

MISP



GSS - Dani Pérez (A-04)

¿Qué es?

La plataforma de intercambio de amenazas MISP es un software gratuito y de código abierto que ayuda a compartir información de inteligencia de amenazas, incluidos los indicadores de seguridad cibernética.

Una plataforma de inteligencia de amenazas para recopilar, compartir, almacenar y correlacionar indicadores de compromiso de ataques dirigidos, inteligencia de amenazas, información de fraude financiero, información de vulnerabilidad o incluso información de lucha contra el terrorismo.

Enlaces de referencia

1. Sitio web: <http://www.misp-project.org/>
2. Imágenes Virtuales: <https://www.circl.lu/misp-images/latest/>
3. Documentación: <https://www.circl.lu/doc/misp/>
4. GitHub: <https://github.com/MISP/>
5. Quick Start: <https://www.circl.lu/doc/misp/quick-start/>
6. Material Training: <https://www.circl.lu/services/misp-training-materials/>

Historia

1. Comenzó alrededor de junio de 2011 por Christophe Vandeplas que lo llamó **CyDefSIG**: Cyber Defense Signatures.
2. A mediados de julio de 2011 presentó su proyecto personal en el trabajo (Defensa belga).
3. Después de dar acceso a **CyDefSIG** ejecutándose en su servidor personal, la Defensa Belga comenzó a usar **CyDefSIG** oficialmente a partir de mediados de agosto de 2011, la OTAN se enteró de este proyecto.
4. Meses después la OTAN contrató a un desarrollador a tiempo completo para mejorar el código y agregar más funciones. A partir de esa fecha se inició un desarrollo colaborativo.
5. El proyecto pasó a llamarse **MISP**: Malware Information Sharing Project, un nombre inventado por Alex Vandurme de la OTAN.

Perfiles



Christophe
Vandeplas



Andrzej Dereszowski



Andras Iklody



Alex Vandurme

<https://www.misp-project.org/contributors/>

Motivadores

- Compartir indicadores de compromiso para una cuestión de detección.

¿Tengo sistemas infectados en mi infraestructura o en los que trabajo?

- Compartiendo indicadores para bloquear.

“Utilizo estos atributos para bloquear o desviar el tráfico”.

- Compartiendo indicadores para realizar inteligencia.

Recopilación de información sobre campañas y ataques. ¿Quién me está apuntando?

¿Quiénes son los enemigos?

Perfiles de los usuarios

- **Analistas de malware:** dispuestos a compartir indicadores.
- **Analistas de seguridad:** buscando, validando y utilizando indicadores en operaciones.
- **Analistas de inteligencia:** reuniendo información sobre adversarios específicos.
- **Equipos de análisis de riesgos:** dispuestos a conocer las nuevas amenazas, probabilidad y ocurrencias.
- **Analistas de fraude:** dispuestos a compartir indicadores financieros para detectar fraudes financieros.

Organizaciones que usan MISP

Las comunidades son grupos de usuarios que comparten dentro de un conjunto de targets/valores.

- **CIRCL** opera múltiples instancias MISP con más de 950 organizaciones y 2400 usuarios.
- **Grupos de confianza** que ejecutan comunidades MISP en modo aislado.
- Sector financiero utilizan MISP como un mecanismo de intercambio.
- **Organizaciones militares e internacionales** (OTAN, militares, CSIRTs, ...)
- Los proveedores de seguridad que ejecutan sus propias comunidades (Fidelis, etc.)
- Interactuar con las comunidades MISP (OTX, etc.)

Dificultades

Compartir las dificultades y amenazas no es realmente un problema técnico difícil, pero a menudo es un problema de confianza entre organizaciones.

Dificultades

Restricciones legales

“Nuestro marco legal no nos permite compartir información”

“El riesgo de fuga de información es demasiado alto y es demasiado arriesgado para nuestra organización o socios”

Restricciones prácticas

“No tenemos información para compartir”

“No tenemos tiempo para procesar o aportar indicadores”

“Nuestro modelo de clasificación no es tu modelo”

“Las herramientas para compartir información están vinculadas a un formato específico, y usamos uno diferente”:

Dificultades 2.0

Tarea de red de CSIRT del anexo I (2)

¿Apoyado por MISP?

