CIRCL / Team MISP Project

http://www.misp-project.org/
Twitter: @MISPProject

CIRCL - Uni.lu

MISP
Threat Sharing

MISP - VM

- 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/`

MISP - VM

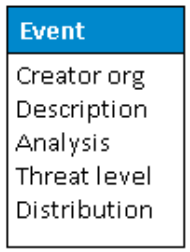
- Je moet zelf wel nog enkele aanpassingen doen
  - sudo -s
  - cd /var/www/MISP/
  - sudo pear install INSTALL/dependencies/Console_CommandLine/package.xml
  - sudo pear install INSTALL/dependencies/Crypt_GPG/package.xml
  - cd /usr/local/src/misp-modules
  - pip3 install -r REQUIREMENTS
  - pip3 install .
  - reboot

MISP - Algemeen gebruik

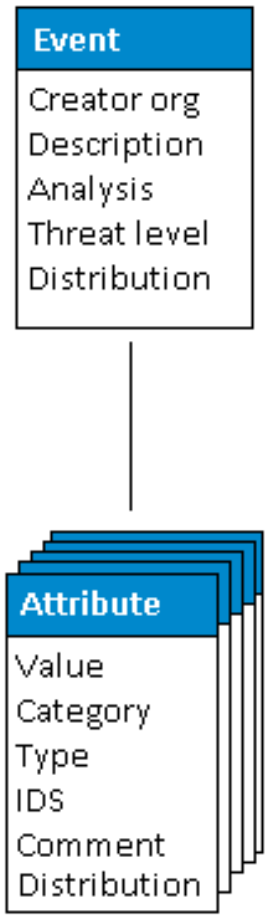
De planning voor deze training

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

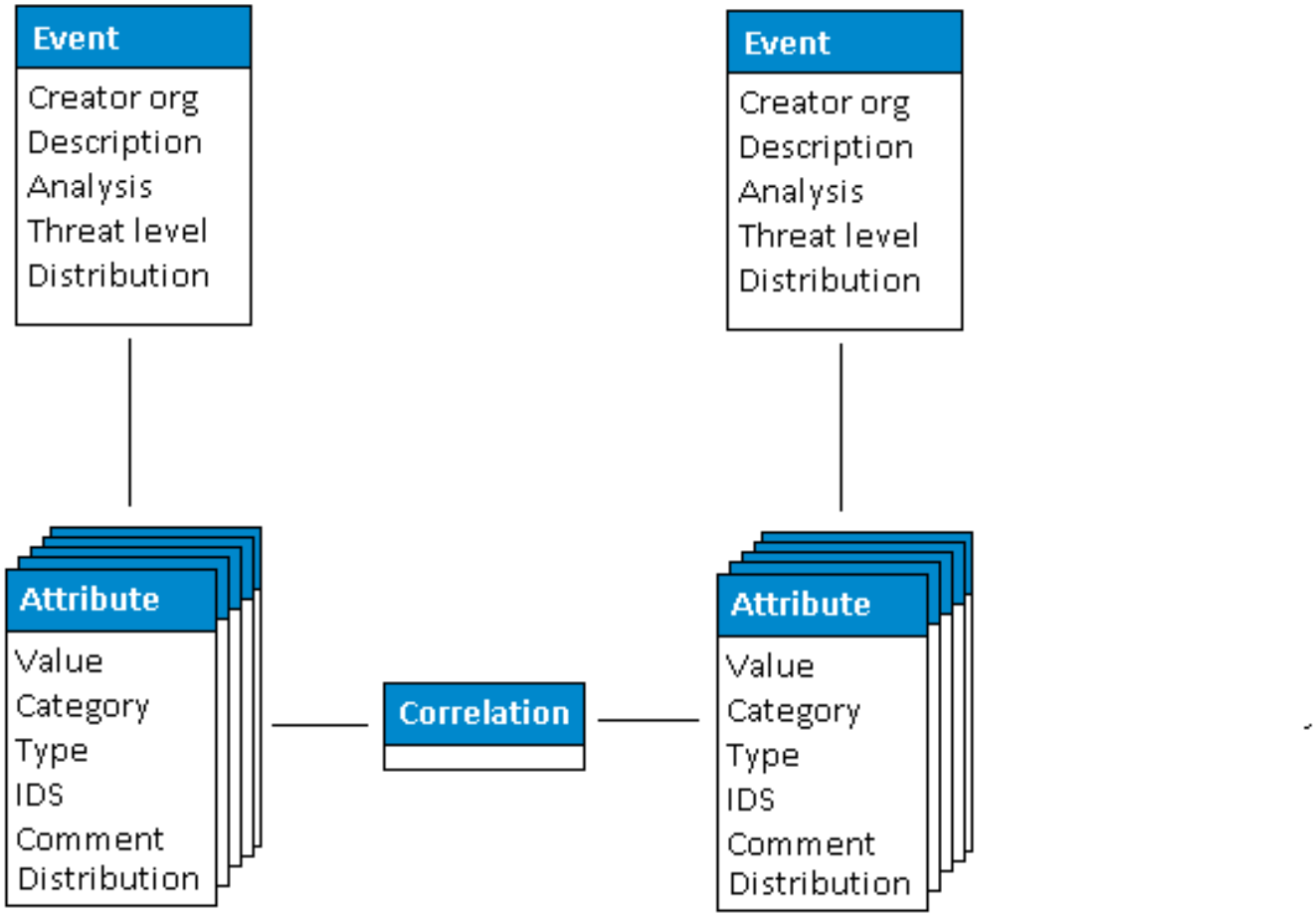
MISP - Event
(de basis bouwsteen van MISP)



