MISP

INTELLIGENCE SHARING

# MISP 2.5: análisis cotidiano

## Buscar, crear, revisar y utilizar un registro

CIRCL / Team MISP Project

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

Referencia: 3 de noviembre de 2026

# Qué va a practicar

- Buscar e interpretar un registro existente.
- Crear un evento, atributos y un objeto estructurado.
- Revisar contexto, destinatarios y la opción IDS.
- Examinar una correlación, aportar feedback y exportar.

# Empiece en un laboratorio autorizado

- Use la cuenta y URL proporcionadas por el formador.
- Use solo los valores sintéticos de documentación.
- Mantenga los eventos sin publicar y solo para su organización.
- No active feeds, sincronización ni enriquecimiento externo.

# Siga un informe sintético

- El equipo A registra `login-support.example` en un mensaje.
- El equipo B tiene otro informe con el mismo dominio.
- Otro ejemplo aporta una relación entre dominio e IP.
- Conserve fuente, incertidumbre y propósito con los datos.

# Conserve el significado con el modelo de datos

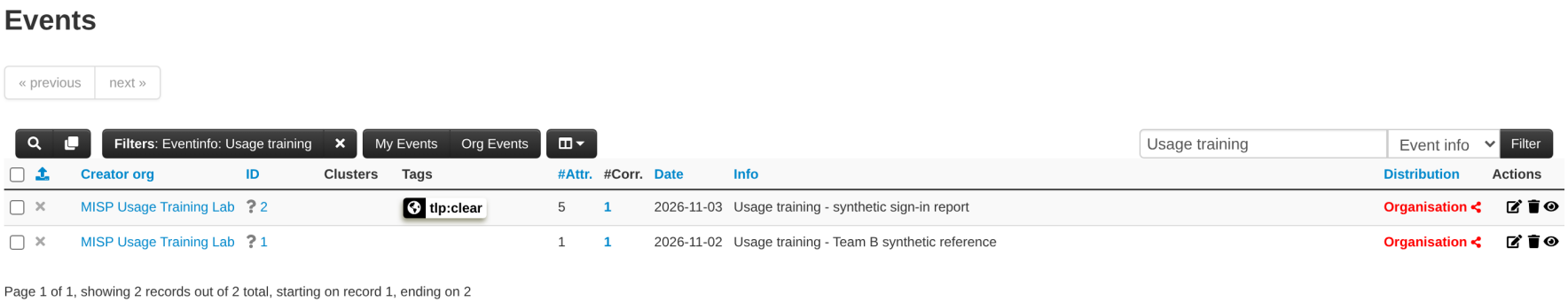
**Evento: un informe y su contexto**

**Atributo independiente**
`domain:`
`login-support.example`

**Objeto: atributos relacionados**
`domain-ip`
`domain + ip: 192.0.2.25`

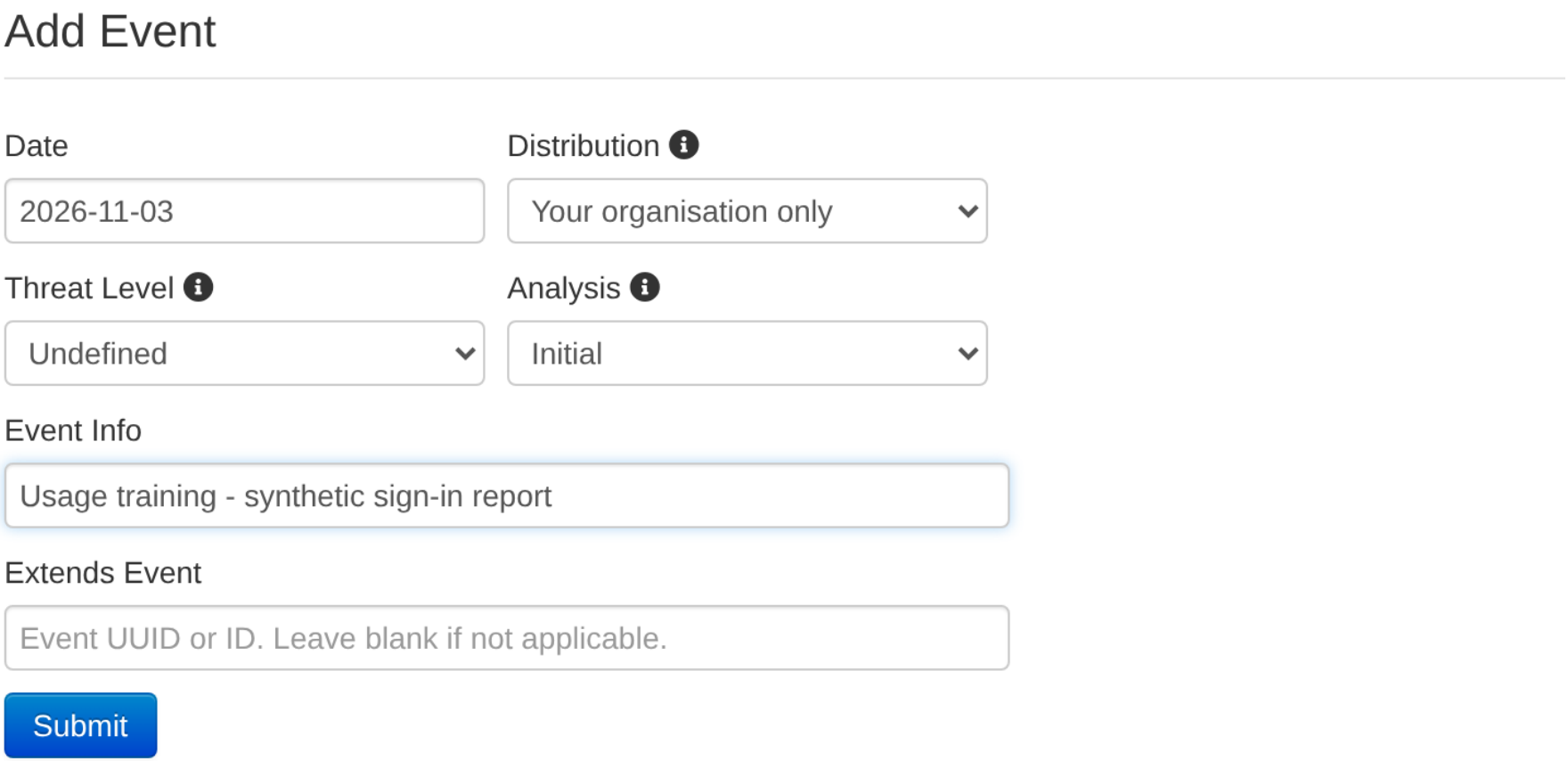
Las etiquetas y los clusters Galaxy aportan contexto; los sightings aportan observaciones.

