CIRCL / Team MISP Project

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

CTIS 2022

MISP
Threat Sharing

MISP - VM

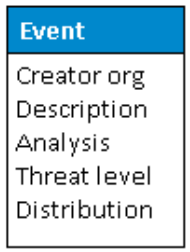
- Credenciales
  - MISP admin: admin@admin.test/admin
  - SSH: misp/Password1234
- Disponible para descargar aquí (VirtualBox and VMWare):
  - `https://www.circl.lu/misp-images/latest/`

MISP - Uso Básico

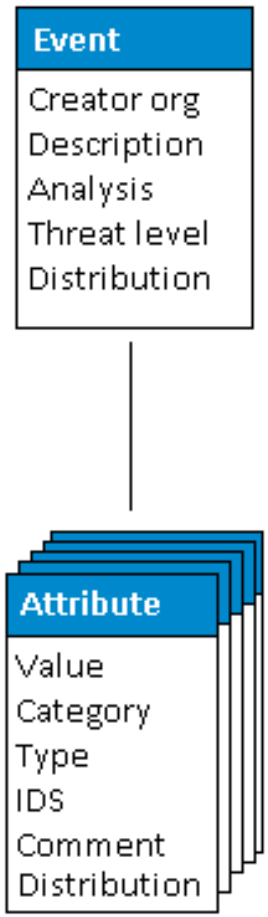
Plan para esta parte de la capacitación

- Modelo de datos
- Visualizando datos
- Alta de datos
- Cooperación
- Distribución
- Exportando datos

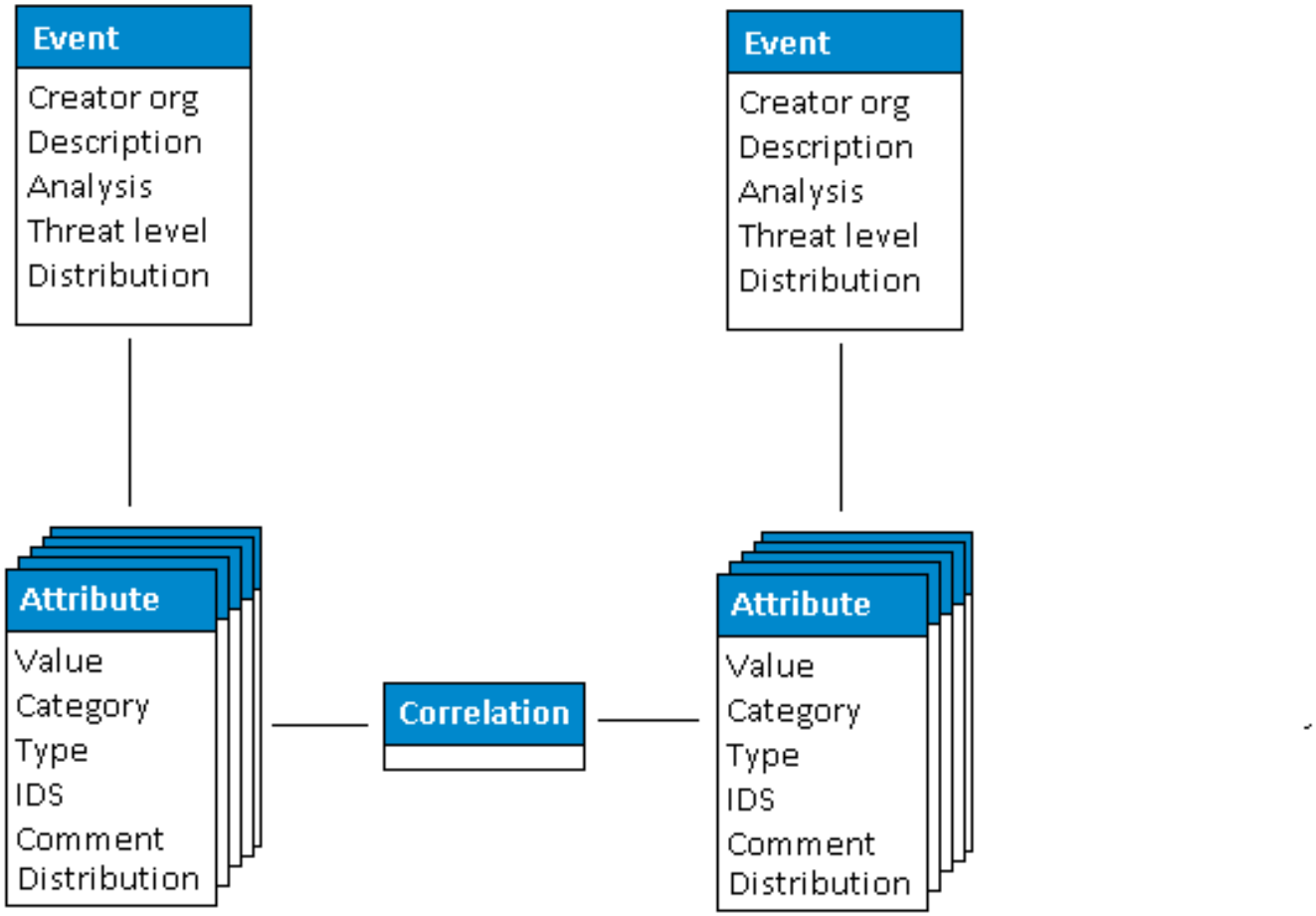
MISP - Eventos (El componente fundamental de MISP)