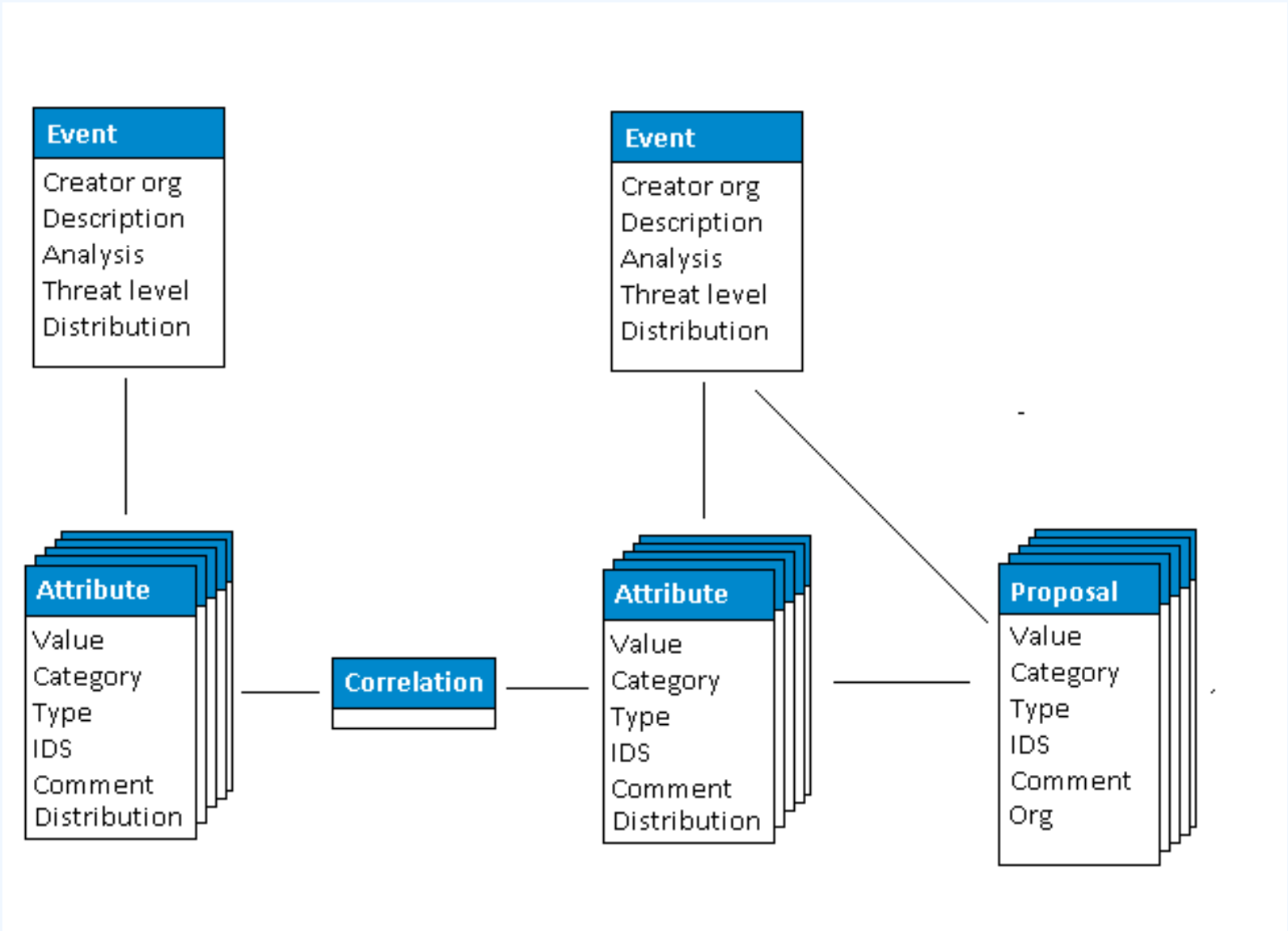
MISP - Event
(Attributen, geven een betekenis aan events)