# Busque antes de crear




Use Event info y Filter para localizar los informes; compruebe organización, fecha y distribución.

# Cree un evento con alcance limitado




Add Event: seleccione Your organisation only, una descripción clara y la fecha; después Submit.

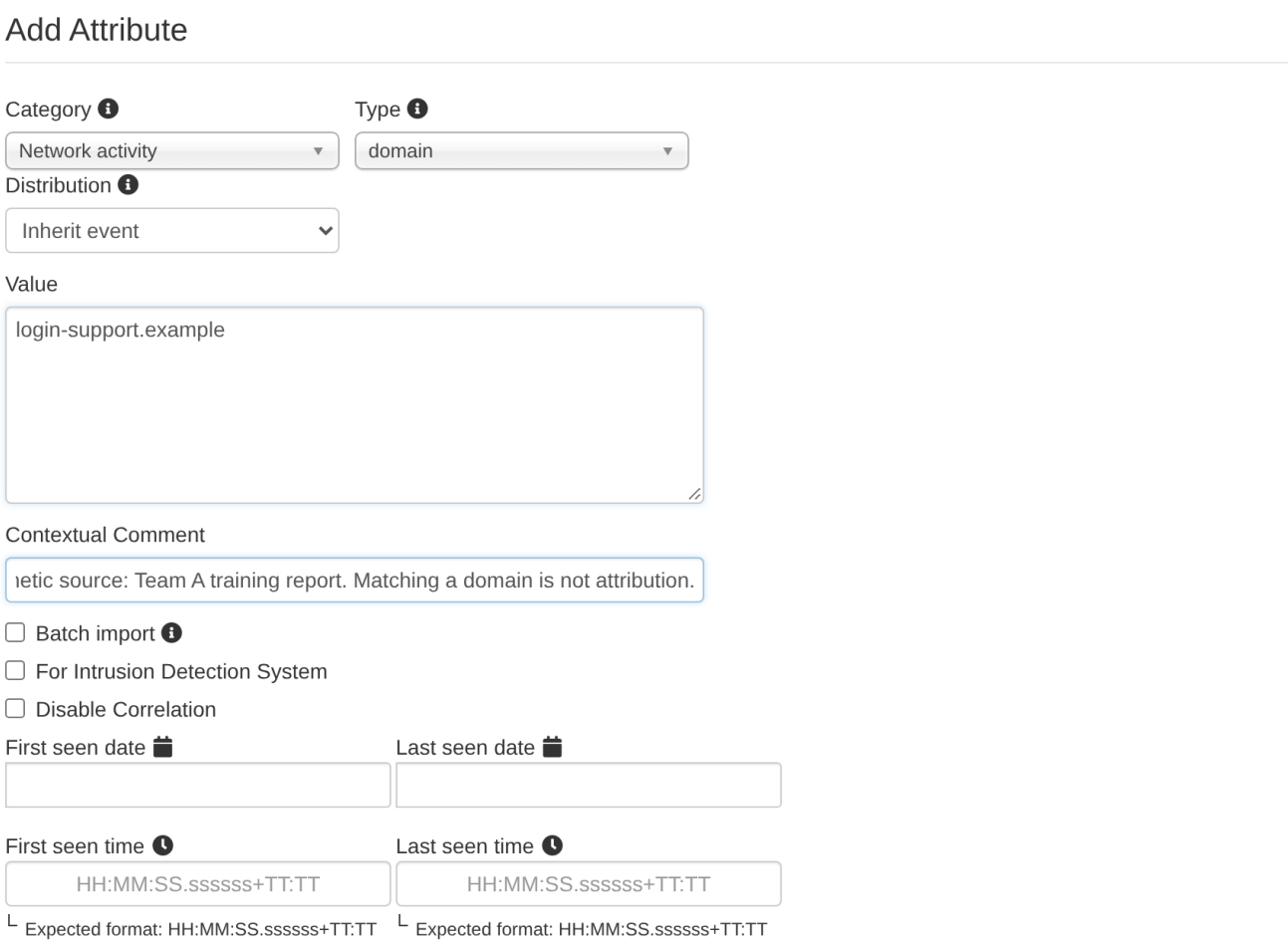
# Revise el evento guardado

## 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.<br>Switch to protected mode |
| **Tags** | |
| **Date** | 2026-11-03 |
| **Threat Level** | Undefined |
| **Analysis** | Initial |
| **Distribution** | Your organisation only |
