

StepbyStep: Adding an Incident to MISP

StepbyStep: Adding an Incident to MISP	1
The TL;DR Version	1
Add an event to MISP	2
Add tags to the event	2
Add AMITT techniques to the event	3

The TL;DR Version

- Go to MISP <https://covid-19.iglocska.eu>
 - If you don't have an account yet, sign up at <https://covid-19.iglocska.eu> and register with the organisation "covid-19".
- Add a new incident to the MISP
 - Event Actions -> Add Event
 - Set distribution = "connected communities"
 - Set threat level = undefined
 - Set event info = name of incident
 - Hit "submit"
- Next page: add details to the new incident
 - Set tags = "[current-event:pandemic="covid-19"](#)" (in global -> pandemic)
 - Set tags = "[pandemic:covid-19="disinformation"](#)" (in global -> pandemic)
 - Click inside Galaxies -> global -> misinfosec -> Misinformation pattern
 - Click on techniques you're seeing in this incident (you can add more later)
 - Scroll up, and click on "submit"
- You now see the incident listed.

With pictures:

Add an event to MISP

The screenshot shows the MISP 'Add Event' form. Red circles highlight the following elements:

- Left sidebar:** 'List Events', 'Add Event', 'Import from...', 'REST client', 'List Attributes', 'Search Attributes', 'View Proposals', 'Events with proposals', 'View delegation requests', 'Export', and 'Automation'.
- Form fields:** 'Date' (2020-04-13), 'Distribution' (Connected communities), 'Threat Level' (Undefined), 'Analysis' (Initial), 'Event Info' (paperflyer), and 'Extends Event' (Event UUID or ID. Leave blank if not applicable).
- Buttons:** 'Submit'.

Add tags to the event

The screenshot shows the MISP 'Add tags' dialog box. Red circles highlight the following elements:

- Event details:** 'Event ID' (1204), 'UUID' (5ebae5ee-5164-400d-8bd4-733b44b7dd05), 'Creator org' (covid-19), 'Date' (2020-04-16), 'Threat Level' (Undefined), 'Analysis' (Initial), and 'Distribution'.
- Tags:** 'current-event:pandemic=covid-19'.
- Dialog box:** 'Add a tag', 'Taxonomy Library:pandemic', 'pandemic:covid-19=disinformation', 'COVID-19: Disinformation', and 'Submit'.

Add AMITT techniques to the event