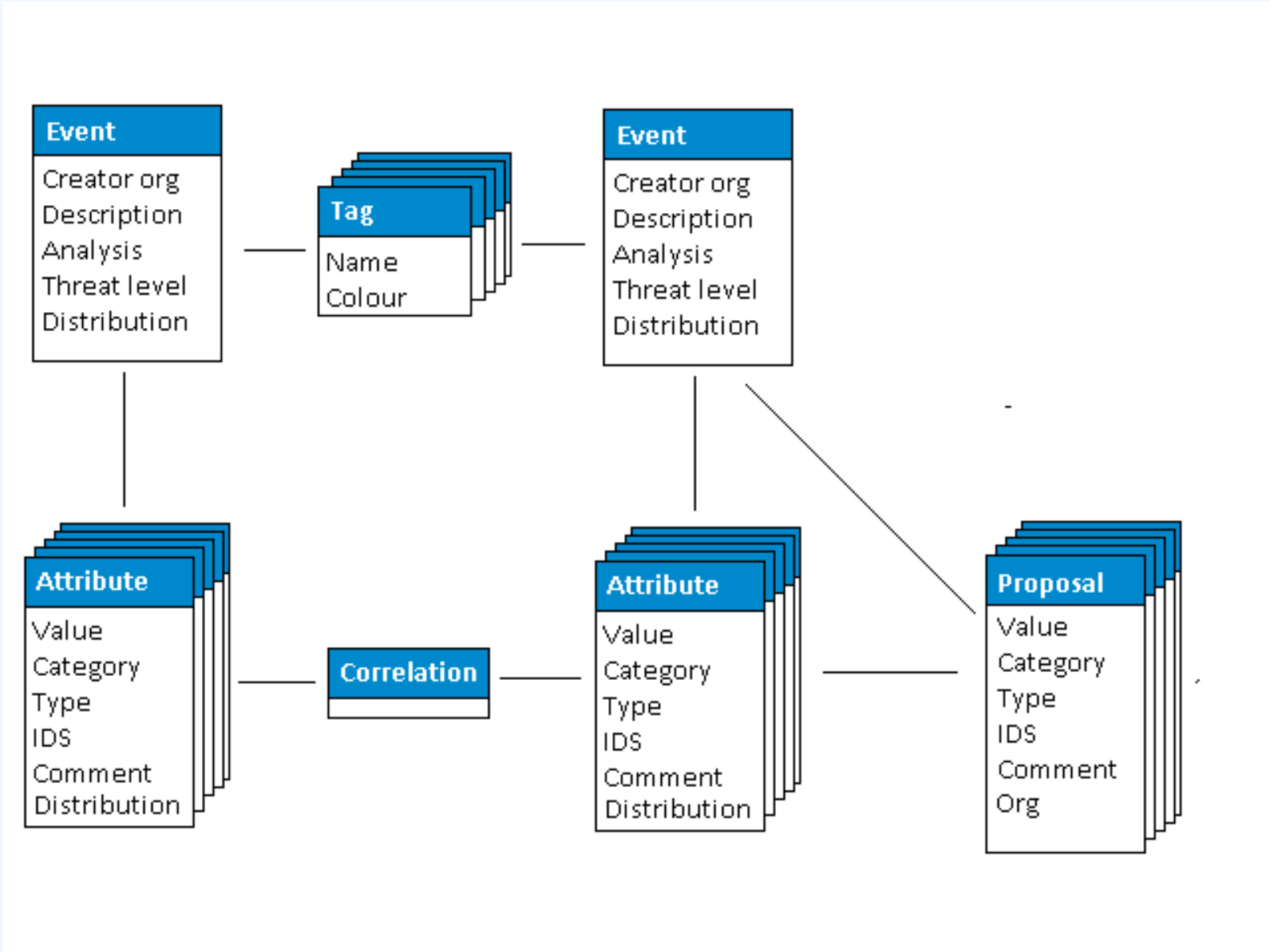
MISP - Event
(Correlaties op gelijkaardige attributen)