| **Warnings** | **Content**:<br>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.<br>**Contextualisation**:<br>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 |

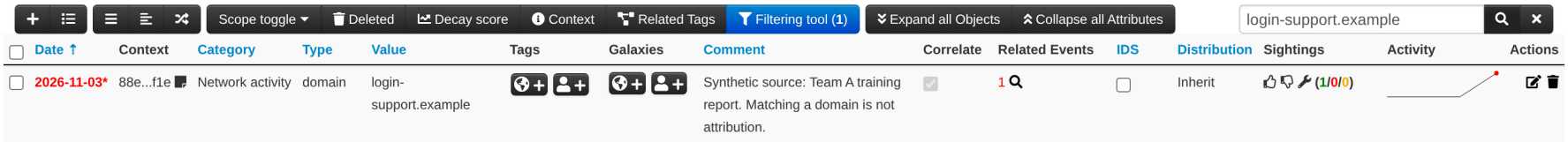
Compruebe la organización, la distribución y Published: No. Al principio se esperan avisos de evento vacío.

# Añada una observación tipada




Add Attribute: elija domain, Inherit event y un comentario; desmarque For Intrusion Detection System.

# Inspeccione los atributos guardados

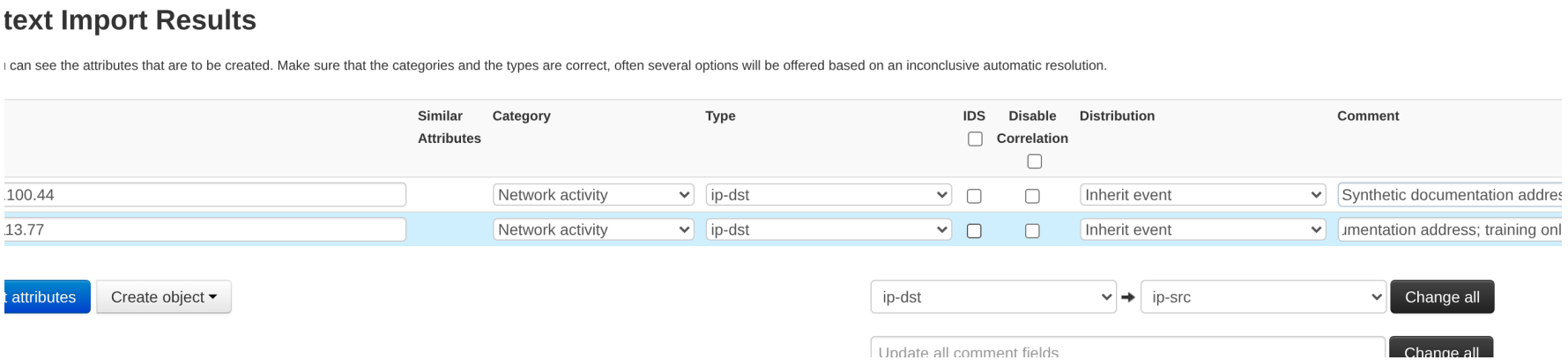



Revise Type, Value, Comment, IDS, Distribution y Related Events después de guardar.

