MISP

INTELLIGENCE SHARING

MISP 2.5: dagelijks analysewerk

Een record vinden, maken, beoordelen en gebruiken

CIRCL / Team MISP Project

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

Referentie: 3 november 2026

Wat u gaat oefenen

- Een bestaand record vinden en interpreteren.
- Een event, attributen en een gestructureerd object maken.
- Context, ontvangers en de IDS-instelling beoordelen.
- Een correlatie bekijken, feedback geven en bewust exporteren.

Begin op een toegestane trainingsinstantie

- Gebruik het account en de URL van de trainer.
- Gebruik alleen de fictieve documentatiewaarden.
- Houd oefenevents ongepubliceerd en organisatie-only.
- Schakel geen feeds, sync of externe verrijking in.

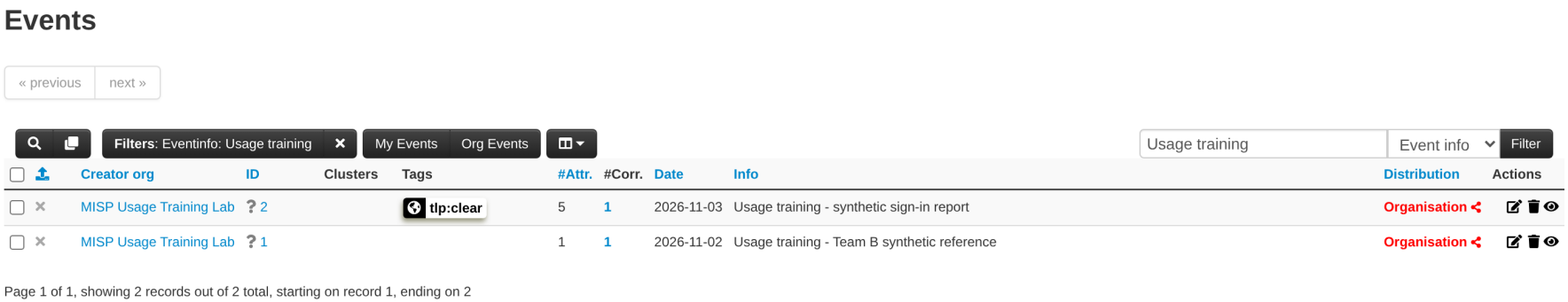
Volg één fictief rapport

- Team A registreert `login-support.example` in een bericht.
- Team B heeft een apart rapport met hetzelfde domein.
- Een tweede voorbeeld geeft een domein/IP-relatie.
- Bewaar bron, onzekerheid en doel bij elk record.

Bewaar betekenis met het gegevensmodel

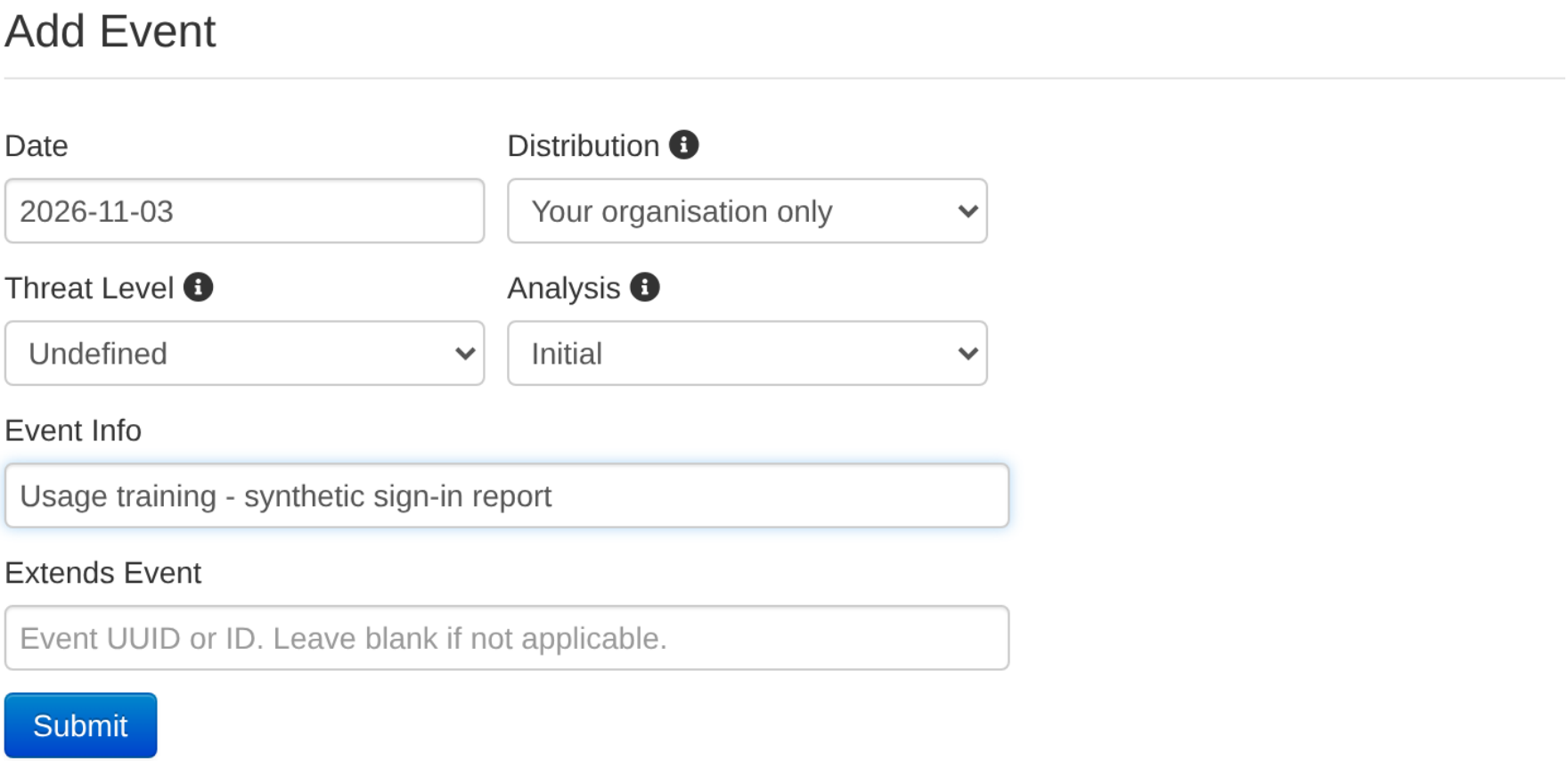
Tags en Galaxy-clusters voegen context toe; sightings geven waarnemingen terug.