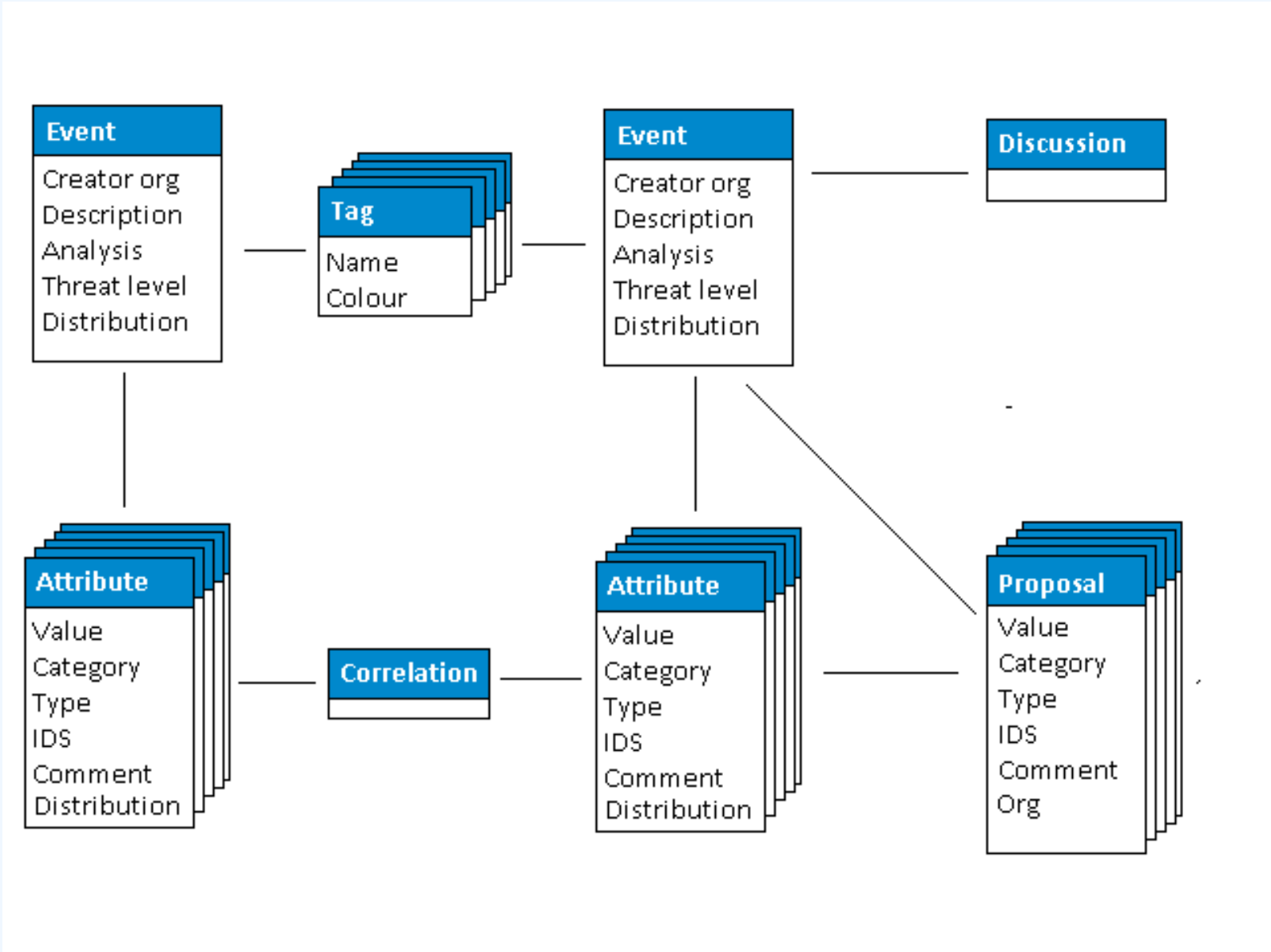
MISP - Event (Voorstellen voor Attributen)