# Tipo, categoría e IDS tienen funciones distintas

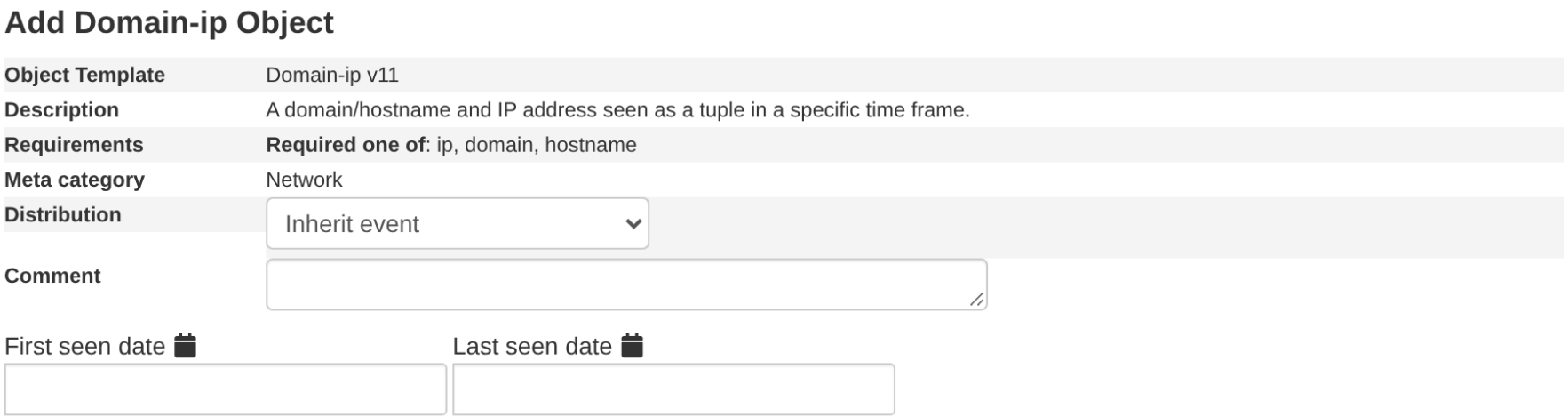
- El tipo define la representación del valor.
- La categoría proporciona una clasificación contextual amplia.
- Comentario y tiempo explican la observación.
- IDS influye en filtros y exports; no demuestra seguridad.

# Revise la extracción de texto antes de guardar




Populate from… / Freetext import: revise tipos propuestos, selección e IDS antes de importar.

# Elija la plantilla para la relación




Revise versión, descripción y requisitos de domain-ip antes de introducir valores.

# Introduzca una relación respaldada por la fuente

### Object pre-save review

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

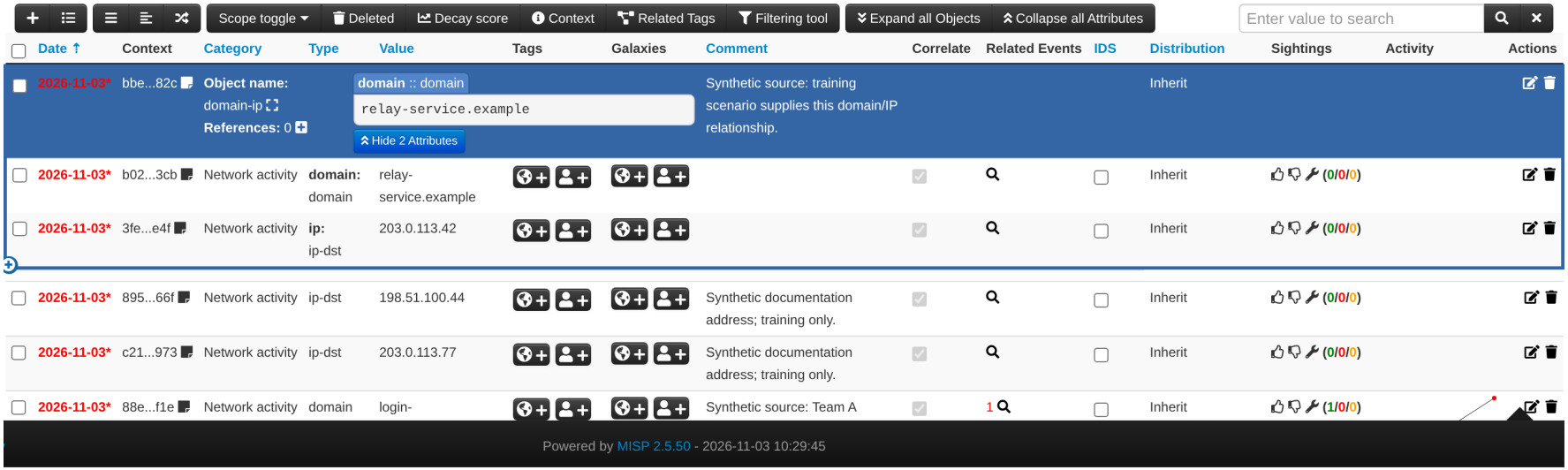
| | |
|---|---|
| **Name** | domain-ip |
| **Template version** | 11 |
| **Meta-category** | network |
| **Distribution** | Inherit event |
| **Comment** | Synthetic source: training scenario supplies this domain/IP relationship. |
| **First seen** | |
| **Last seen** | |

