

CIRCL / TEAM MISP PROJECT

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

TWITTER: [@MISPPROJECT](https://twitter.com/MISPPROJECT)

CIRCL - UNI.LU



MISP
Threat Sharing

■ Credenciales

- ▶ MISP admin: admin@admin.test/admin
- ▶ SSH: misp/Password1234

■ Disponible para descargar aquí (VirtualBox and VMWare):

- ▶ <https://www.circl.lu/misp-images/latest/>

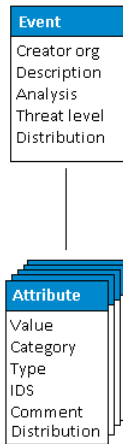
Plan para esta parte de la capacitación

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

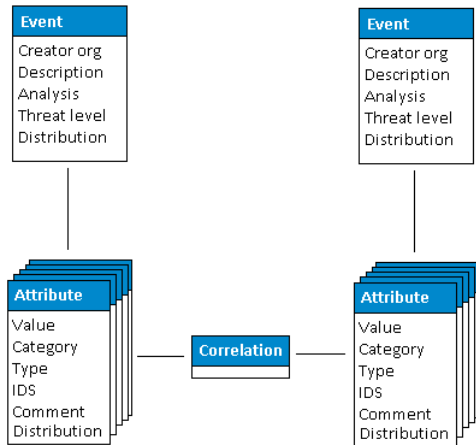
MISP - EVENTOS (EL COMPONENTE FUNDAMENTAL DE MISP)

Event
Creator org
Description
Analysis
Threat level
Distribution

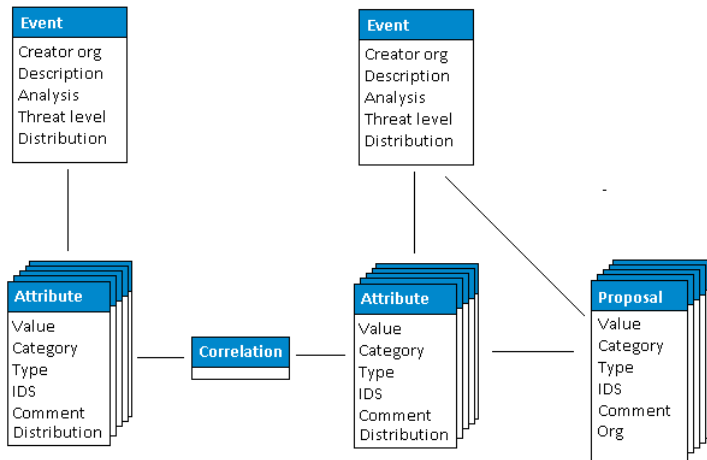
MISP - EVENTOS (ATRIBUTOS, DANDO SIGNIFICADO A LOS EVENTOS)



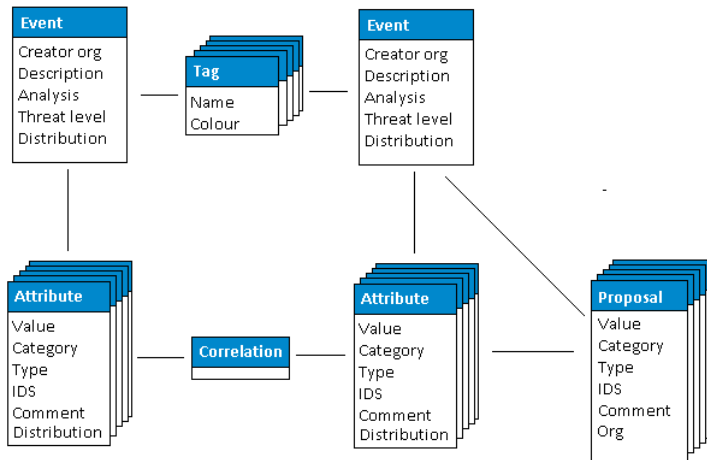
MISP - EVENTOS (CORRELACIONES ENTRE ATRIBUTOS SIMILARES)