Zoek voordat u iets aanmaakt



Gebruik Event info en Filter voor de fictieve rapporten; controleer organisatie, datum en distributie.

Maak een event met beperkte ontvangers



Add Event: kies Your organisation only, duidelijke Event Info en een rapportdatum; daarna Submit.

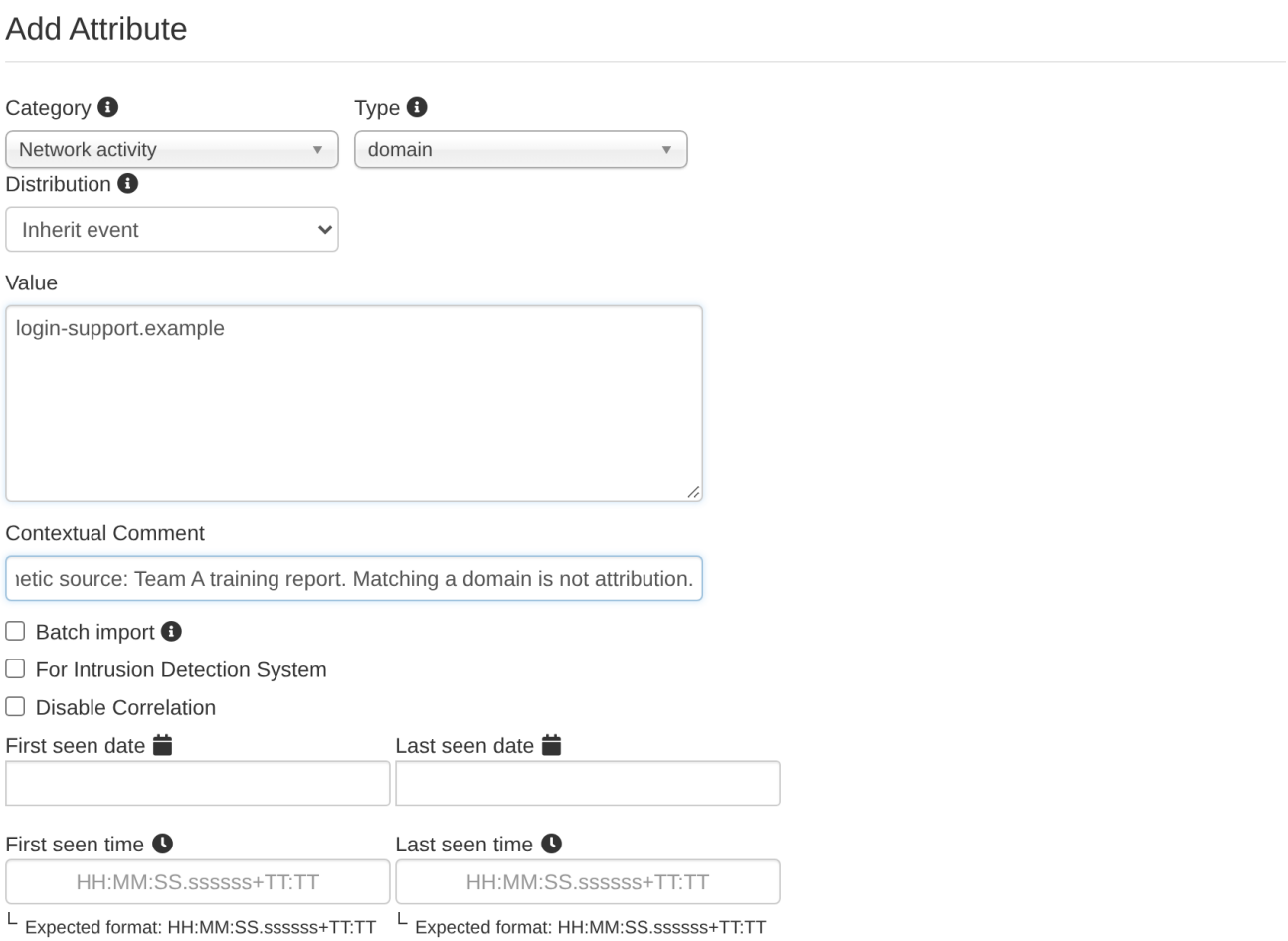
Lees het opgeslagen event

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

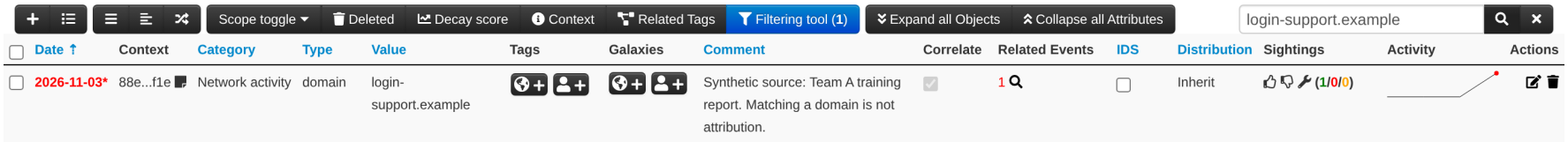