- | | |
|--|----|
| (a) (i) seguimiento de incidentes a nivel nacional; | sí |
| (a) (ii) proporcionar alertas tempranas, alertas, anuncios y difusión de información a las partes interesadas pertinentes sobre riesgos e incidentes; | sí |
| (a) (iii) respuesta a incidentes; | sí |
| (a) (iv) proporcionar análisis dinámicos de riesgos e incidentes y conocimiento de la situación; | sí |
| (a) (v) participar en la red de CSIRT. | sí |
| (b) Los CSIRT establecerán relaciones de cooperación con el sector privado. | sí |
| (c) promover la adopción y el uso de prácticas comunes o estandarizadas para los procedimientos de manejo de incidentes y riesgos; esquemas de clasificación de incidentes, riesgos e información. | sí |

<https://misp-project.org/compliance/NISD/>

Más beneficios

- Reutilización de **TTPs** (Tactics, Techniques and Procedures) en todos los sectores.
- Conocer antes de ser golpeado por algo que otro sector ha enfrentado antes.
- Amenazas híbridas: cómo pueden ser cosas aparentemente no relacionadas.
- Interesante para correlacionar.
- Preparar otras comunidades para la capacidad y cultura de compartir.

Creación de Comunidades de Colaboración

- Comenzar una nueva comunidad para compartir es fácil y difícil al mismo tiempo.
- Muchas partes móviles, y lo más importante, se trata de un grupo diverso de personas o instituciones.
- Entendiendo y trabajando con sus electores para ayudarlos a enfrentar sus desafíos es la clave.

Modelos

Diferentes modelos para constituyentes.

- Conectándose a una instancia MISP alojada por un CSIRT.
- Alojando su propia instancia y conectándose al MISP de CSIRT.
- Convertirse en miembro de una comunidad sectorial MISP que está conectada a la comunidad de CSIRT.

Colaboración/Compartir

De todas las comunidades actuales, solamente el 30% de las organizaciones comparte activamente datos.

Conclusiones iniciales

- Las prácticas de intercambio de información provienen del uso y de ejemplos (por ejemplo, aprendizaje por imitación de información compartida).
- MISP es solo una herramienta. Lo relevante son sus políticas y prácticas de intercambio.
- La herramienta debe ser lo más transparente posible para apoyar.