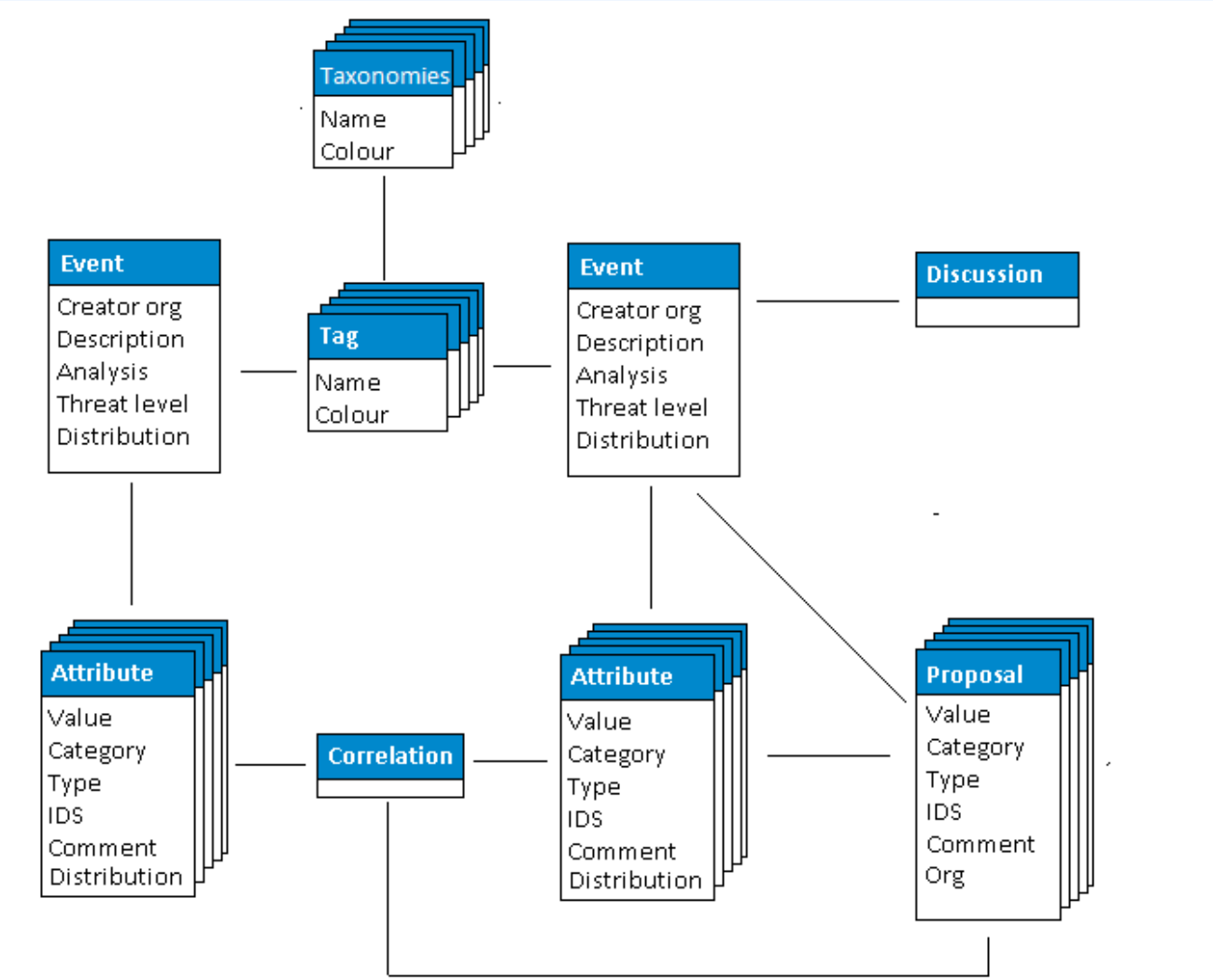
MISP - Event (Tags)



