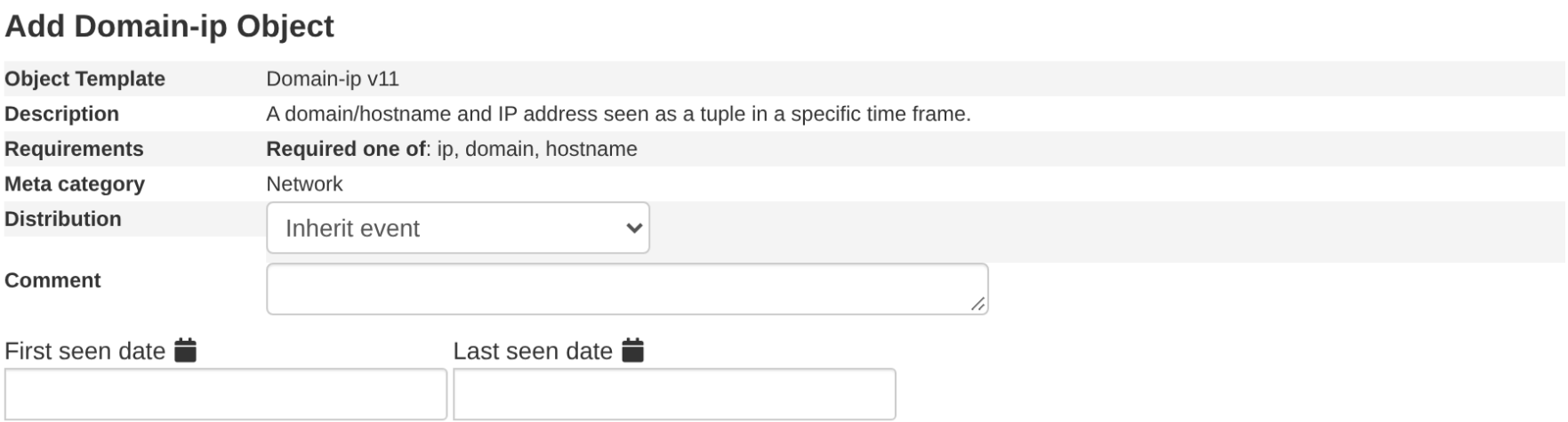
- Type defines the value representation.
- Category supplies a broad contextual classification.
- Comment and time explain the observation.
- IDS influences relevant export/filter policies; it does not prove safety.

Review free-text extraction before saving



Populate from… / Freetext import: inspect the proposed types, selection and IDS flags before import.

Choose the object template for the relationship



Review the domain-ip template version, description and requirements before entering values.

Populate a supported relationship

Object pre-save review

Make sure that the below Object reflects your expectation before submitting it.

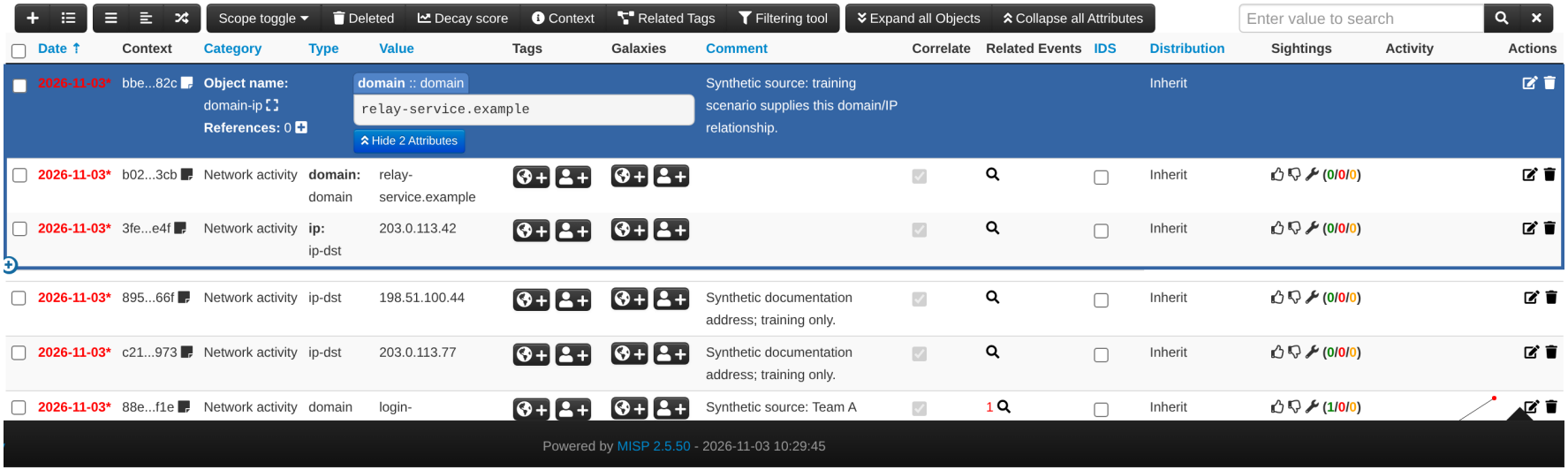
Name	domain-ip
Template version	11
Meta-category	network
Distribution	Inherit event
Comment	Synthetic source: training scenario supplies this domain/IP relationship.
First seen	
Last seen	

