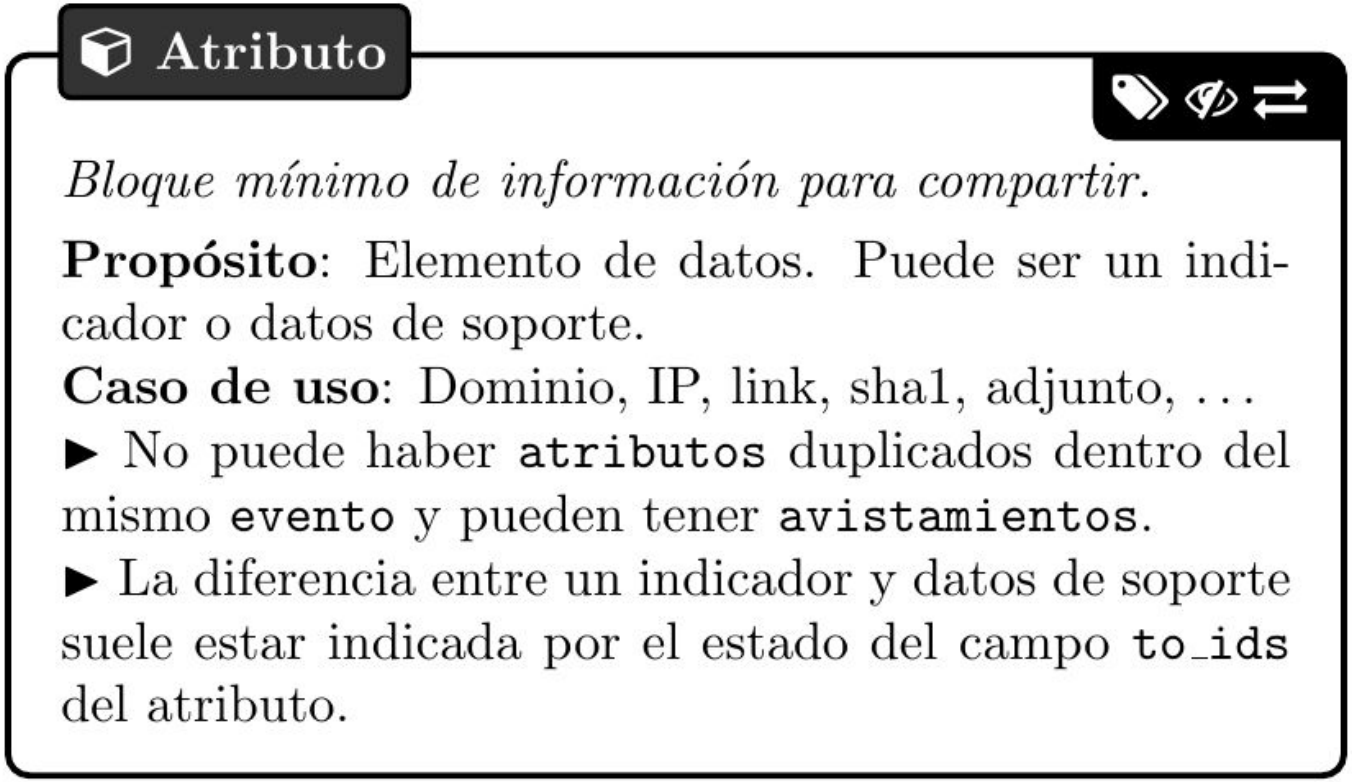
Modelo de Datos en MISP

Tipos de datos

Capa de Datos

MISP Atributos



MISP Objetos

MISP Objeto

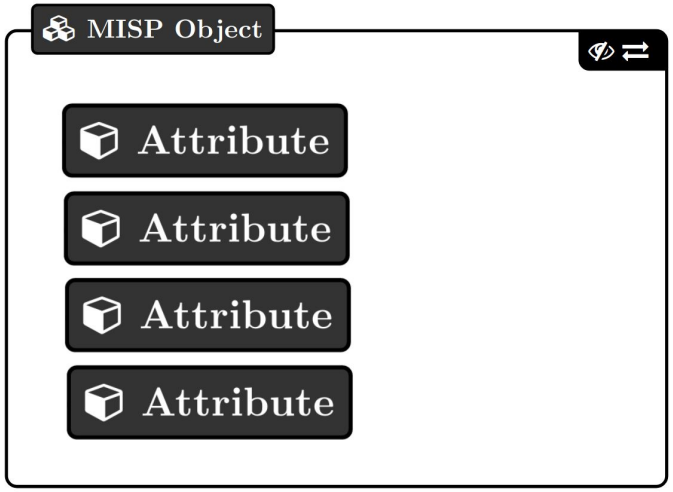
Bloque avanzado que soporta composición de `atributos` *via plantillas.*

Propósito: Agrupa `atributos` que están instrínsecamente relacionados.

Caso de uso: Fichero, persona, tarjeta de crédito, x509, dispositivo, ...

▶ Los `objetos` tienen definida su composición de `atributos` en su respectiva plantilla. Son instanciados con `atributos` y pueden `referenciar` otros `atributos` u `objetos`.

▶ MISP no requiere tener la plantilla para guardar y mostrar el `objeto`. Sin embargo, no será posible *editar* dado que es necesaria la plantilla para validarlo.



MISP Eventos

Evento

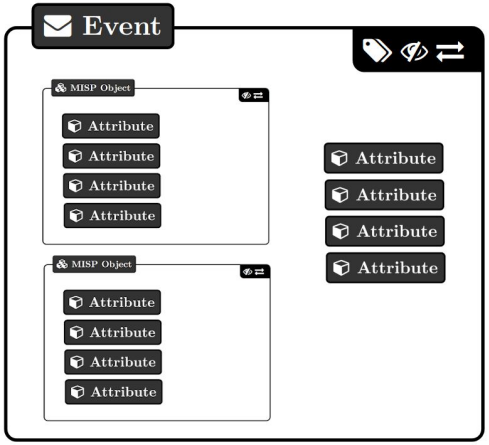
Encapsula información vinculada contextualmente.

Propósito: Agrupa datos y contexto. Actúa como un contenedor, permite definir la distribución y sus propias reglas de intercambio y los elementos que contiene.

Caso de uso: Codifica incidentes/eventos/reportes/...

▶ Los `eventos` pueden contener otros elementos como `atributos`, `objetos` y `reportes`.

▶ El nivel de distribución y el contexto agregado a nivel `evento` (como `taxonomías`) son propagados a los elementos dependientes.



MISP Reporte de Evento

Reporte de Evento

Bloque avanzado para escribir reportes en lenguaje natural.

Propósito: Elemento de soporte en formato texto para describir eventos o procesos.

Caso de uso: Codificar reportes, proporcionar más información acerca de un `evento`, ...

▶ Los `reportes`, pueden ser escritos en markdown e incluyen una sintaxis especial para referenciar elementos tales como `atributos` o contexto.