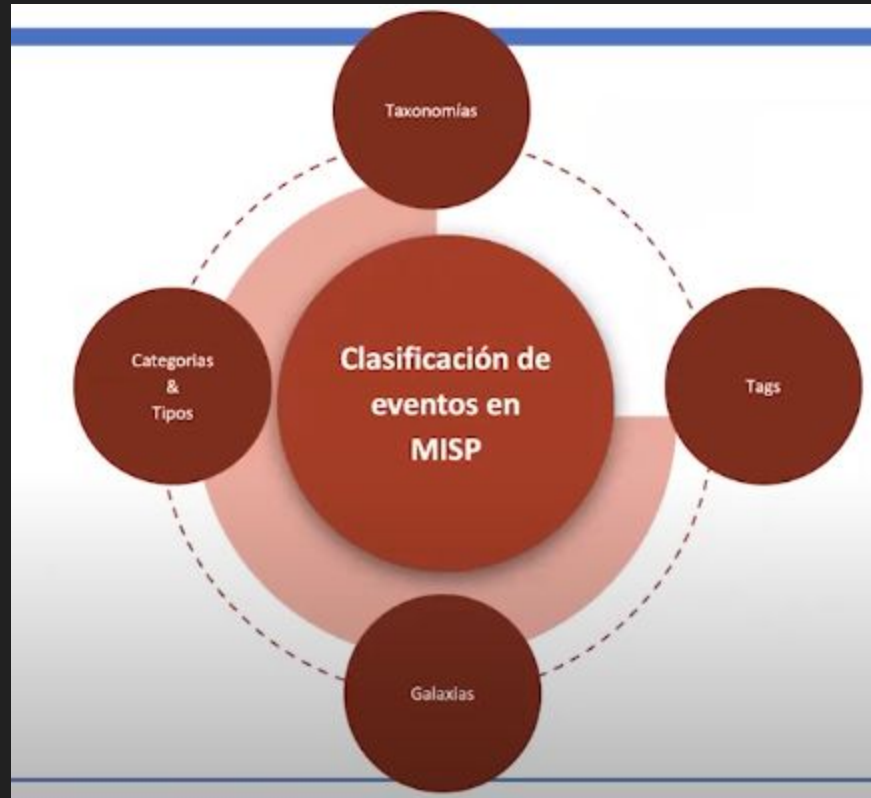
Contenido

- Usuarios
- Organizaciones
- Eventos
- Roles
- Feeds
- Dashboard

¿Y qué es un evento?

No es más que el registro de una muestra con sus IOC (Indicadores de Compromiso) que hayamos descubierto o se nos haya remitido desde un SIEM, IDS o IPS, y así poder correlacionar con nuestra lista de feeds.

Contenido



Contenido 2.0

1. Clasificación de eventos en MISP:
 - a. **Categorías y Tipos**
 - i. **Categoría** -> network activity, financial fraud...
 - ii. **Tipo de atributo** -> md5, filename, hostname, ip-src, ip-dst...
 - b. **Taxonomías** -> listas con contenido de etiquetas.
 - i. **Tags** -> con etiquetas podemos clasificar los eventos
 - c. **Galaxias** -> nos permite agrupar diferentes grupos de eventos (piezas de malware) y entender tendencias de malware.
 - d. **Warning-list** -> nos permite trabajar con falsos positivos (indicadores que no se aplican a nosotros ya que son de otras regiones...).
 - e. **TLP** -> etiqueta por cómo compartir el evento.

Clasificación, etiquetas (Tags) y Taxonomías

[Home](#) [Event Actions](#) [Galaxies](#) [Input Filters](#) [Global Actions](#) [Sync Actions](#) [Administration](#) [Audit](#) ★ **MISP** [Admin](#) [Log out](#)

Warning: MISP is currently disabled for all users. Enable it in Server Settings (Administration -> Server Settings -> MISP tab -> live). An update might also be in progress, you can see the progress in [Update Progress](#)

[List Favourite Tags](#)
[List Tags](#)
[Add Tag](#)

Tags

[« previous](#) [next »](#)

[Simple](#) [Advanced](#)

Enter value to search [Filter](#)

ID	Exportable	Hidden	Name ↓	Restricted to org	Restricted to user	Taxonomy	Tagged events	Tagged attributes	Activity	Favourite	Actions
2	✓	✗	threatmatch-malware-types:malware_type="Adware"	✗	✗	threatmatch-malware-types	0	0		<input type="checkbox"/>	↶ ✎ 🗑
3	✓	✗	threatmatch-malware-types:malware_type="Botnet"	✗	✗	threatmatch-malware-types	0	0		<input type="checkbox"/>	↶ ✎ 🗑
1	✓	✗	tip:amber	✗	✗		1	1		<input type="checkbox"/>	↶ ✎ 🗑

Taxonomías

[Home](#) [Event Actions](#) [Galaxies](#) [Input Filters](#) [Global Actions](#) [Sync Actions](#) [Administration](#) [Audit](#)

Warning: MISP is currently disabled for all users. Enable it in Server Settings (Administration -> Server Settings -> MISP tab -> live). An update might also be in progress, you can see the progress in [Update Progress](#) ✕

[List Taxonomies](#)
[Update Taxonomies](#)

Taxonomies

« previous 1 2 3 next » last »

All Enabled Disabled

Enter value to search Filter

ID	Namespace	Description	Ver
121	workflow	Workflow support language is a common language to support intelligence analysts to perform their analysis on data and information.	10
120	vocabulaire-des-probabilites-estimatives	Ce vocabulaire attribue des valeurs en pourcentage à certains énoncés de probabilité	3
119	veris	Vocabulary for Event Recording and Incident Sharing (VERIS)	2
118	use-case-applicability	The Use Case Applicability categories reflect standard resolution categories, to clearly display alerting rule configuration problems.	1