Controleer eigenaar, distributie en Published: No. Een leeg event geeft in deze fase verwachte waarschuwingen.

Voeg een getypeerde waarneming toe



Add Attribute: kies domain, Inherit event en context; vink For Intrusion Detection System uit.

Inspecteer de opgeslagen attributen

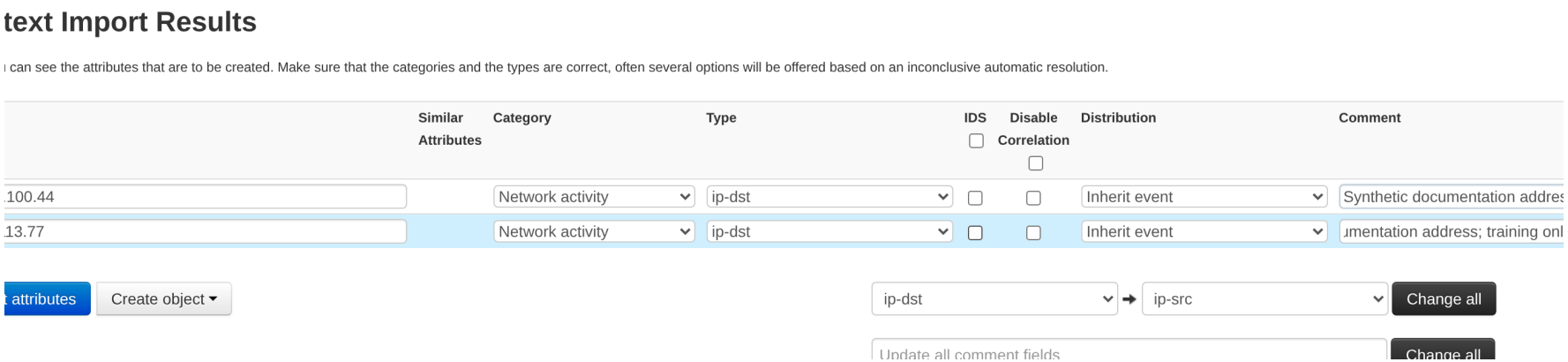


Controleer Type, Value, Comment, IDS, Distribution en Related Events na het opslaan.