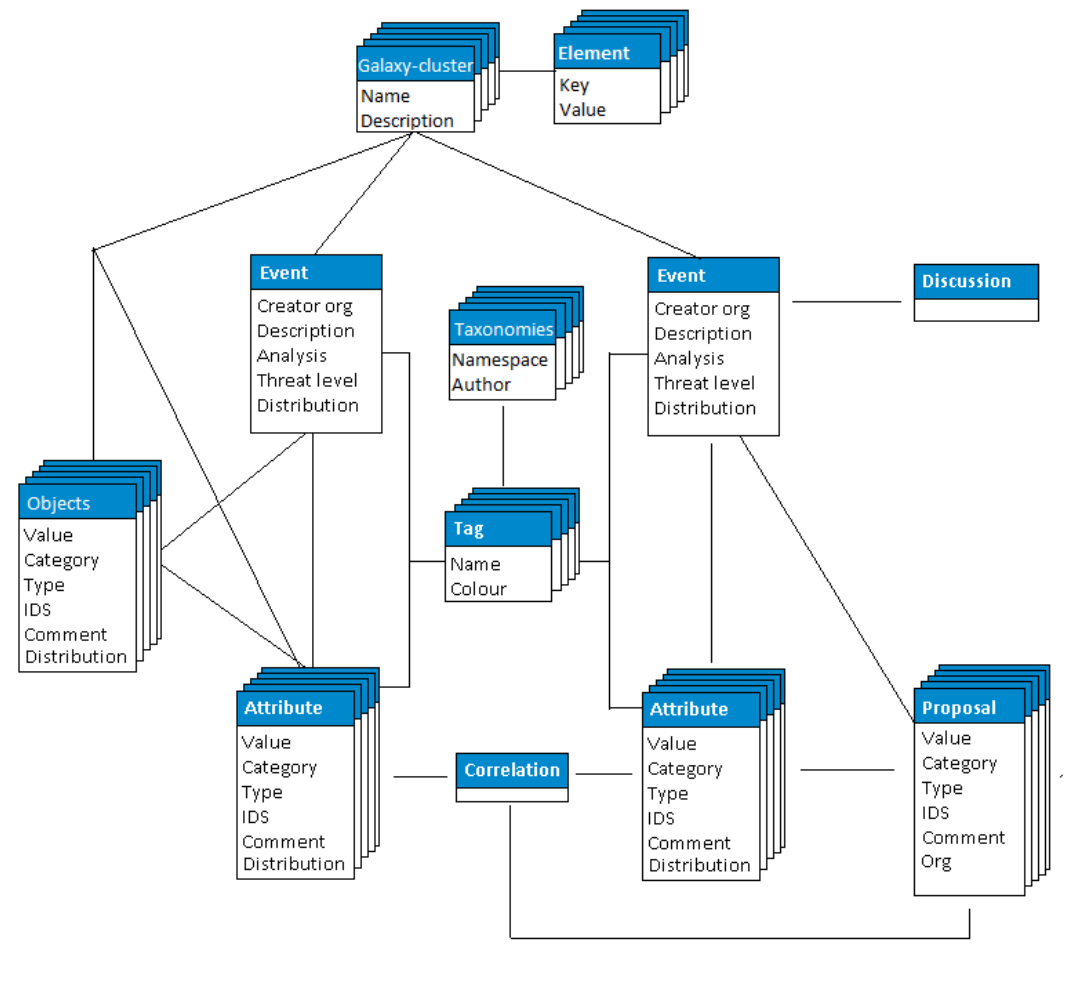
MISP - Event (Discussies)