Object name	Category	Type	Value	To IDS	Comment	UUID	Distribution
domain	Network activity	domain	relay-service.example	No		b02a0bcb-c957-4058-b6b2-5f4d7783b3cb	Inherit event
ip	Network activity	ip-dst	203.0.113.42	No		3fee7114-8088-437d-9cf1-b0cb8eb7fe4f	Inherit event

Create new object | Back to review | Cancel

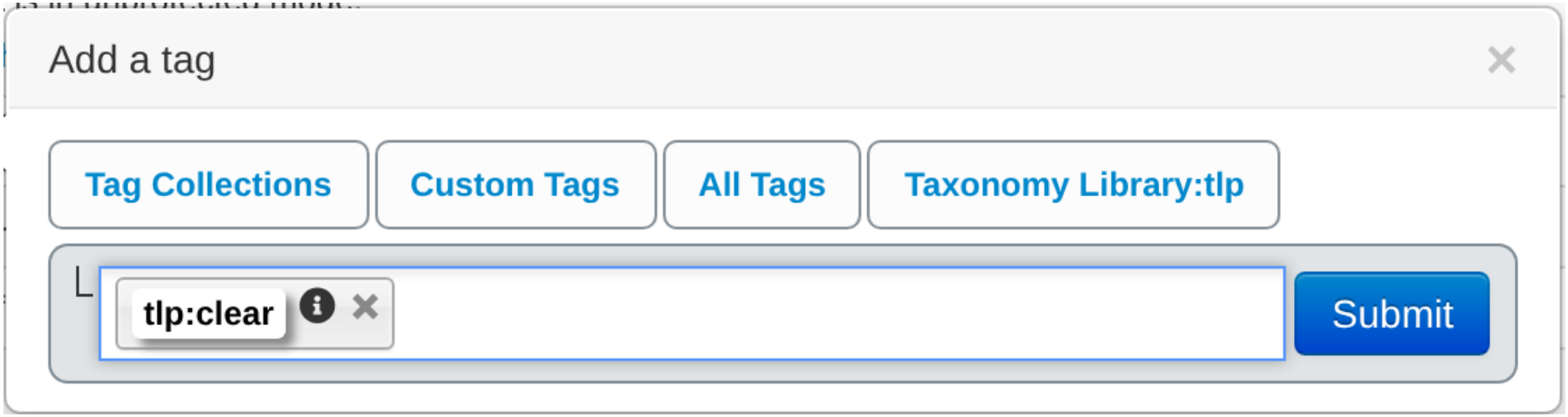
Review values, Inherit event and To IDS: No before Create new object.