Type, categorie en IDS hebben verschillende taken

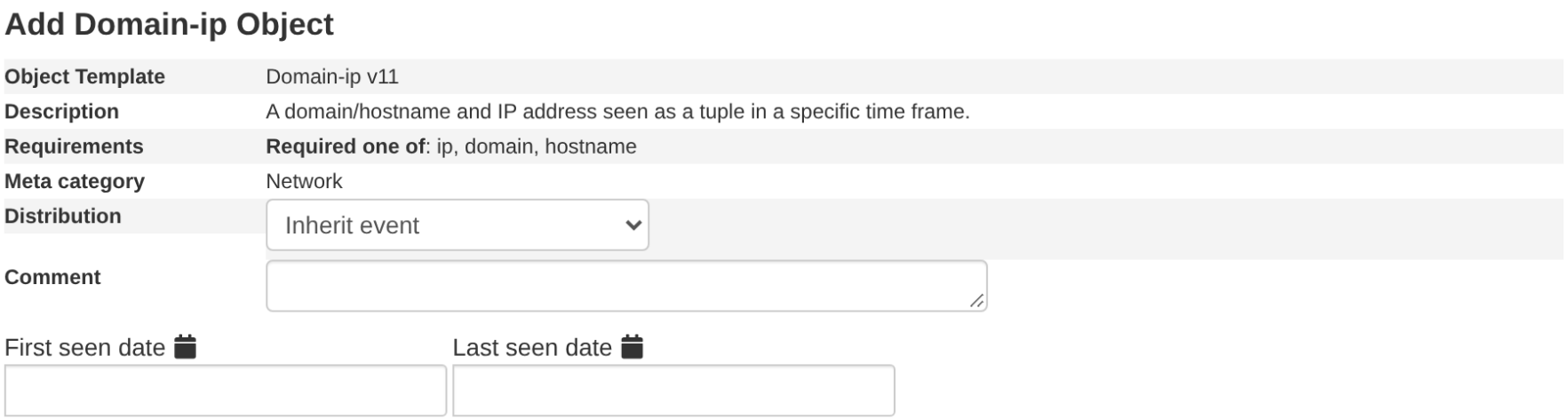
- Het type bepaalt de representatie van de waarde.
- De categorie geeft een brede contextuele indeling.
- Commentaar en tijd verklaren de waarneming.
- IDS beïnvloedt filters en exports; het bewijst geen veiligheid.

Beoordeel vrije-tekstextractie vóór opslaan



Populate from… / Freetext import: controleer typen, selectie en IDS vóór importeren.

Kies het sjabloon bij de relatie



Bekijk versie, beschrijving en voorwaarden van domain-ip vóór het invoeren.

Vul een onderbouwde relatie in

Object pre-save review

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

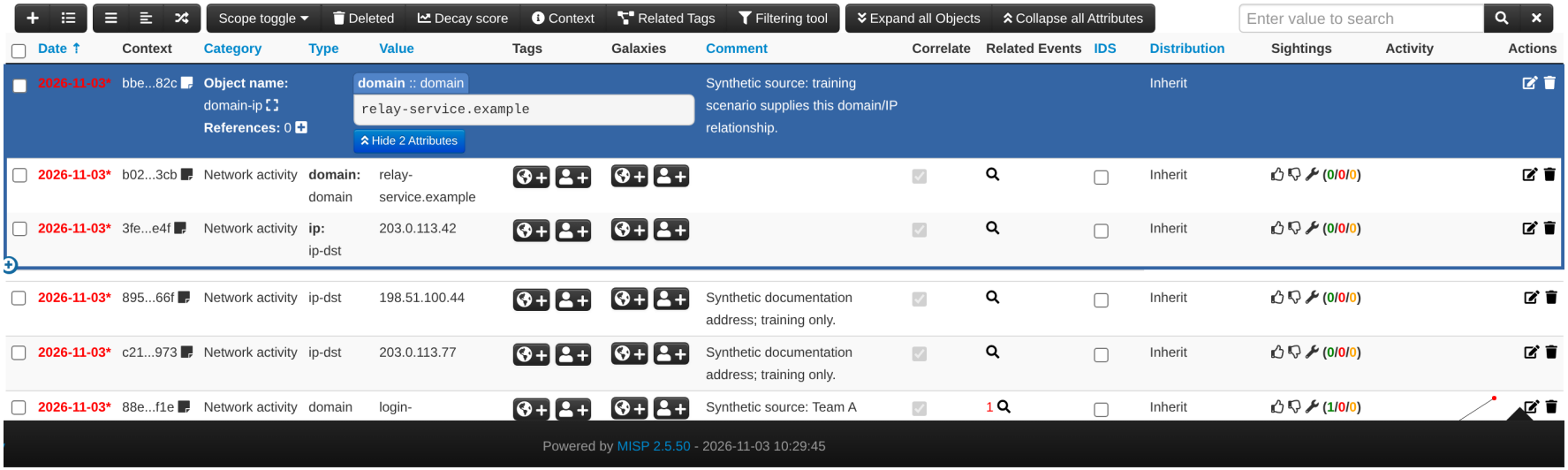
Name	domain-ip
Template version	11
Meta-category	network
Distribution	Inherit event
Comment	Synthetic source: training scenario supplies this domain/IP relationship.
First seen	
Last seen	