| 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

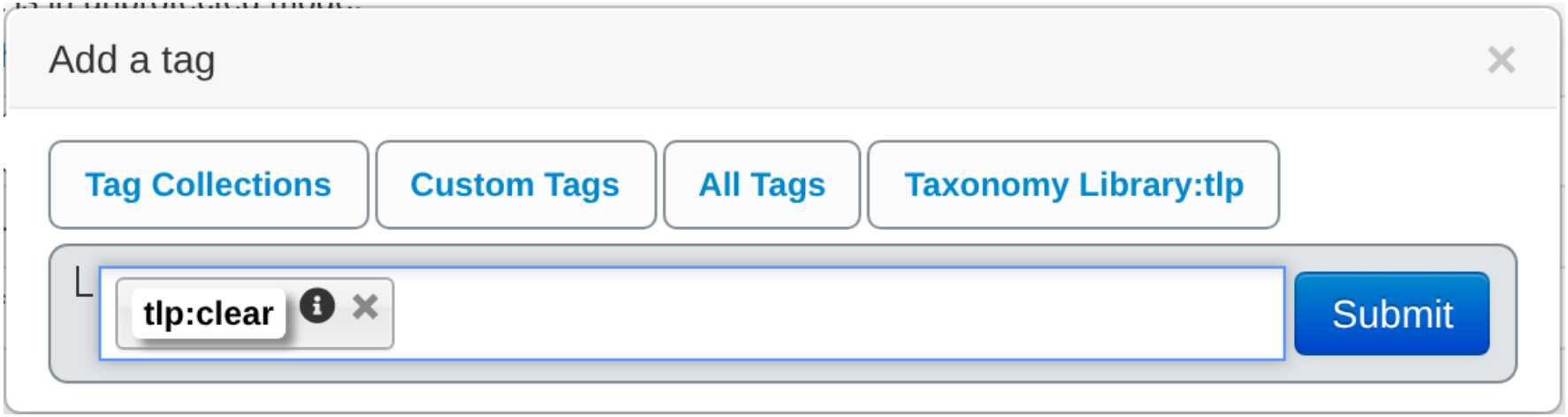
Revise valores, Inherit event y To IDS: No antes de Create new object.

# Verifique el objeto guardado



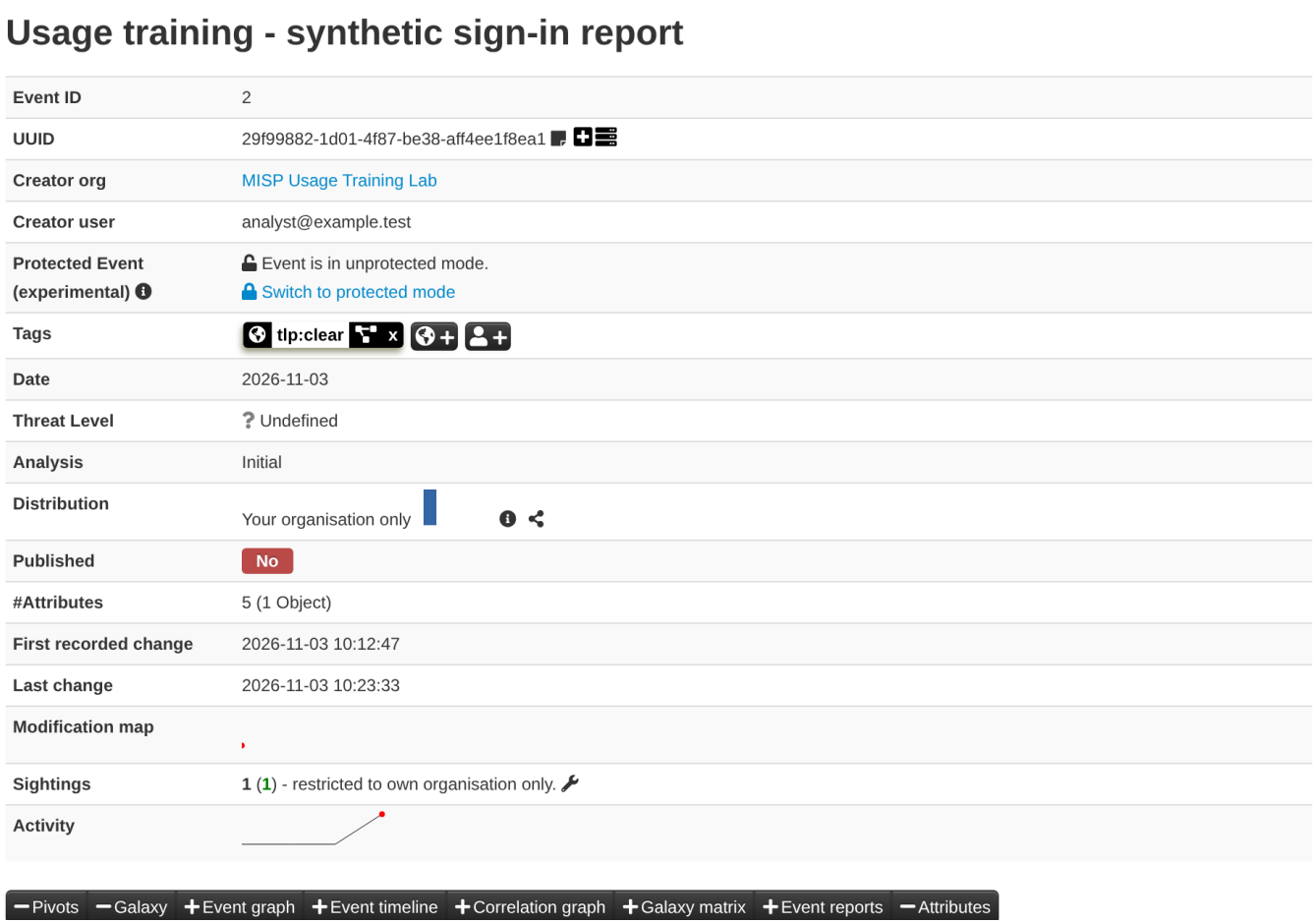

Compruebe el nombre del objeto, las relaciones de sus atributos y sus valores tras guardar.