Verify the saved object



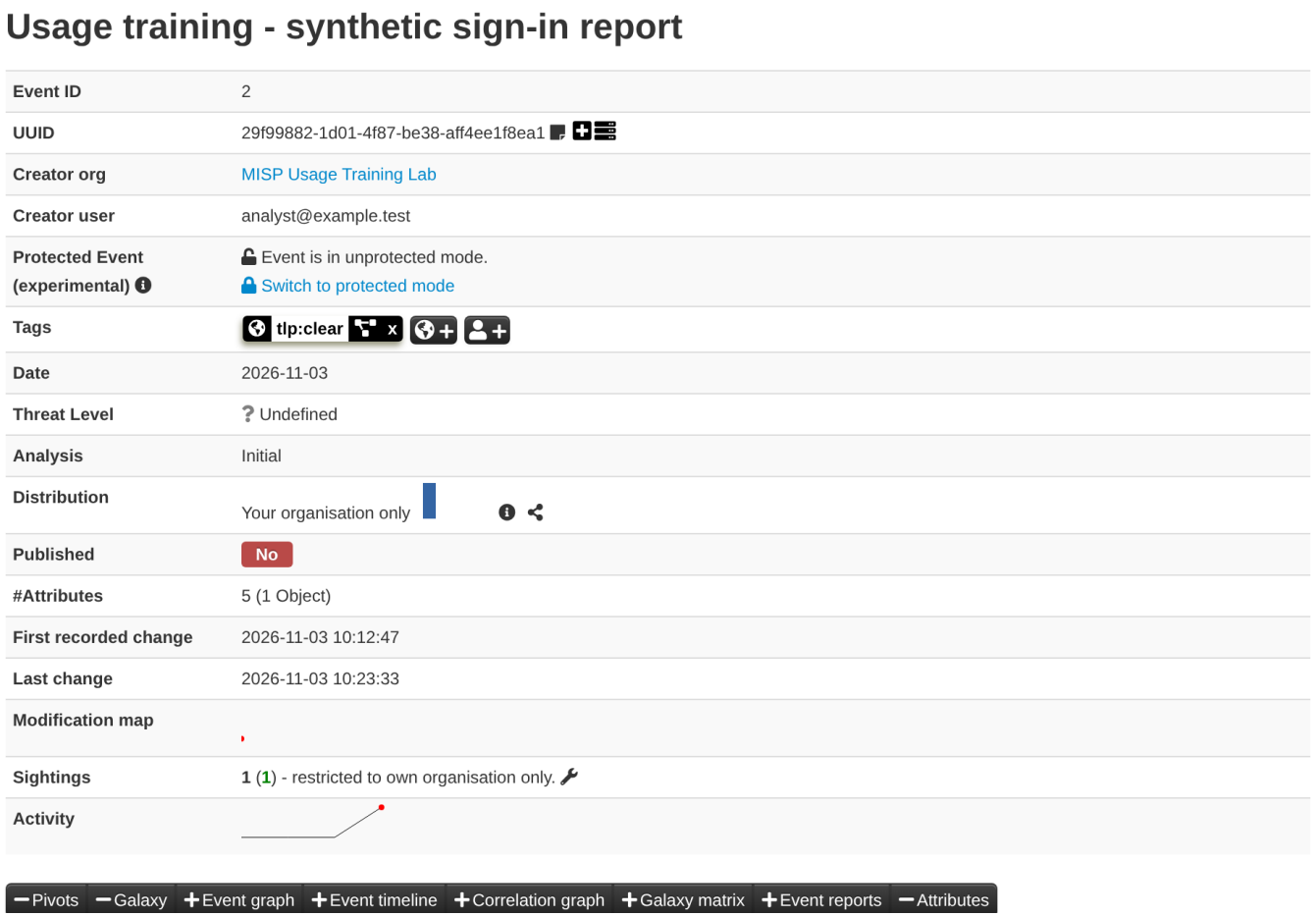
Check the object name, attribute relations and values after the final save.

Select a handling tag deliberately



Open the event Tags selector and choose the current TLP 2.0 label used by the exercise.

Verify the tag and keep visibility separate

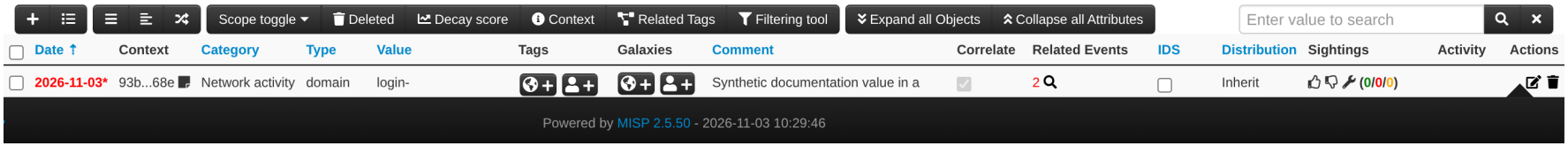


The saved tag is visible, while the event remains organisation-only and unpublished.