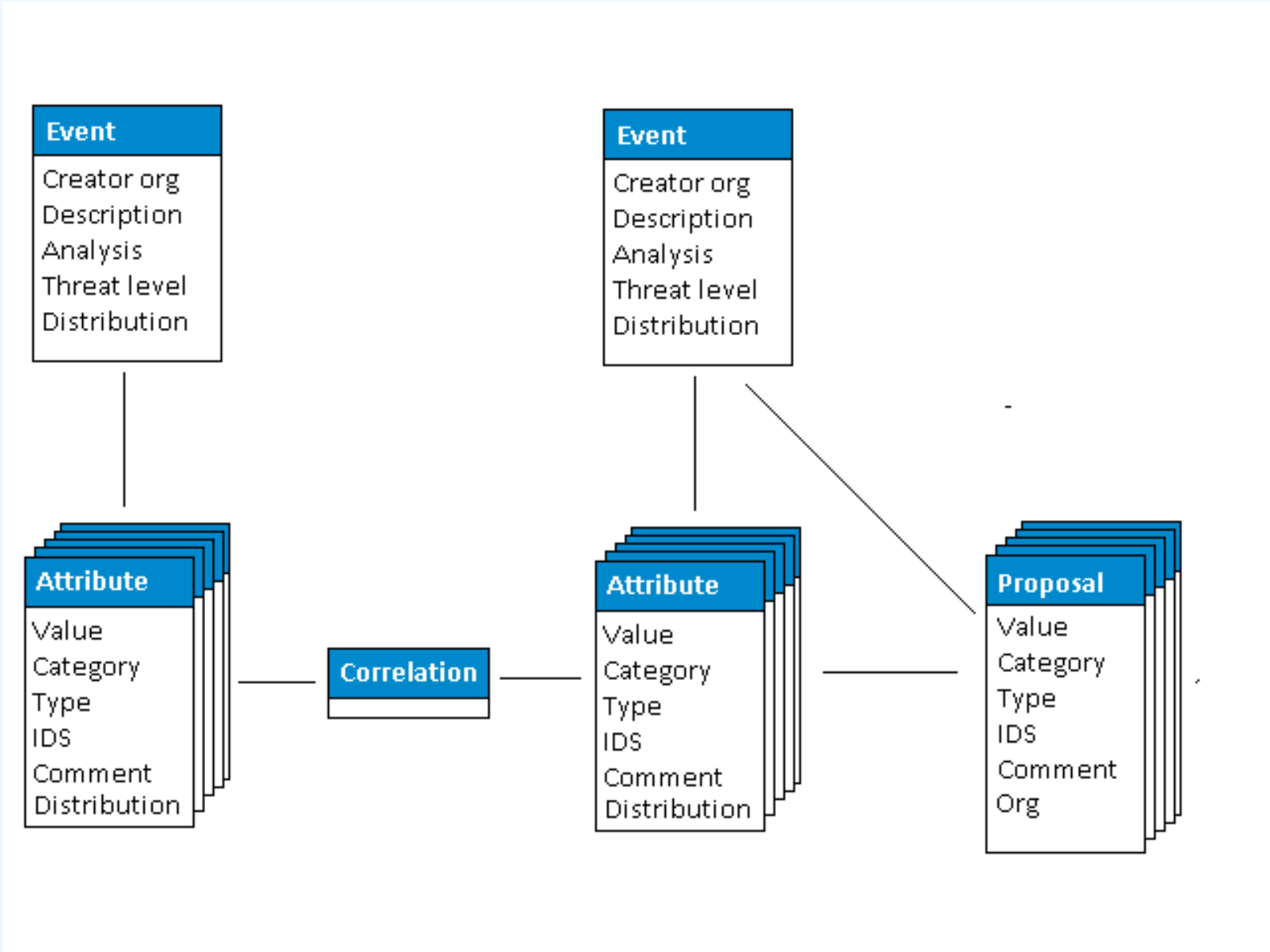
MISP - Eventos (Atributos, dando significado a los eventos)