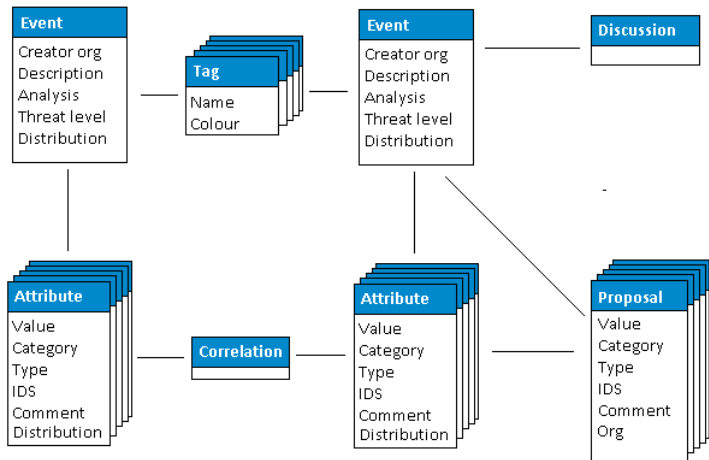
MISP - EVENTOS (PROPUESTAS)



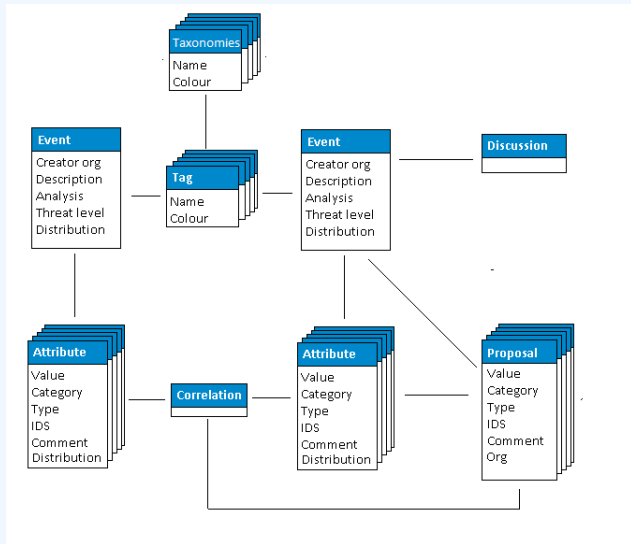
MISP - EVENTOS (ETIQUETAS)



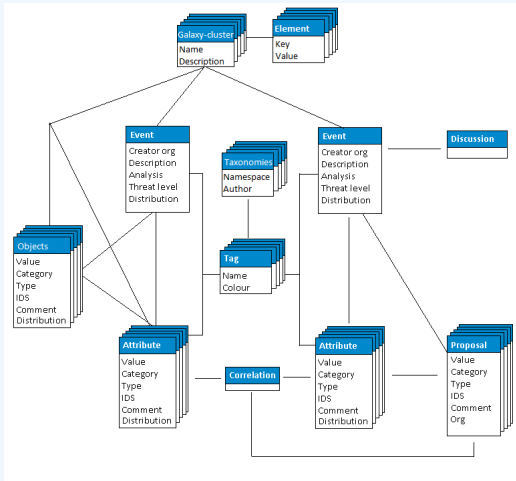
MISP - EVENTOS (DISCUSIONES)



MISP - EVENTOS (TAXONOMÍAS Y PROPUESTAS DE CORRELACIONES)



MISP - EVENTOS (EL ESTADO DEL ARTE DEL MODELO DE DATOS DE MISP)



■ Listar Eventos

- ▶ Contexto del Evento
- ▶ Etiquetas
- ▶ Distribución
- ▶ Correlaciones

■ Filtros

■ 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

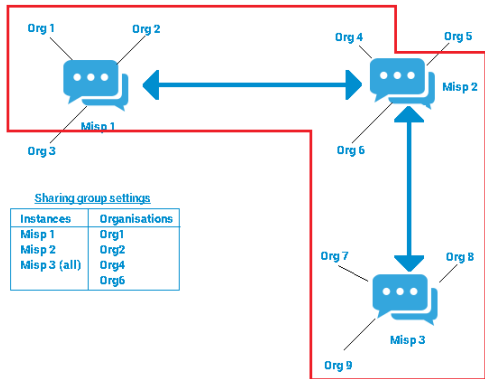
- Grafos de correlaciones
- Descargando la información en diferentes formatos
- API (más detalles luego)
- Colaborando con usuarios (propuestas, discusiones, emails)

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

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

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

MISP - DISTRIBUCIÓN Y TOPOLOGÍA



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

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