Referencias de Objetos

↗ Referencias de Objetos

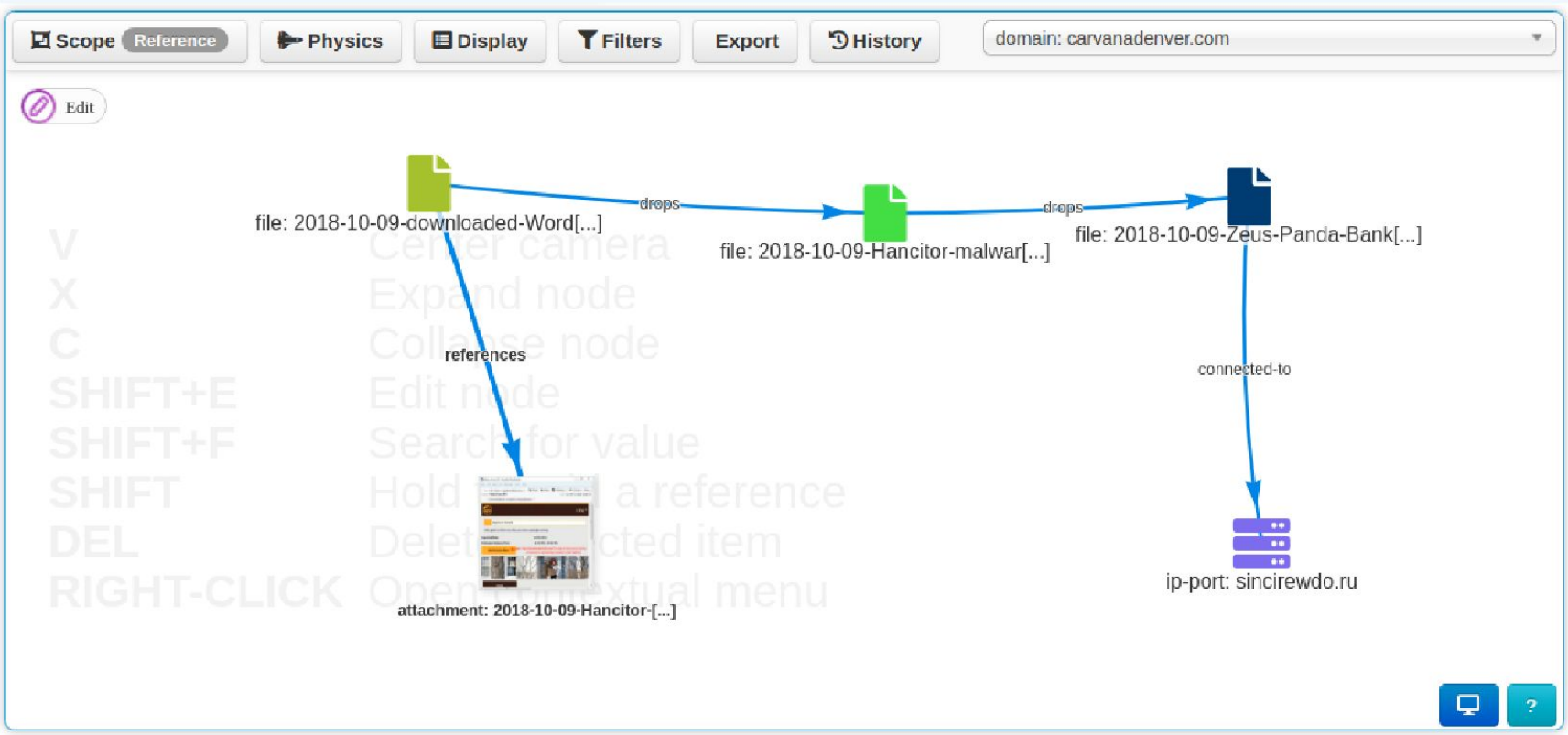
Relaciones entre bloques individuales.

Propósito: Permite crear relaciones entre entidades, creando un grafo donde las relaciones son líneas y las entidades los nodos.