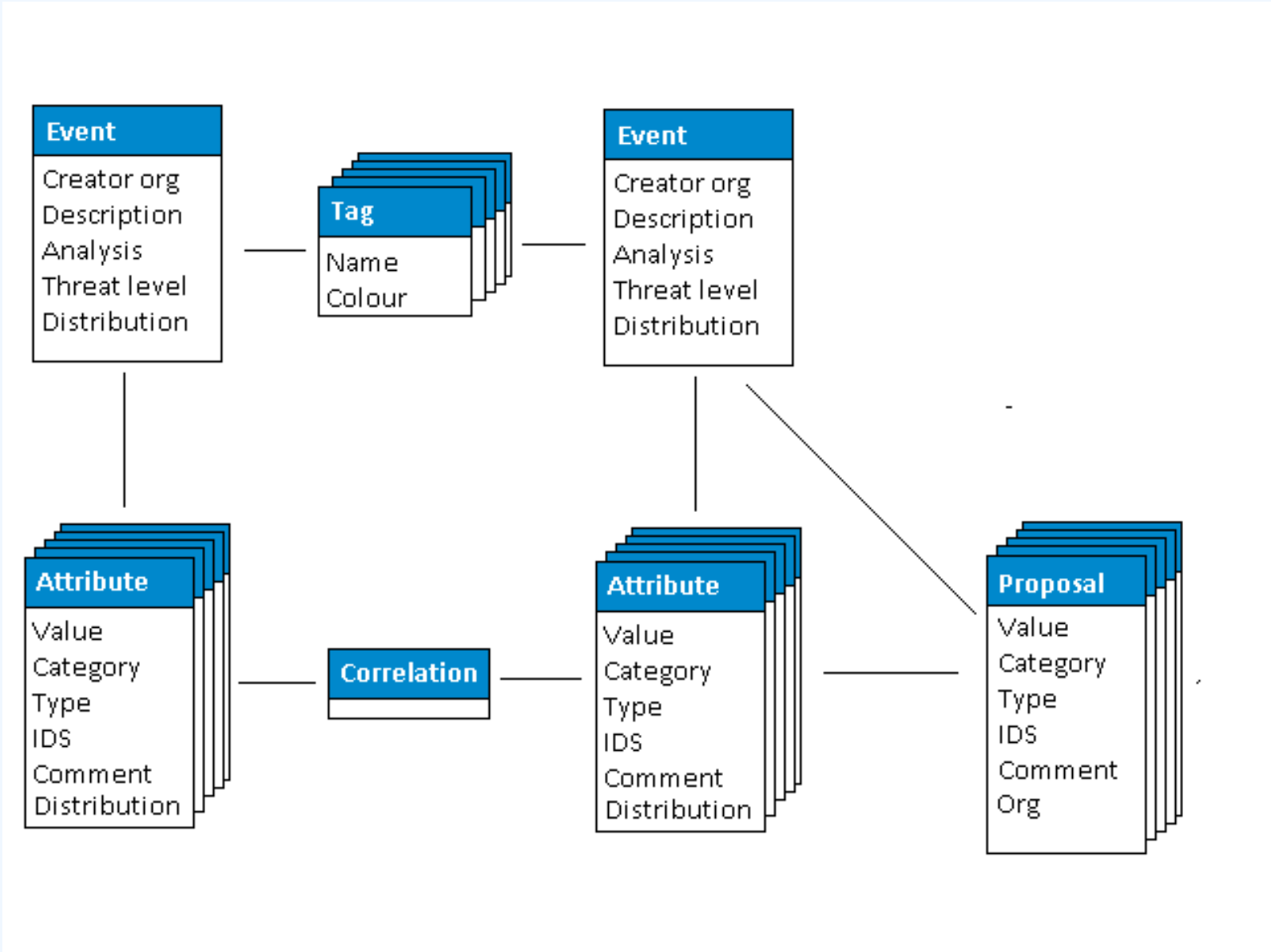
MISP - Eventos (Correlaciones entre atributos similares)