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

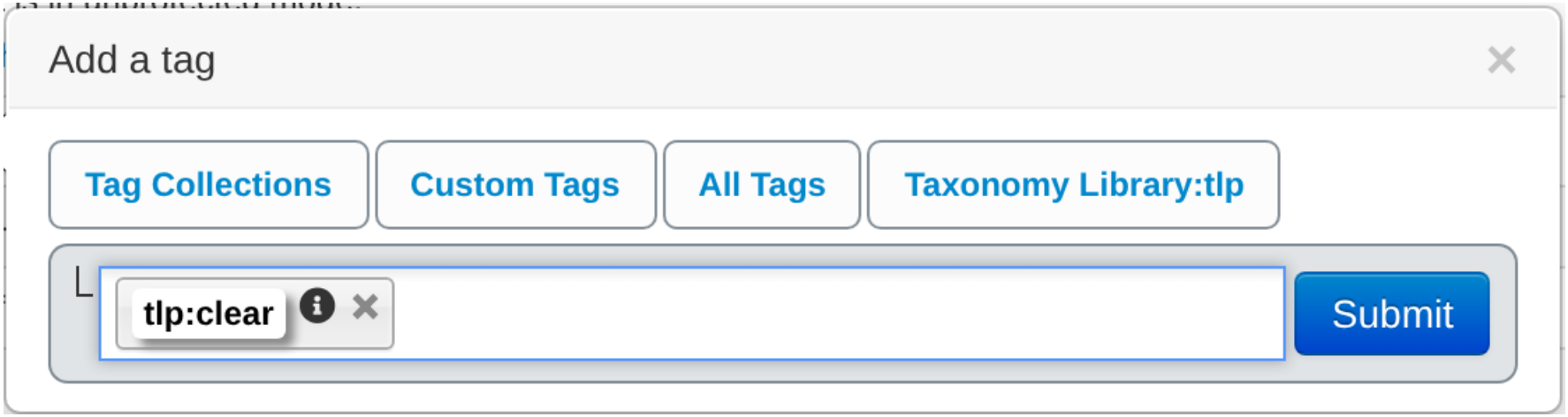
Controleer waarden, Inherit event en To IDS: No vóór Create new object.

Controleer het opgeslagen object



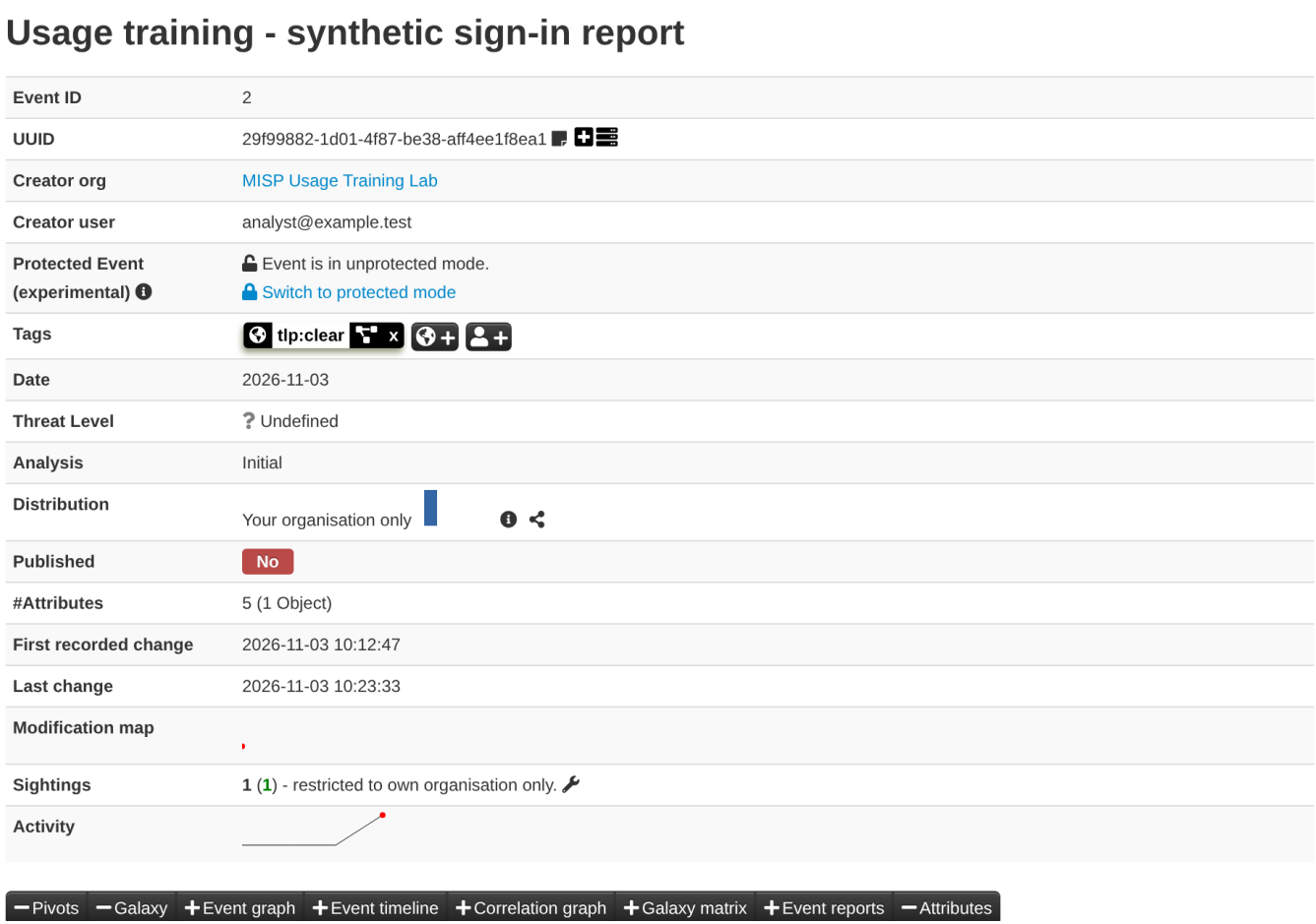
Controleer objectnaam, attribuutrelaties en waarden na de definitieve opslag.