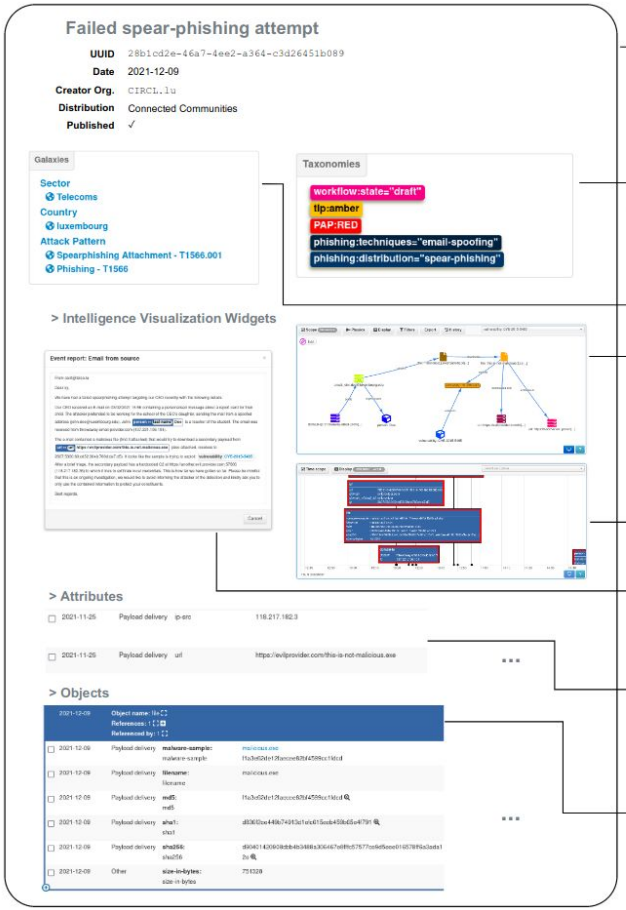
Caso de uso: Representan comportamientos, similaridades, asociaciones, ...

▶ Las `referencias` pueden tener una relación que puede estar definida en MISP o ser de texto libre.

Referencias de Objetos



Anatomía de un Evento



Representation of an incident in MISP

Event: Encapsulates contextually linked information.
Events also have basic information including ownership and access-control
Here: Contains all the information related to the spear-phishing incident.

Taxonomies: Simple label standardised on common set of vocabularies.
Here: Usage of labels to classify the current completeness of the Event, what recipient can do with the information and the category of the incident.

Galaxies & Galaxy-Clusters: Advanced label containing meta-data
Here: The sector affected by the incident as well as the country. The kill-chain of the attack can be described using the MITRE ATT&CK framework

Event Graph: Visualization of the relationships between entities contained in the Event.
Here: The whole story of the attack can be described with relationships defined between Attributes and Objects

Event Timeline: Visualization of the temporality of the data contained in the event.
Here: A timeline of the steps performed during the attack. The time data is taken directly from the Attributes and Objects belonging to the Event.

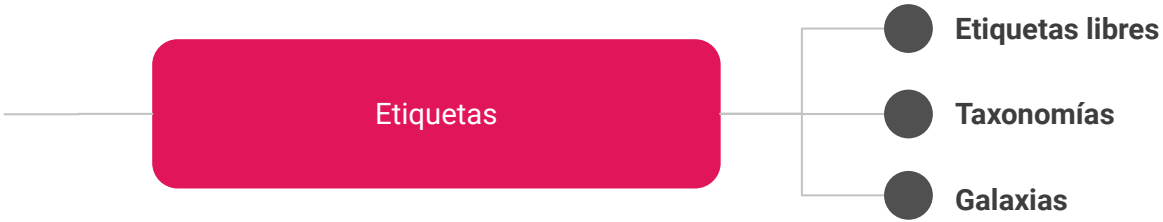
Event Report: Markdown-aware supporting text document to describe events or incidents
Here: The report describe the steps taken by the attacker and provide additional contextual information. It also contains references to Attributes and Object encoded in the Event

Attributes: Basic building block to represent information.
They can have context such as taxonomy and express if they are supportive data or meant for automation. An Event can have multiple Attributes
Here: Two Attributes representing payload delivery. One is an IP address, the other is an URL.