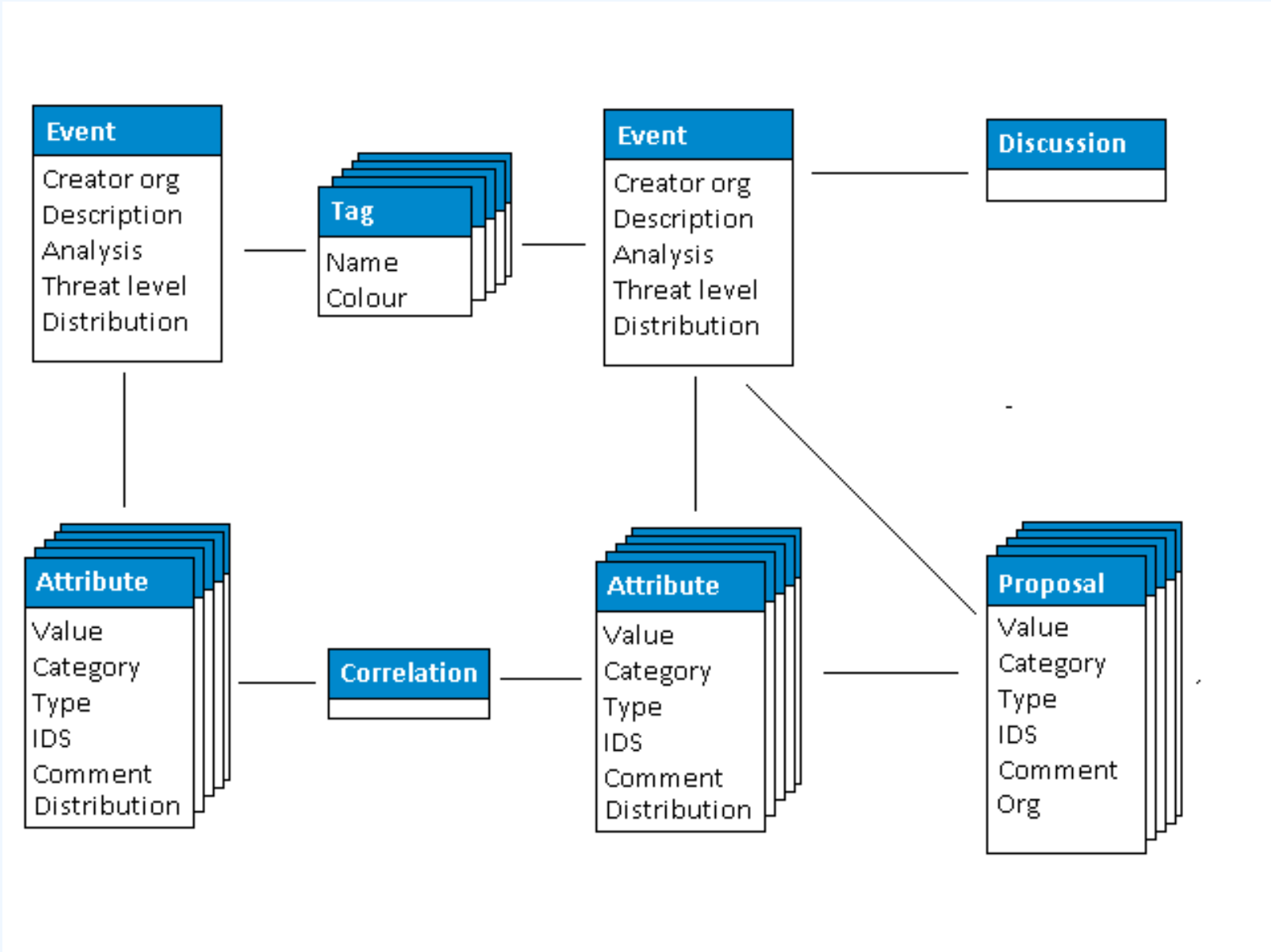
MISP - Eventos (Propuestas)



