

CIRCL / TEAM MISP PROJECT

[HTTP://WWW.MISP-PROJECT.ORG/](http://www.misp-project.org/)

TWITTER: @MISPPROJECT

13TH ENISA-EC3 WORKSHOP



**MISP**  
**Threat Sharing**

- Aanmeldgegevens
  - ▶ MISP admin: admin@admin.test/admin
  - ▶ SSH: misp/Password1234
- Beschikbaar op deze locatie (zowel VirtualBox als VMWare):
  - ▶ <https://www.circl.lu/misp-images/latest/>

## ■ Je moet zelf wel nog enkele aanpassingen doen

- ▶ `sudo -s`
- ▶ `cd /var/www/MISP/`
- ▶ `sudo pear install`  
`INSTALL/dependencies/Console_CommandLine/package.xml`
- ▶ `sudo pear install`  
`INSTALL/dependencies/Crypt_GPG/package.xml`
- ▶ `cd /usr/local/src/misp-modules`
- ▶ `pip3 install -r REQUIREMENTS`
- ▶ `pip3 install .`
- ▶ `reboot`

## De planning voor deze training

- Het data model
- Bekijken van gegevens
- Aanmaken van gegevens
- Verschillende vormen van samenwerking
- Verdelen van informatie
- Exporteren van gegevens

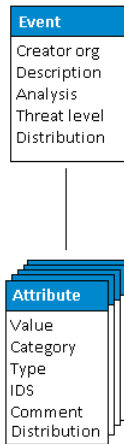
# MISP - EVENT

## (DE BASIS BOUWSTEEN VAN MISP)

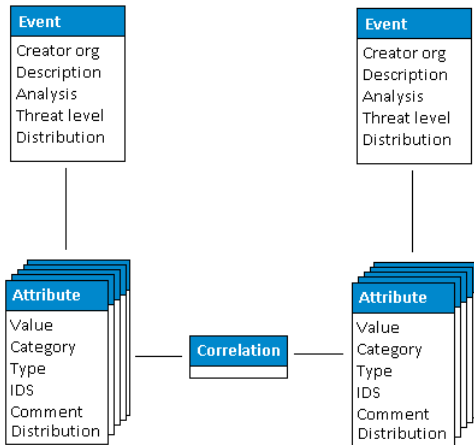
Event
Creator org
Description
Analysis
Threat level
Distribution

# MISP - EVENT

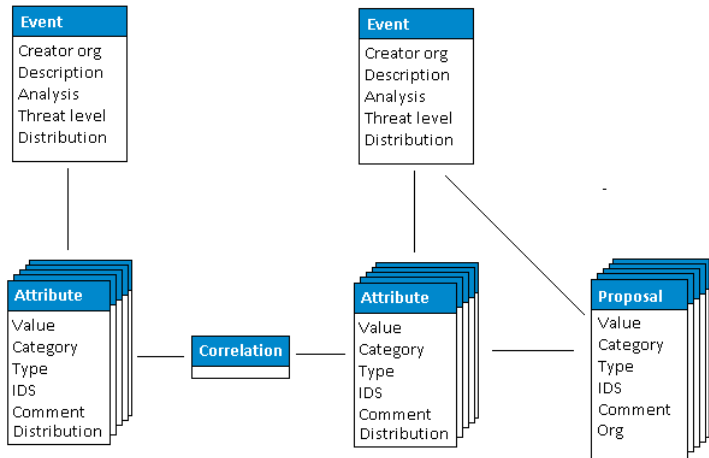
(ATTRIBUTEN, GEVEN EEN BETEKENIS AAN EVENTS)