# Seleccione una etiqueta de manejo




Abra el selector Tags del evento y elija la etiqueta TLP 2.0 del ejercicio.

# Separe la etiqueta de la visibilidad

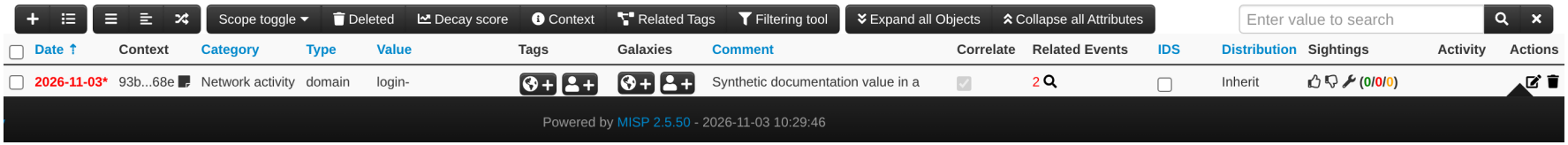



La etiqueta guardada aparece, pero el evento sigue limitado a la organización y sin publicar.

# Use Galaxies para contexto respaldado

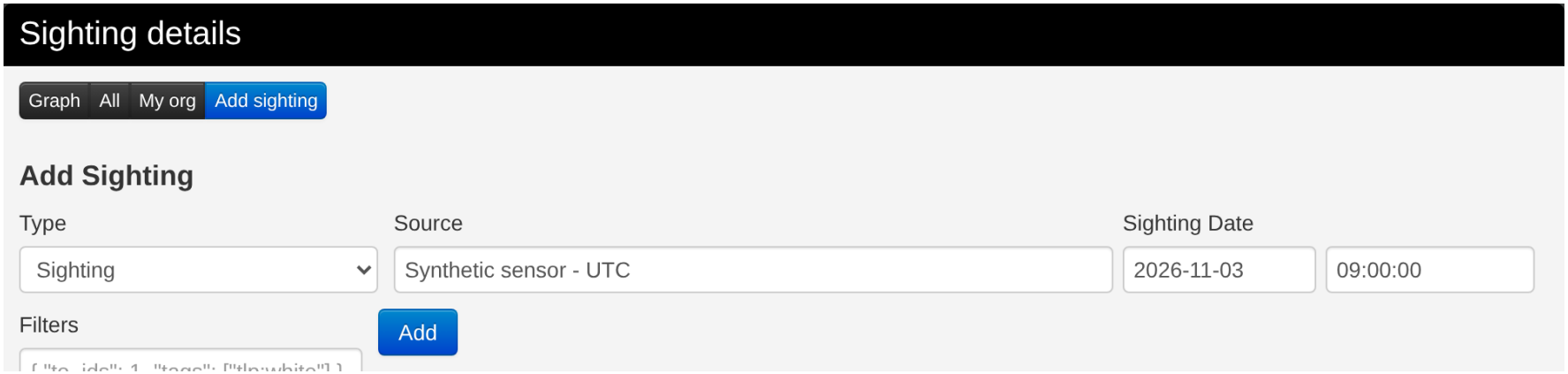
- Las etiquetas de taxonomías clasifican el registro.
- Los clusters Galaxy añaden conocimiento estructurado.
- Asocie técnicas, malware o actores solo con fuentes.
- Consulte la guía Galaxy para el selector actual.

# Compare el informe correlacionado



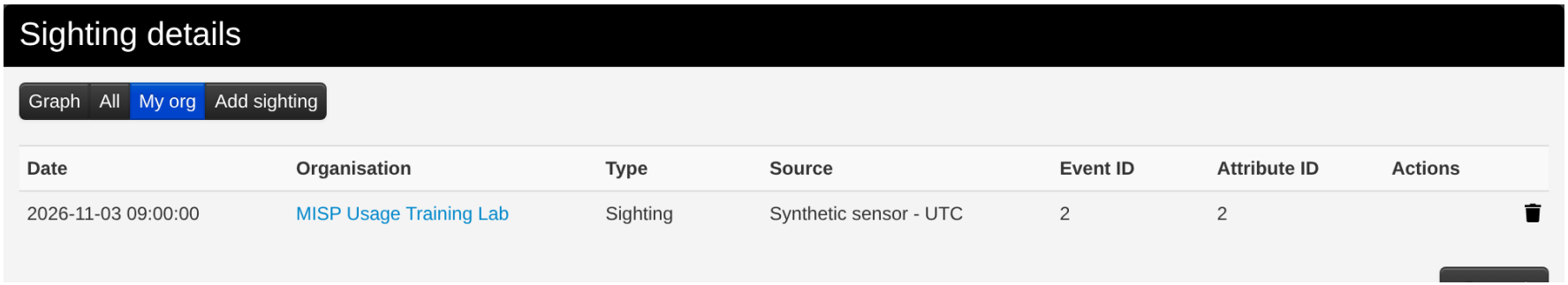

Abra el informe relacionado y compare fuente, fecha y contexto antes de concluir.