Kies bewust een omgangstag



Open de Tags-selector van het event en kies de TLP 2.0-tag voor de oefening.

Controleer tag en zichtbaarheid afzonderlijk

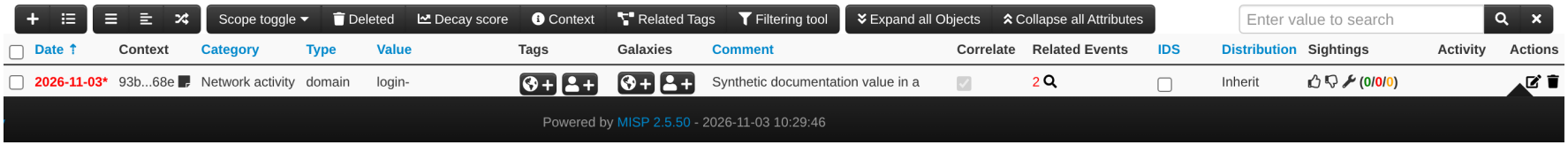


De opgeslagen tag is zichtbaar; het event blijft organisatie-only en ongepubliceerd.

Gebruik Galaxies voor onderbouwde context

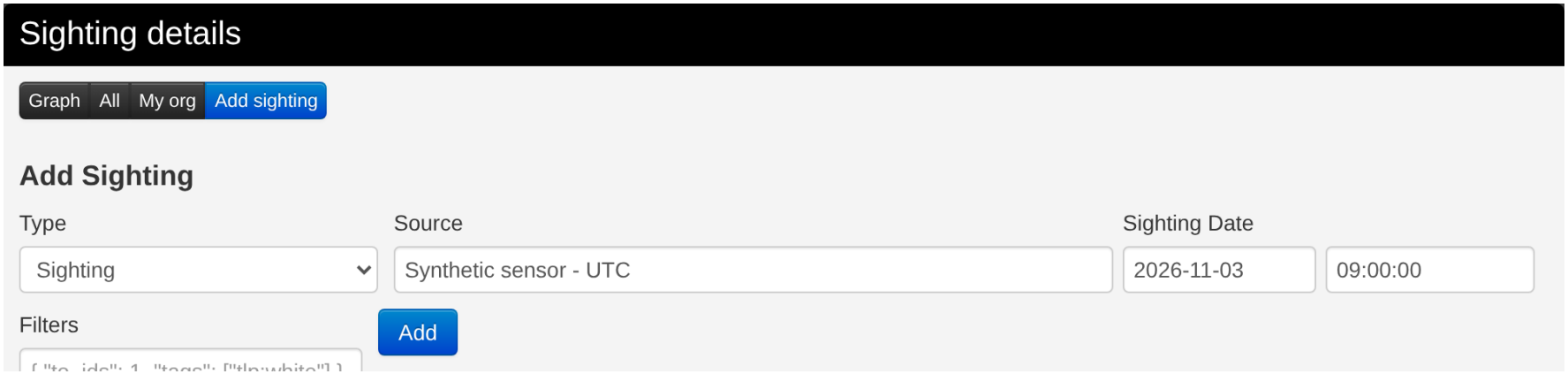
- Taxonomietags classificeren het record.
- Galaxy-clusters voegen herbruikbare kennis toe.
- Koppel technieken, malware of actoren met bronnen.
- Gebruik de Galaxy-cursus voor de actuele selector.

Vergelijk het gecorreleerde rapport



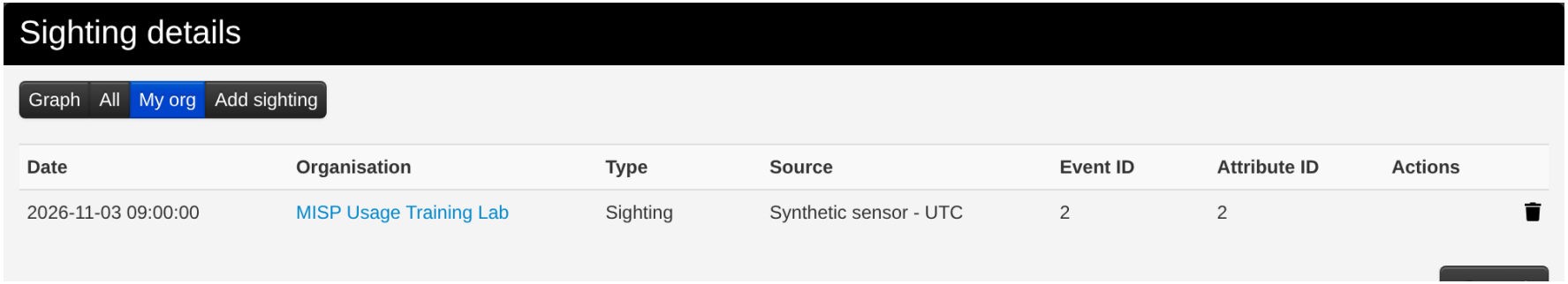
Open het verwante rapport en vergelijk bron, datum en context vóór een conclusie.