Use Galaxies for supported context

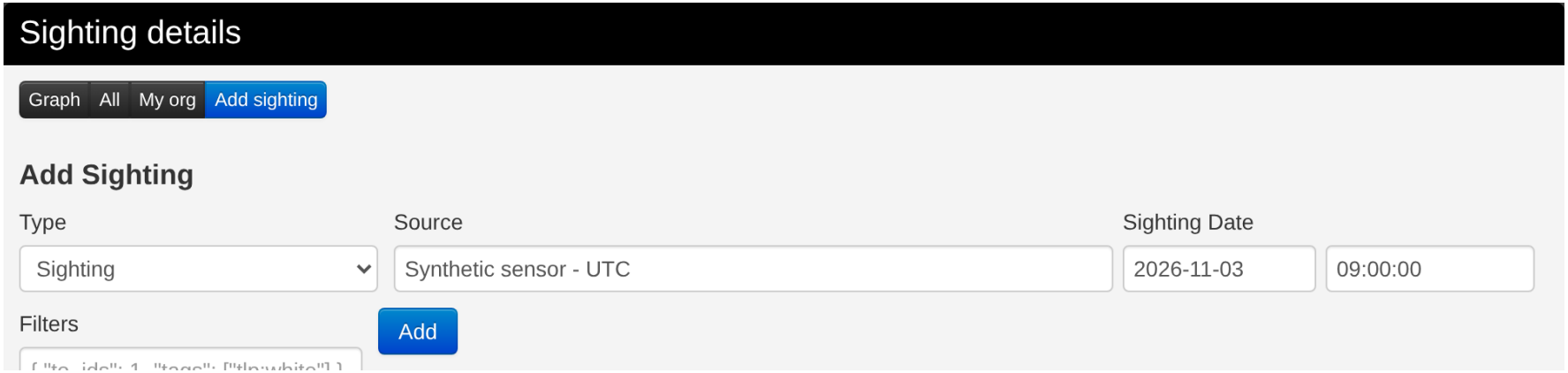
- Taxonomy tags classify the record.
- Galaxy clusters add reusable structured knowledge.
- Attach techniques, malware or actors only with supporting sources.
- Use the Galaxy course for the current selector walkthrough.

Compare the correlated report



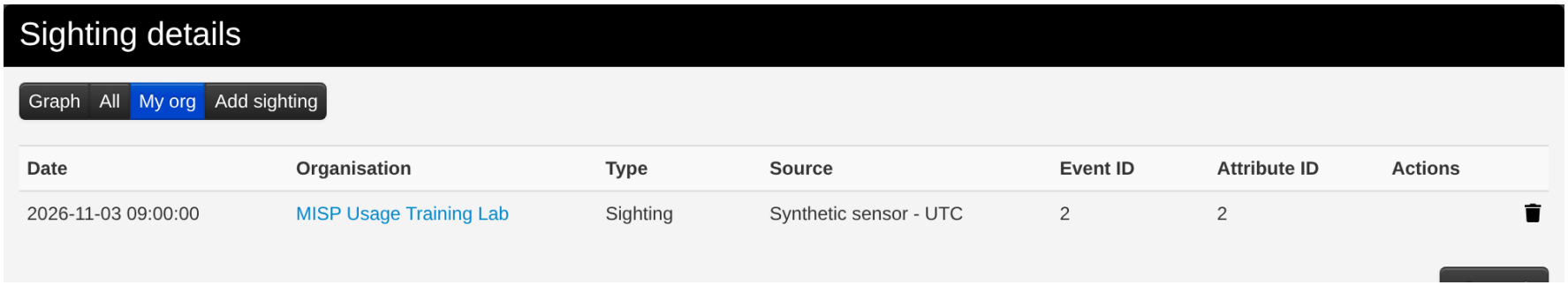
Open the related report and compare source, date and context before drawing a conclusion.

Add a sighting as explicit feedback



Choose the intended sighting type, source and observation time for the selected attribute.