# Añada un sighting explícito




Elija tipo, fuente y hora de observación para el atributo seleccionado.

# Inspeccione el feedback registrado

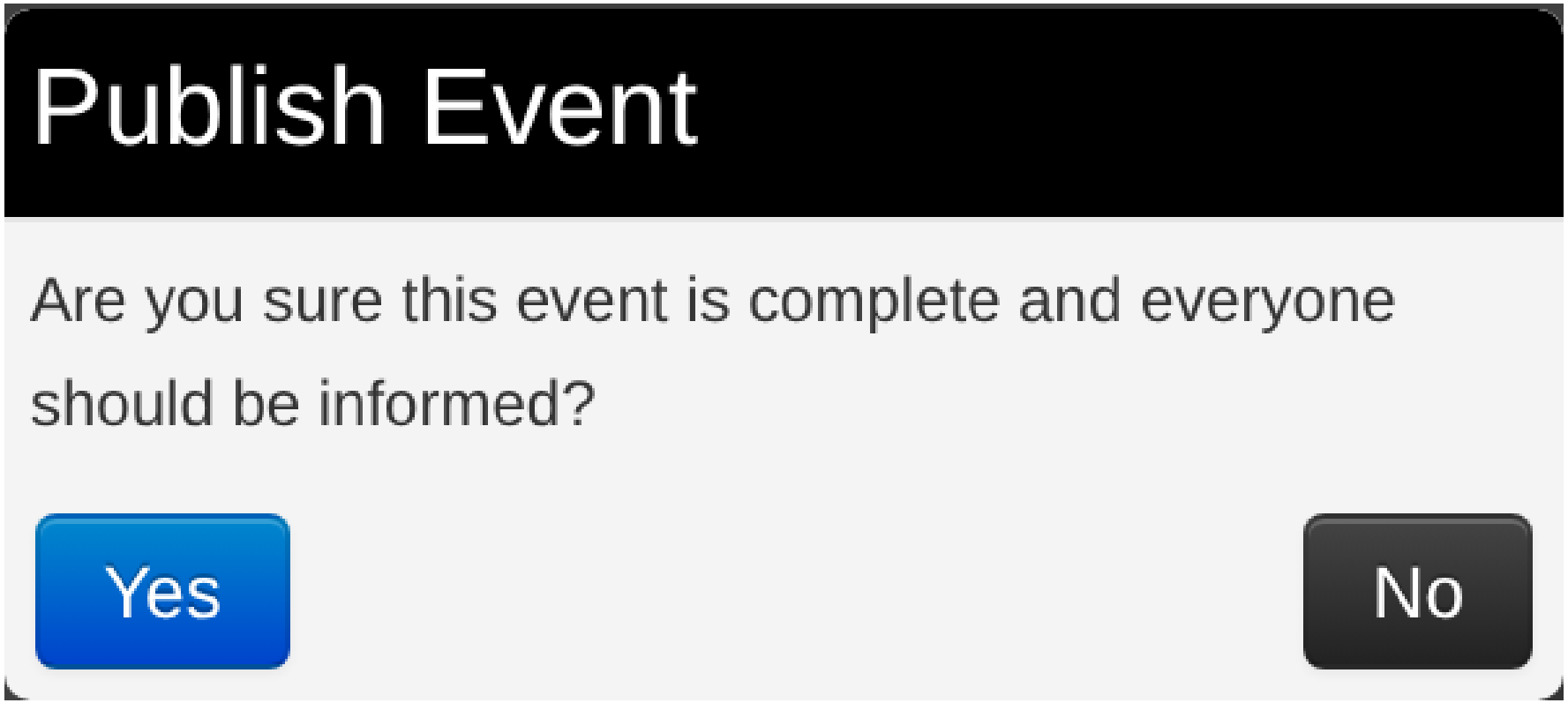



Compruebe la entrada guardada en My org; un contador no prueba malicia.

# Revise la audiencia en cada nivel

- La distribución del evento establece el contexto exterior.
- Objetos y atributos pueden heredar o limitar el alcance.
- Sharing groups definen destinatarios explícitos.
- También importan permisos, pertenencia y rutas de intercambio.