Voeg een expliciete sighting toe



Kies het bedoelde type, de bron en de waarnemingstijd voor het geselecteerde attribuut.

Bekijk de opgeslagen feedback

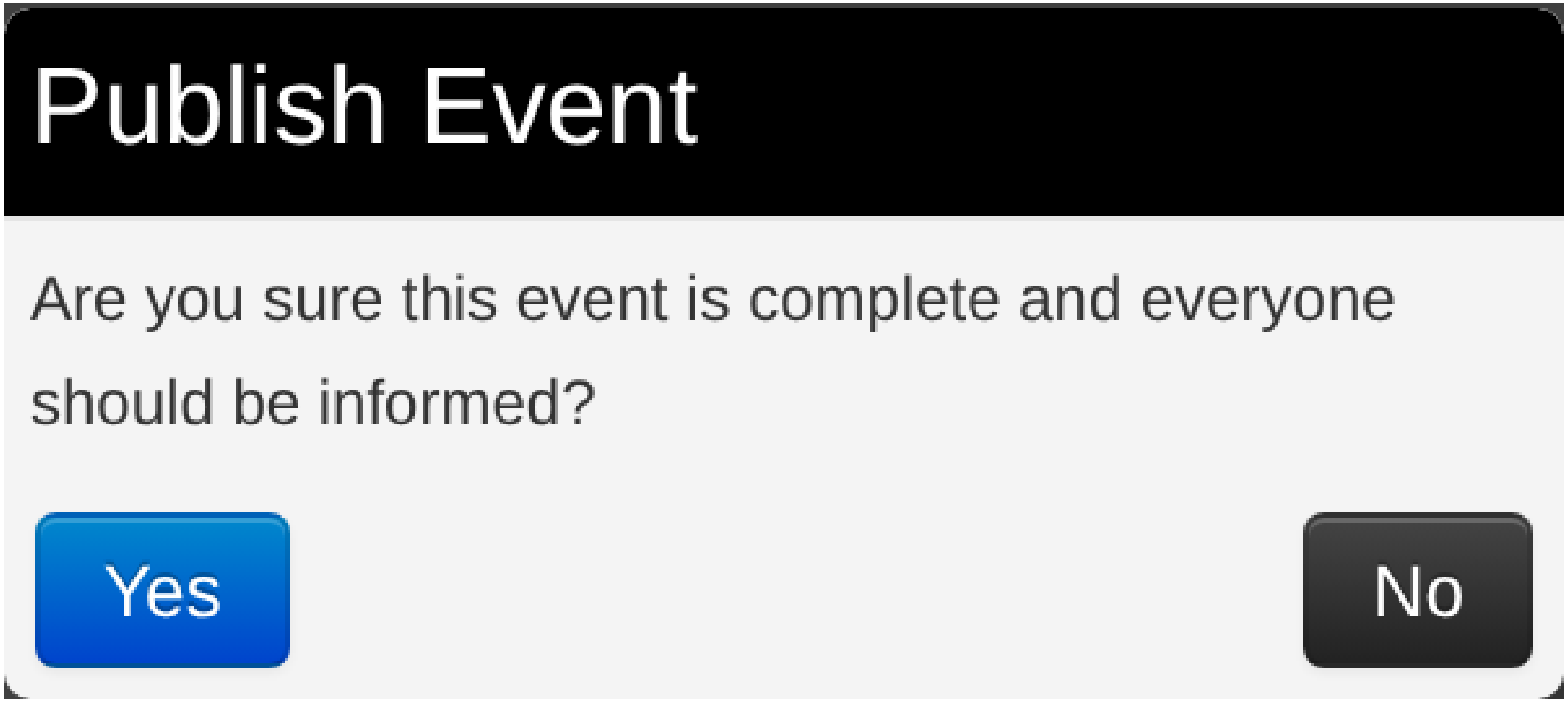


Controleer de opgeslagen sighting onder My org; een teller bewijst geen kwaadaardigheid.

Beoordeel de doelgroep op elk niveau

- Eventdistributie geeft de buitenste deelcontext.
- Objecten en attributen kunnen erven of beperken.
- Sharing groups bepalen expliciete ontvangers.
- Ook rollen, lidmaatschap en uitwisselingspaden tellen.