# MISP - EVENT (CORRELATIES OP GELIJKAARDIGE ATTRIBUTEN)

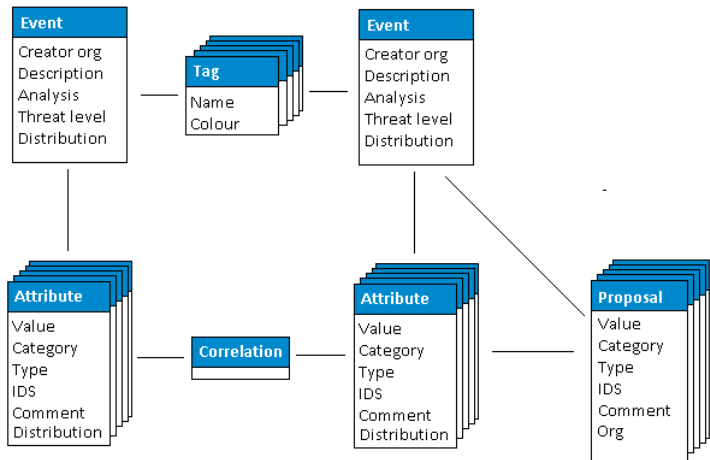


# MISP - EVENT (VOORSTELLEN VOOR ATTRIBUTEN)

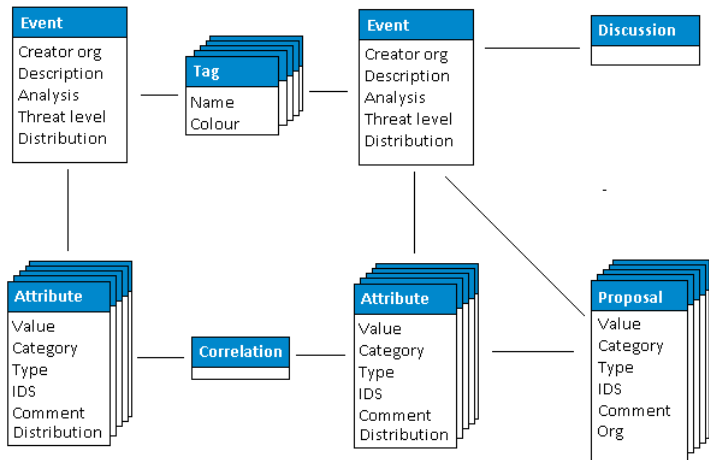




# MISP - EVENT (TAGS)

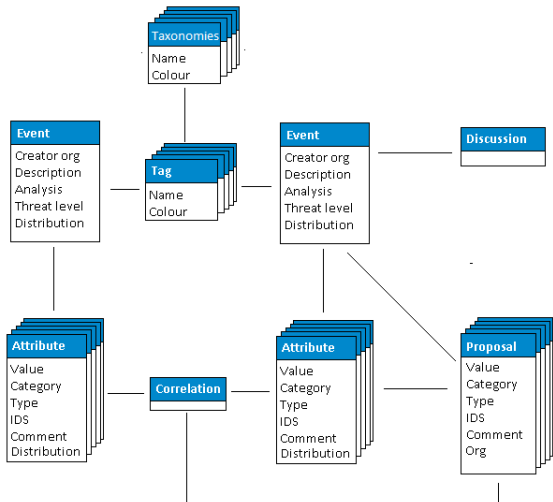


# MISP - EVENT (DISCUSSIONS)



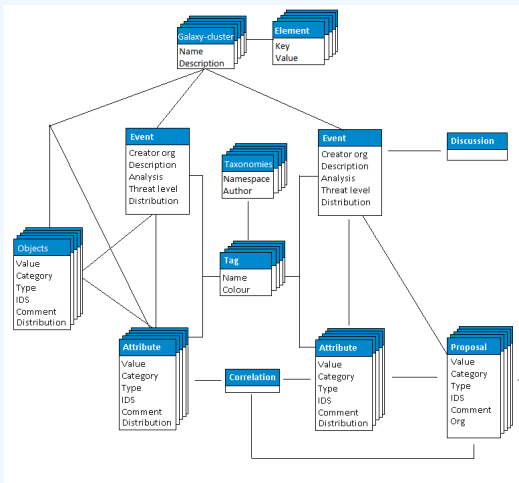
# MISP - EVENT (TAXONOMIËN EN CORRELATIES VOORSTELLEN)