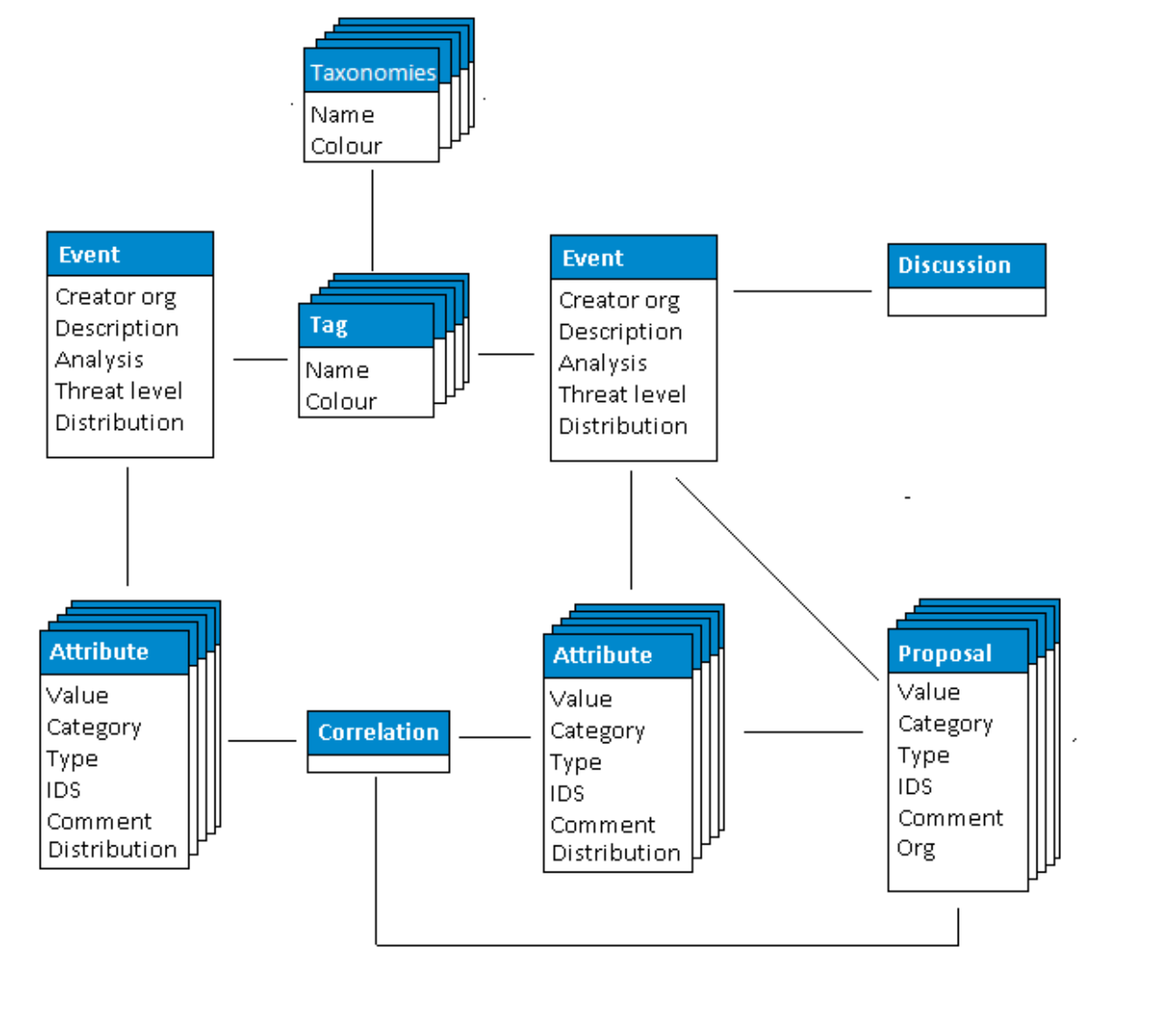
MISP - Eventos (Etiquetas)