Beoordeel publicatie zonder te publiceren

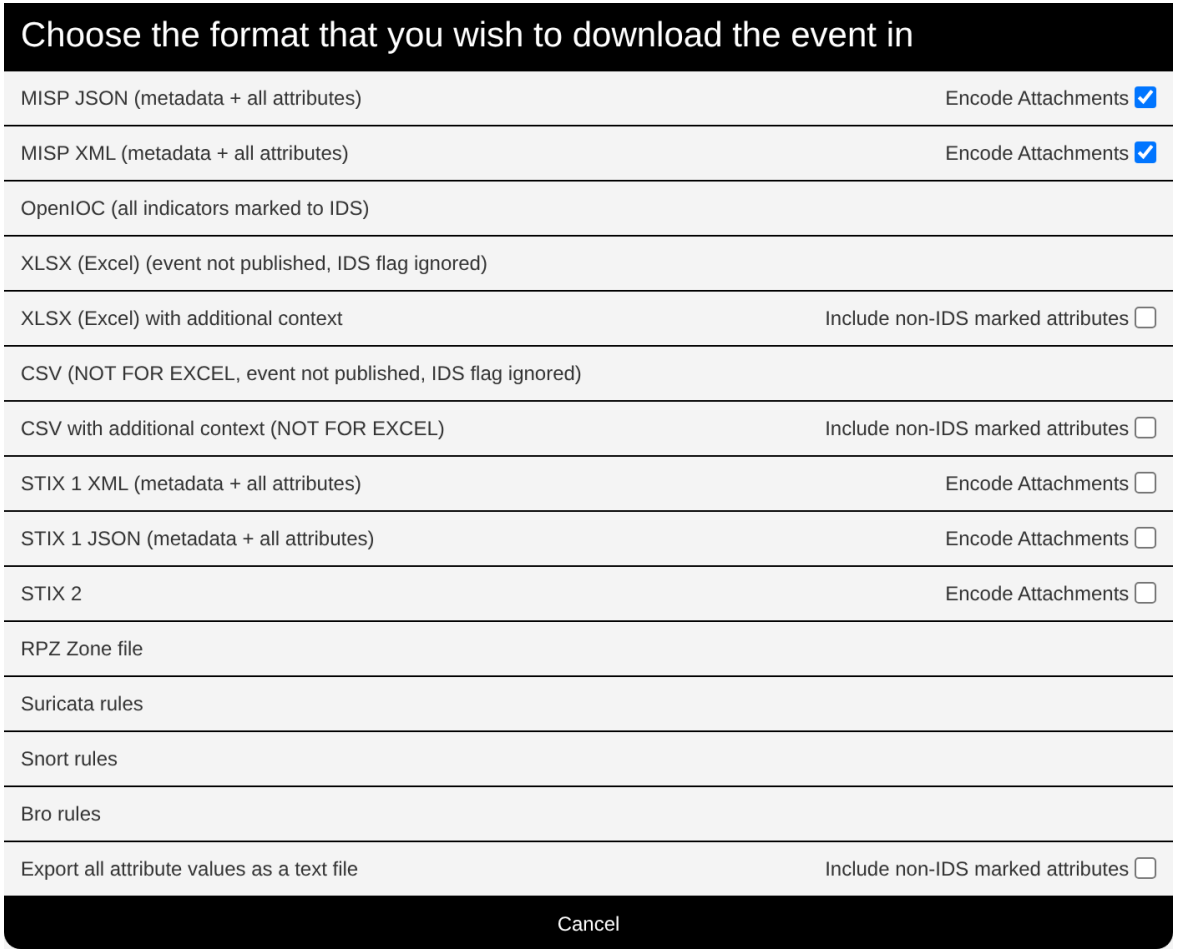


Publisher-rechten zijn nodig. Kies No en controleer daarna Published: No.

Werk samen met duidelijke verantwoordelijkheid

- Stel wijzigingen aan andermans attributen voor via proposals.
- Gebruik discussie of contact volgens gemeenschapsbeleid.
- Beoordeel en accepteer correcties expliciet.
- Gebruik extended events voor gescheiden eigenaarschap.

Exporteer voor een bepaalde afnemer



Download as…: kies het formaat en inspecteer de gegevens vóór gebruik.

Gebruik zoeken en API voor de volgende taak

- Search Attributes zoekt waarden; eventfilters zoeken context.
- De REST API ondersteunt precieze queries en integraties.
- PyMISP helpt afgebakende Python-processen automatiseren.
- Houd sleutels buiten slides, screenshots en voorbeelden.

Controlepunt: maak en verklaar het record

- Maak het event met de fictieve waarnemingen.
- Voeg het domain-ip-object en de omgangstag toe.
- Verklaar de overeenkomst en een onderbouwde actie.
- Controleer distributie, publicatie en alle IDS-instellingen.

Controlepunt: corrigeer, exporteer en draag over

- Leg één fictieve sighting met bron en tijd vast.
- Inspecteer een JSON-export zonder te publiceren.
- Beschrijf hoe een correctie de verantwoordelijke bereikt.
- Verwijder tijdelijke oefengegevens volgens het labbeleid.

Ga verder met de passende workshop

- Objecten en Galaxies: rijkere context met bronnen.
- Taxonomieën en decay: classificatie en kwaliteit.
- REST API en PyMISP: beoordeelde automatisering.
- Administratie en feeds: de uitwisseling beheren.