MISP - Event (Taxonomieën en correlaties tussen voorstellen)



MISP - Event
(Het allernieuwste MISP datamodel)



MISP - De lijst van Events Bekijken

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

MISP - Een Event Bekijken

- 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

MISP - Manieren om de gegevens te gebruiken

- 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

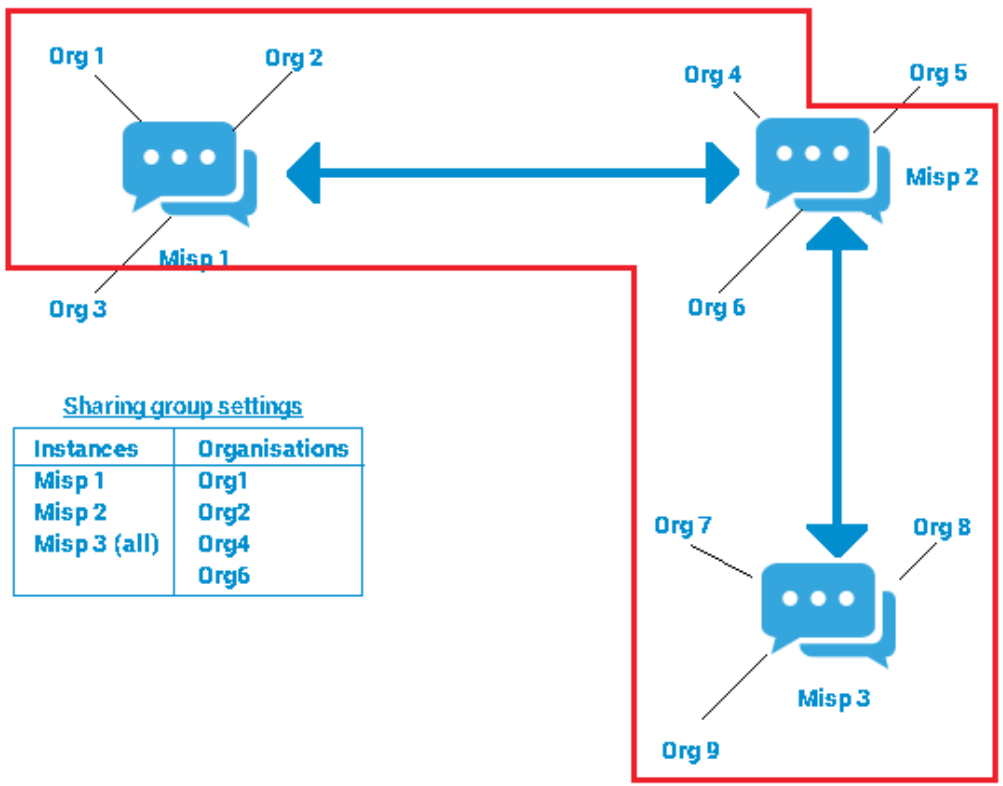
MISP - Feeds uitgeled (voor de 'niet-admin' training)

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

MISP - Verdeling van informatie uitgelegd

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

MISP - Verdeling en Topologie



Sharing group settings

Instances	Organisations
Misp 1	Org1
Misp 2	Org2
Misp 3 (all)	Org4
	Org6

MISP - Exporteren en API

- 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