## TUSSEN



# MISP - EVENT

## (HET ALLERNIEUWSTE MISP DATAMODEL)



- Lijst van Events
  - ▶ De context van het event
  - ▶ Tags
  - ▶ Verdelingen
  - ▶ Correlaties
- Filters

- Event scherm
  - ▶ Context van het event
  - ▶ Attributen
    - Verschillende categorieën/types, IDS, Correlaties
  - ▶ Objecten
  - ▶ Galaxies
  - ▶ Voorstellen voor attributen
  - ▶ Discussies
- Hulpmiddelen als ondersteuning om te vinden wat je zoekt
- Grafieken voor correlatie

# MISP - VERSCHILLENDE MANIEREN OM EEN EVENT AAN TE MAKEN EN AAN TE VULLEN (DEMO)

- De belangrijkste hulpmiddelen om een event aan te vullen
  - ▶ Bijvoegen van attributen / in groep bijvullen van attributen
  - ▶ Bijvoegen van objecten en hoe de templates voor objecten werken
  - ▶ Invoeren via vrije tekst
  - ▶ Importeren
  - ▶ Templates
  - ▶ Bijvoegen van bijlagen / schermafbeeldingen
  - ▶ API

# MISP - FUNCTIES BESCHIKBAAR TIJDENS HET BIJVOEGEN VAN GEGEVENS

- Wat gebeurt er automatisch tijdens het toevoegen van gegevens?
  - ▶ Automatische correlatie
  - ▶ Aanpassingen van de invoer via validatie en filters (regex)
  - ▶ Tagging / Clusters van Galaxies
- De verschillende manieren om gegevens te publiceren
  - ▶ Publiceren met of zonder e-mail
  - ▶ Publiceren via de API
  - ▶ Publiceren door middel van delegatie



- Grafieken voor correlatie
- Downloaden van gegevens in verschillende formaten
- Voorgemaakte exports
- API (later besproken)
- Samenwerking met gebruikers (voorstellen, discussies, emails)

# MISP - SYNCHRONISATIE UITGELEGD (VOOR DE 'NIET-ADMIN' TRAINING)

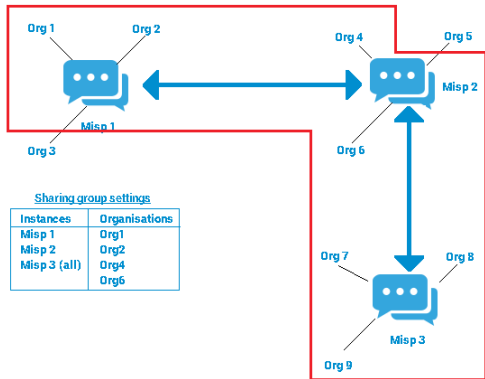
- Het synchronizeren van connecties
- Trekken (Pull) of Duwen (Push) model
- Vooraf bekijken van een instantie
- Filters voor de synchronisatie
- De connectie eerst testen
- Selectieve keuzes voor synchronisatie

# MISP - FEEDS UITGELED (VOOR DE 'NIET-ADMIN' TRAINING)

- Types van feeds (MISP, vrije tekst, CSV)
- Bijvoegen of aanpassen van feeds
- Vooraf bekijken van feeds
- Lokale feeds ten opzichte van netwerk feeds

- Enkel jouw organisatie
- Enkel deze gemeenschap
- Aangesloten gemeenschappen
- Alle gemeenschappen
- Groepen voor delen

# MISP - VERDELING EN TOPOLOGIE



- Downloaden van een event
- Een snelle introductie tot de APIs
- Downloaden van zoekresultaten
- Voorgemaakte exports

# MISP - EENVOUDIGE INTRO TOT ADMIN (VOOR DE 'NIET-ADMIN' TRAINING)

- Instellingen
- Het oplossen van problemen
- Ondersteuners (workers)
- Logbestanden