Objects: Advanced building block allowing Attribute composition via predefined templates.
As an Object is an instantiation of its template, it is composed of Attributes that make sense Together. They can also have relationship to other entity contained in the Event
Here: A file object composed of Attributes such as the filename, size and hashes. It also have a relationship

Capa de Contexto

Etiquetas



- **Etiquetas libres**: Rótulo donde el texto puede ser definido sin restricciones
- **Taxonomías**: Clasificación normalizada para expresar un mismo vocabulario
- **Galaxias**: Clasificación normalizada con metadata adicional

Etiquetas libres

- Rótulos donde el texto no tiene restricciones
- La forma más sencilla de contextualización
- Puede dificultar la automatización y comprensión

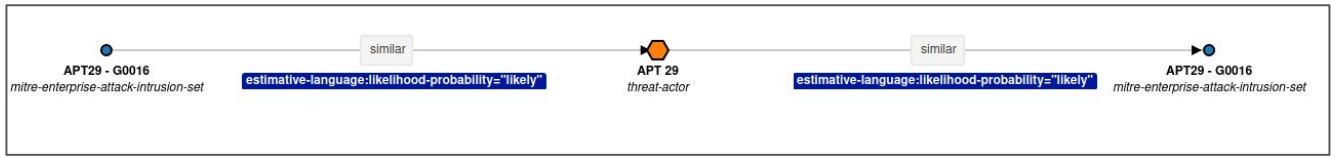
Taxonomías

- Rótulo estandarizado con un vocabulario común
- Clasificación eficiente globalmente comprendida
- Facilita la utilización y automatización

Tag	Events	Attributes	Tags
workflow:state="complete"	11	0	workflow:state="complete"
workflow:state="draft"	0	0	workflow:state="draft"
workflow:state="incomplete"	55	10	workflow:state="incomplete"
workflow:state="ongoing"	0	0	workflow:state="ongoing"

Galaxias

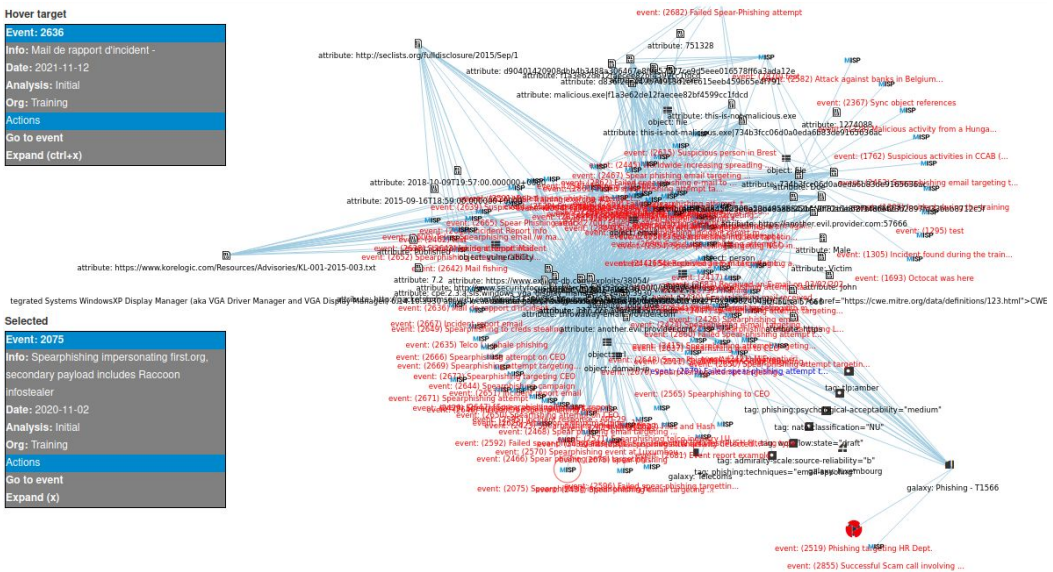
- Clasificación normalizada con metadata adicional
- Permite la descripción de información compleja de alto nivel
- Utilizada internamente para representar la matriz del framework **MITRE ATT&CK**