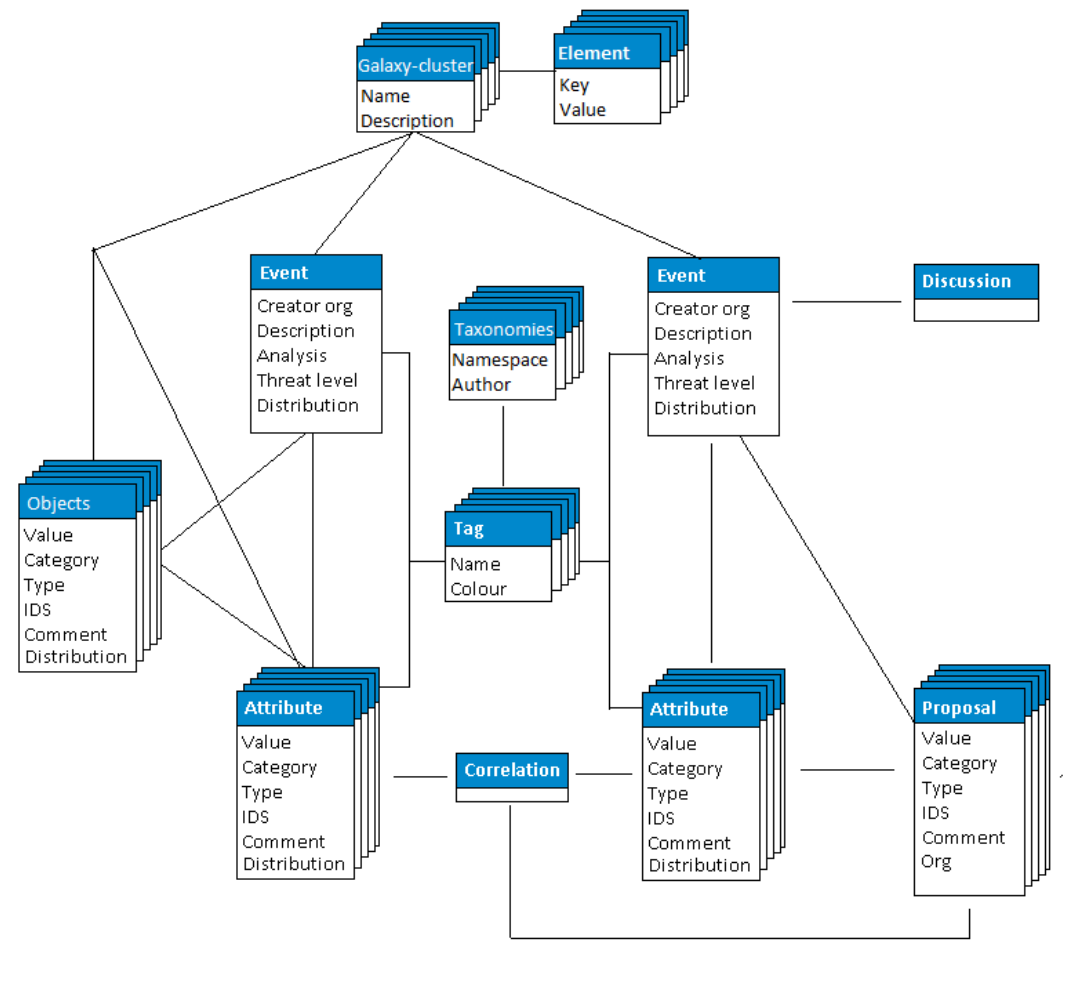
MISP - Eventos (Discusiones)



MISP - Eventos (Taxonomías y propuestas de correlaciones)



MISP - Eventos (El estado del arte del modelo de datos de MISP)



MISP - Visualizando el listado de Eventos

- Listar Eventos
  - Contexto del Evento
  - Etiquetas
  - Distribución
  - Correlaciones
- Filtros

MISP - Visualizando un Evento

- Ver Evento
  - Contexto del Evento
  - Atributos
    - Categoría/tipo, IDS, Correlaciones
  - Objetos
  - Galáxias
  - Propuestas
  - Discusiones
- Herramientas para encontrar lo que buscas
- Grafos de correlaciones

MISP - Alta y carga de eventos en diferentes formas (demo)