Inspect the recorded feedback

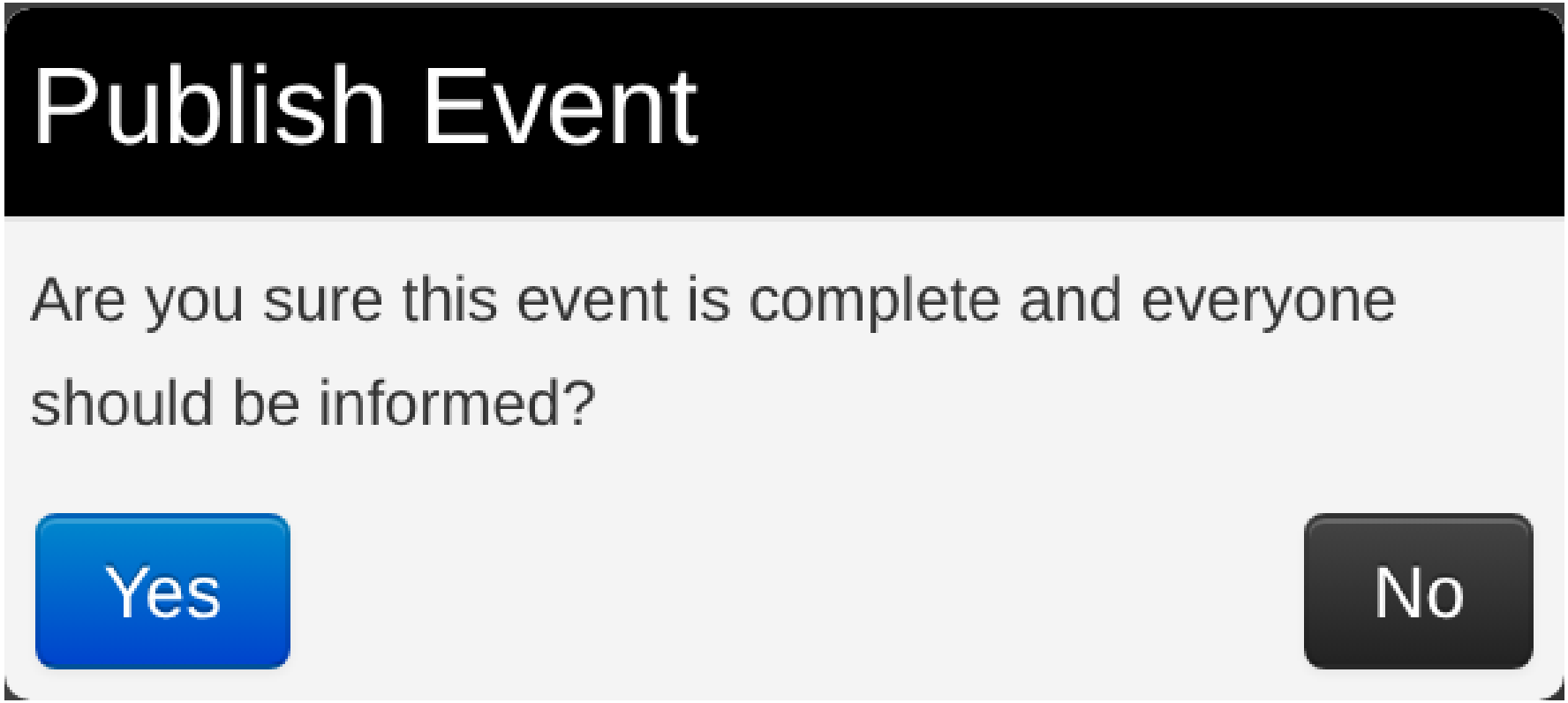


Check the saved entry under My org; a count does not prove maliciousness.

Review the audience at each level

- Event distribution sets the outer sharing context.
- Objects and attributes may inherit or impose a narrower scope.
- Sharing groups define an explicit permitted audience.
- Roles, membership and configured exchange paths also matter.