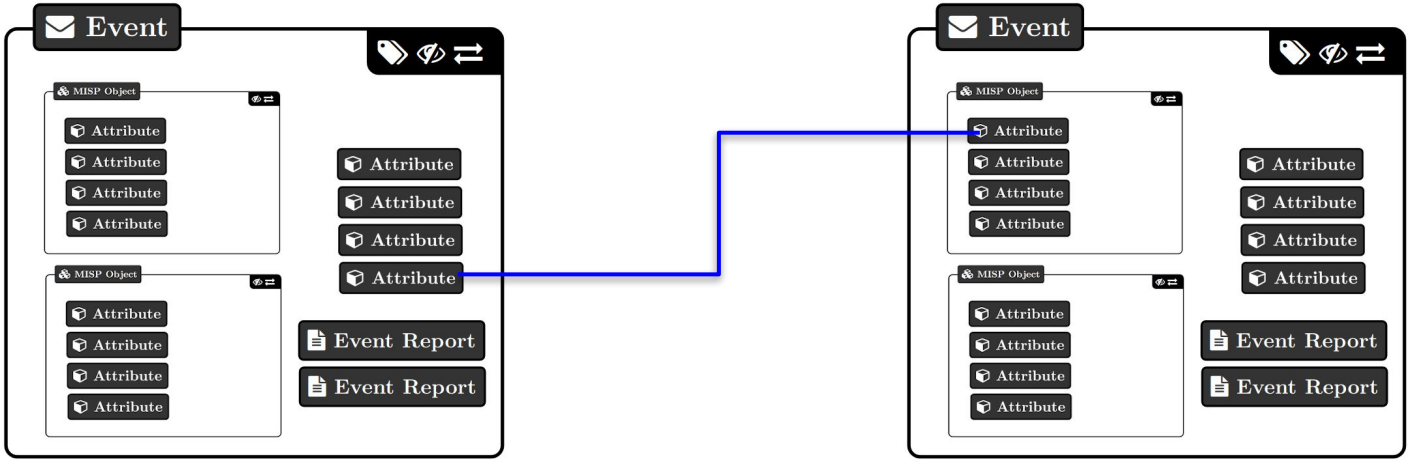
Correlaciones en MISP

Correlaciones en MISP

- Correlaciones
  - Relaciones creadas automáticamente cuando un atributo es creado o modificado. Permiten relacionar Eventos en función de sus Atributos.
- Motor de Correlaciones
  - Es el sistema que MISP utiliza internamente para relacionar los valores de los Atributos



Correlaciones en MISP



01 **Texto**

- Ocurrencia exacta del valor
- `DEADBEEF` <-> `DEADBEEF`

02 **Bloque CIDR**

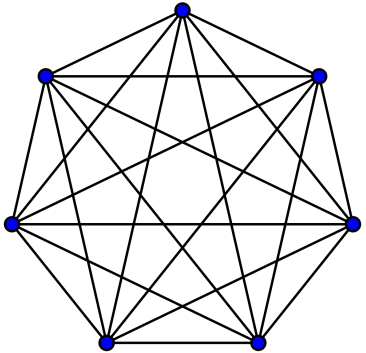
- Si una IP está contenida en un bloque CIDR
- `1.1.1.0/24` <-> `1.1.1.128`

03 **SSDEEP Hash**

- Algoritmo que computa fuzzy-hashes
- `3:q8wK6FuFWcEqlv:3wK6FN1I,"stdin"`
- `ssdeep-1.1/cycles.c matches md5deep-1.12/cycles.c (94)`
- Setting: MISP.ssdeep_correlation_threshold

Correlaciones en MISP

- Agrupar la información correctamente es importante
  - Utilizar eventos extendidos si aplica
  - Separar datos por incidente o por fecha
- Cuidado al importar un feed que no está en el formato MISP



Top correlations index

The values with the most correlation entries.

« previous | next »

Cache age: 2y | Regenerate cache

Value	Excluded	Correlation count	Actions
192.68.2.1	×	132770	
162.248.164.36	×	67222	
45.62.198.89	×	66840	
45.62.198.73	×	63728	
45.62.198.74	×	63056	
45.62.198.243	×	58912	
45.62.198.242	×	58576	
149.56.79.217	×	20666	