- Las principales formas de cargar eventos
  - Añadir atributos / Añadir en lotes
  - Añadir objetos y cómo funcionan las plantillas de objetos
  - Importar texto libre
  - Importar
  - Plantillas
  - Añadir archivos adjuntos / capturas de pantalla
  - API

MISP - Diferentes funcionalidades para añadir información

- ¿Qué sucede automáticamente cuando agregamos información?
  - Correlación automática
  - Modificación de la carga vía validación y filtros (regex)
  - Etiquetado / Cúmulos de galaxias
- Diferentes formas de publicar información
  - Publicar con/sin enviar un e-mail
  - Publicar vía la API
  - Delegación

MISP - Utilizando la información

- Grafos de correlaciones
- Descargando la información en diferentes formatos
- API (más detalles luego)
- Colaborando con usuarios (propuestas, discusiones, emails)

MISP - Sincronización en detalle

- Conexiones de sincronización
- Modelo pull/push
- Previsualización de instancias
- Filtrado de la sincronización
- Herramienta de prueba de conexión
- Modo de selección manual

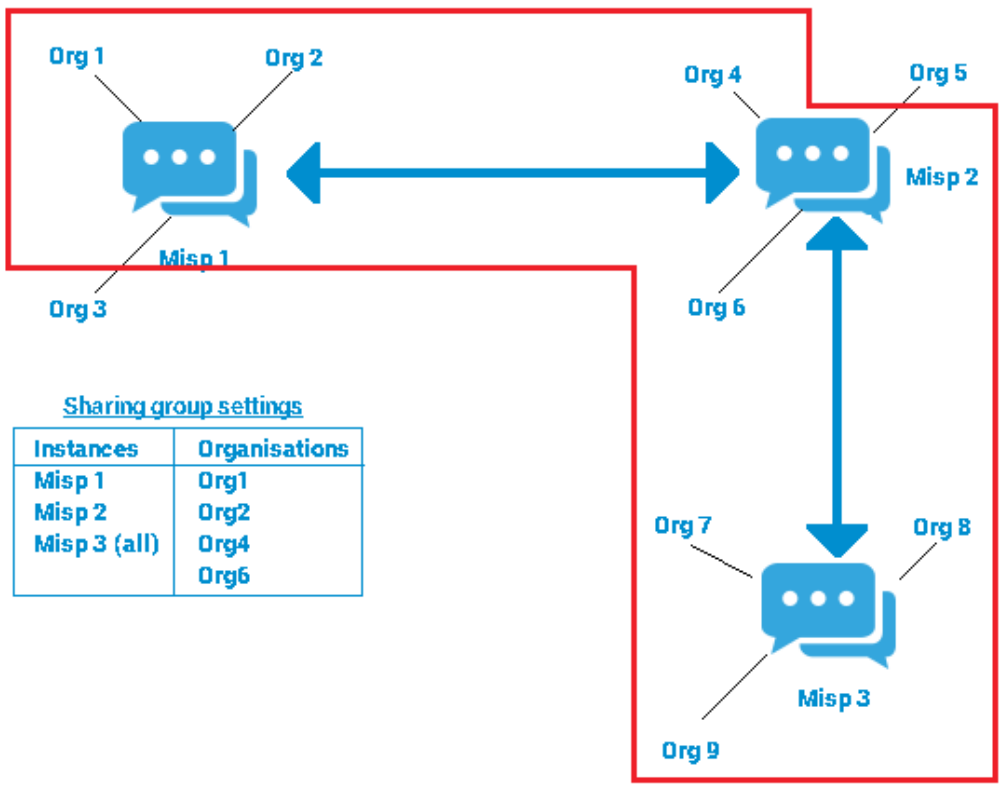
MISP - Fuentes (feeds) en detalle

- Tipos de fuentes (MISP, texto libre, CSV)
- Alta/edición de fuentes
- Previzualización de fuentes
- Fuentes Locales vs. Remotas

MISP - Distribuciones en detalle

- Solo Mi Organización
- Solo Esta Comunidad
- Comunidades Conectadas
- Todas las Comunidades
- Grupo de Intercambio

MISP - Distribución y Topología



Sharing group settings

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

MISP - Exportar y API

- Descargar un evento
- Un vistazo a las APIs
- Descargar resultados de una búsqueda
- API REST y generador de consultas

MISP - Tareas administrativas

- Configuración
- Resolución de problemas
- Trabajadores (workers)
- Registros (logs)