# Revise la publicación sin publicar el ejercicio

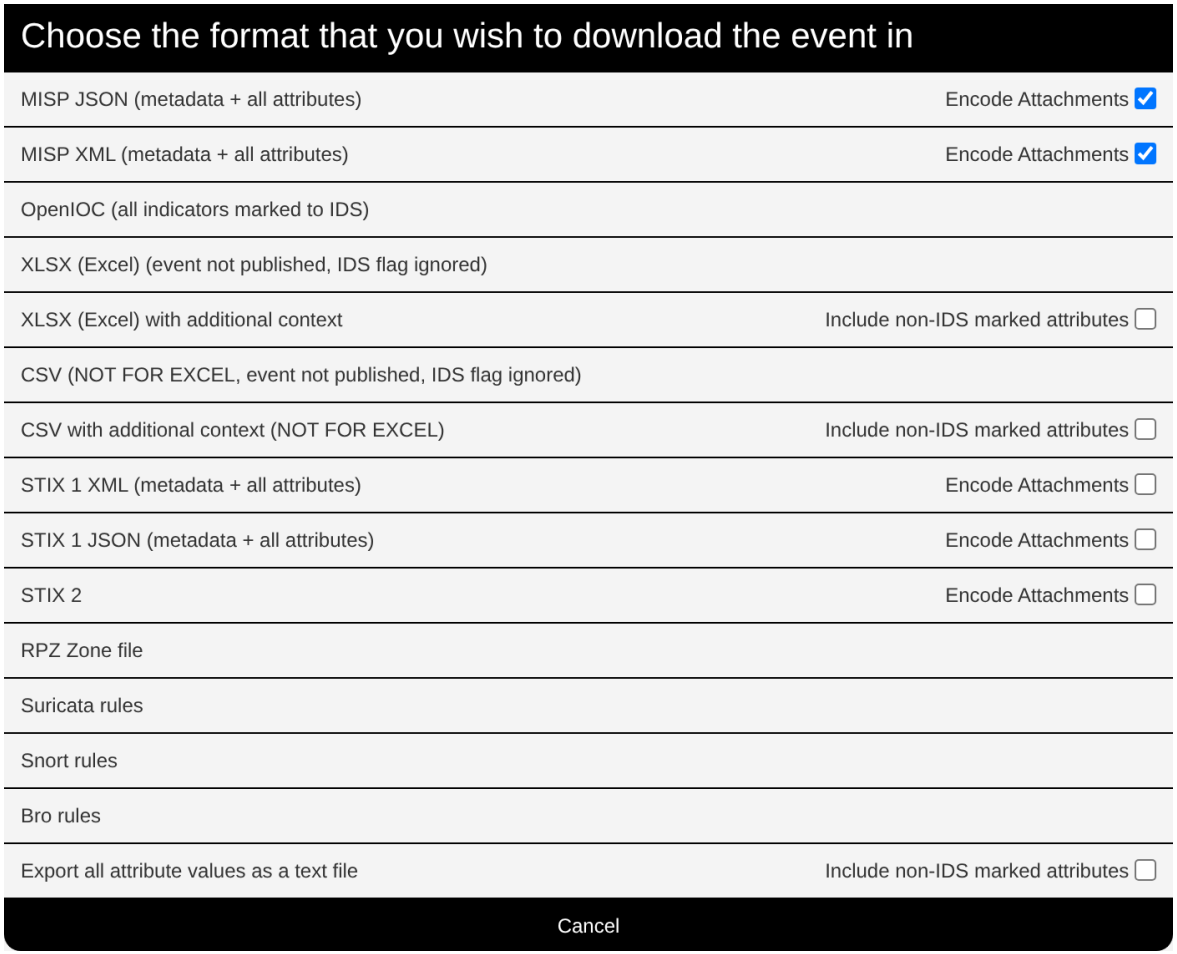



Se requiere permiso Publisher. Elija No y compruebe de nuevo Published: No.

# Colabore con responsabilidad clara

- Use proposals para sugerir cambios a otro propietario.
- Use discusiones o contacto según la política del grupo.
- Revise y acepte correcciones explícitamente.
- Use extended events cuando interese propiedad separada.

# Exporte para un consumidor definido




Download as…: seleccione el formato y revise los datos antes de utilizarlos.

# Use búsquedas y API para el siguiente paso

- Search Attributes busca valores; los filtros de eventos, contexto.
- La REST API permite consultas e integraciones precisas.
- PyMISP facilita procesos definidos en Python.
- Mantenga credenciales fuera de capturas y ejemplos.

# Práctica: cree y explique el registro

- Cree el evento con las observaciones sintéticas.
- Añada el objeto domain-ip y la etiqueta de manejo.
- Explique la coincidencia y una acción justificada.
- Verifique distribución, publicación y todos los IDS.

# Práctica: corrija, exporte y entregue

- Registre un sighting sintético con fuente y hora.
- Inspeccione un export JSON sin publicar.
- Explique cómo llega una corrección al responsable.
- Retire los datos desechables según la política del laboratorio.

# Continúe con el taller adecuado

- Objetos y Galaxies: contexto con fuentes.
- Taxonomías y decay: clasificación y calidad.
- REST API y PyMISP: automatización revisada.
- Administración y feeds: operación del intercambio.