Review publication without publishing the exercise

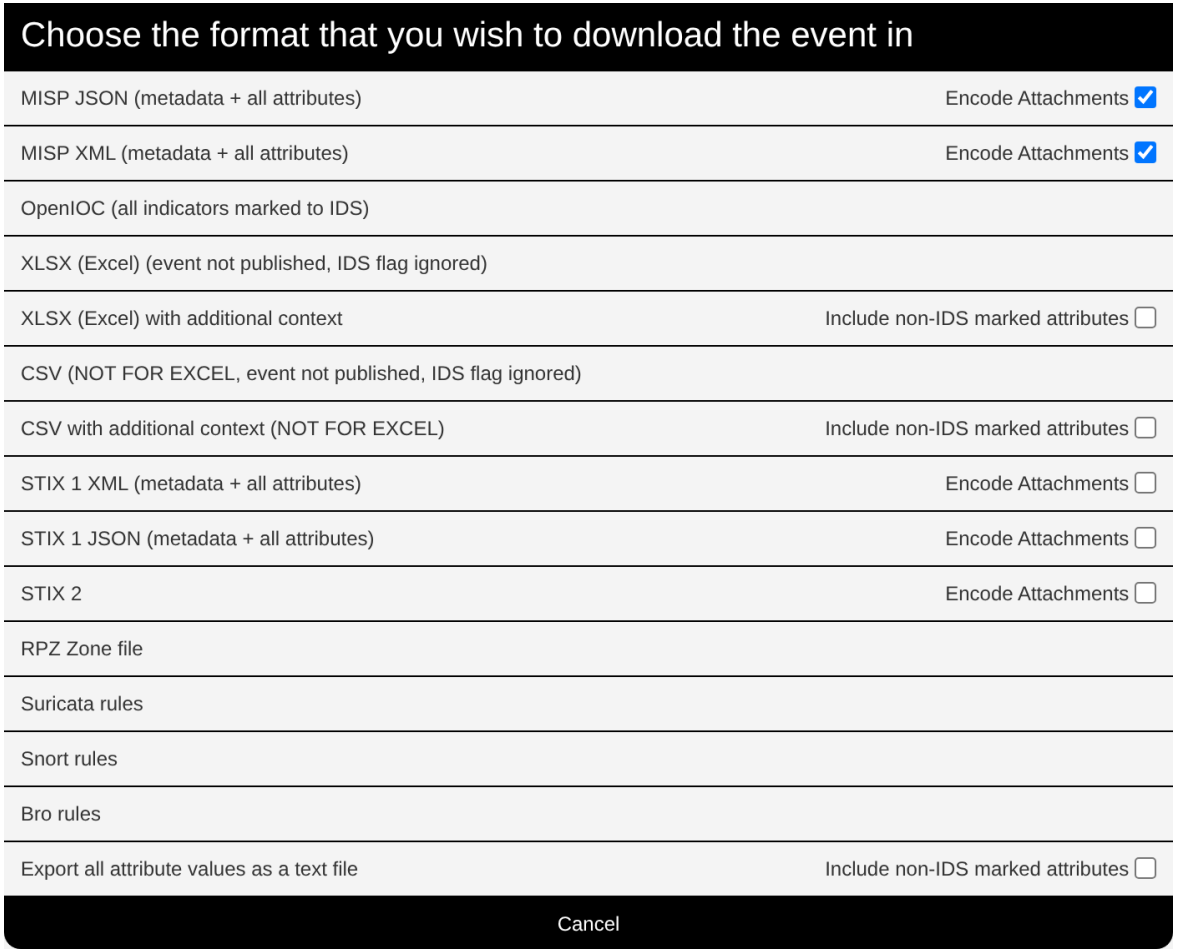


Publisher permission is required. Choose No in this lab, then verify Published: No.

Collaborate without losing ownership

- Use proposals to suggest changes to another owner's attributes.
- Use discussions or contact workflows under community policy.
- Review and accept corrections explicitly.
- Use extended events when separate ownership is useful.

Export for a defined consumer



Download as…: choose a suitable format and inspect the resulting data before using it.

Use search and APIs for the next task

- Search Attributes for values; filter events for report context.
- The REST API supports precise queries and integrations.
- PyMISP helps automate defined Python workflows.
- Keep credentials out of slides, screenshots and exported examples.

Checkpoint: build and explain the record

- Create the event with the supplied synthetic observations.
- Add the domain-ip object and the handling tag.
- Explain the match and one justified next action.
- Verify distribution, publication and every IDS flag.

Checkpoint: correct, export and hand over

- Record one synthetic sighting with source and time.
- Inspect a JSON export without publishing.
- Describe how a correction reaches the maintainer.
- Remove disposable exercise data under lab policy.

Continue with the relevant workshop

- Objects and Galaxies: richer, sourced context.
- Taxonomies and decay: classification and quality.
- REST API and PyMISP: reviewed automation.
- Administration and feeds: operate the exchange.