Taxonomías

THREATMATCH-MALWARE-TYPES Taxonomy Library

ID	111
Namespace	threatmatch-malware-types
Description	The ThreatMatch Malware types are applicable for any ThreatMatch instances and should be used for all CIISI and TIBER Projects.
Version	1
Enabled	Yes (disable)

« previous next »

						Filter	
<input type="checkbox"/> Tag	Expanded	Numerical value	Events	Attributes	Tags	Action	
<input type="checkbox"/>	threatmatch-malware-types:malware_type="Adware"		0	0	threatmatch-malware-types:malware_type="Adware"		
<input type="checkbox"/>	threatmatch-malware-types:malware_type="Backdoor"		N/A	N/A			
<input type="checkbox"/>	threatmatch-malware-types:malware_type="Banking Trojan"		N/A	N/A			
<input type="checkbox"/>	threatmatch-malware-types:malware_type="Botnet"		0	0	threatmatch-malware-types:malware_type="Botnet"		
<input type="checkbox"/>	threatmatch-malware-types:malware_type="Destructive"		N/A	N/A			
<input type="checkbox"/>	threatmatch-malware-types:malware_type="Downloader"		N/A	N/A			
<input type="checkbox"/>	threatmatch-malware-types:malware_type="Exploit Kit"		N/A	N/A			
<input type="checkbox"/>	threatmatch-malware-types:malware_type="Fileless Malware"		N/A	N/A			
<input type="checkbox"/>	threatmatch-malware-types:malware_type="Keylogger"		N/A	N/A			

Taxonomía Threatmatch

Home Event Actions Galaxies Input Filters Global Actions Sync Actions Administration Audit

Warning: MISP is currently disabled for all users. Enable it in Server Settings (Administration -> Server Settings -> MISP tab -> live). A

List Tag Collections

Add Tag Collection

Export Tag Collections

Import Tag Collections

Add Tag Collection

Name

Description

☐ Visible to all orgs

Submit

☐ Tag

☐ threatmatch-malware-types:malware_type="Adware"

☐ threatmatch-malware-types:malware_type="Backdoor"

☐ threatmatch-malware-types:malware_type="Banking Trojan"

☐ threatmatch-malware-types:malware_type="Botnet"

☐ threatmatch-malware-types:malware_type="Destructive"

☐ threatmatch-malware-types:malware_type="Downloader"

☐ threatmatch-malware-types:malware_type="Exploit Kit"

☐ threatmatch-malware-types:malware_type="Fileless Malware"

☐ threatmatch-malware-types:malware_type="Keylogger"

Crear Taxonomías en MISP

```
$ cd /var/www/MISP/app/files/taxonomies/
```

```
$ mkdir privatetaxonomy
```

```
$ cd privatetaxonomy
```

```
$ vi machinetag.json
```

Cree un archivo JSON que describa su taxonomía como etiquetas triples.

For example :

```
mkdir sample
```

```
cd sample
```

```
vim machinetag.json
```

Crear Taxonomías en MISP

MISP taxonomies - Flexible Classification for Information Sharing

MISP taxonomies is a solution to use existing taxonomies (or create your own) to **classify your cybersecurity events, indicators and threats**. This technique is integrated as a default mechanism for tagging in MISP (Malware Information Sharing Platform & Threat Sharing) and to support a distributed classification where organizations can share **common taxonomies in a local or distributed fashion**.

Classifications are distributed as simple JSON files to use with MISP but **can be easily integrated into any other information sharing software**. You can also propose new taxonomies to the community.

Examples of machine tags and human readable tags :

`admiralty-scale:source-reliability="c"`
admiralty-scale:Source Reliability="Fairly reliable"

`admiralty-scale:information-credibility="3"`
admiralty-scale:Information Credibility="Possibly true"

`nato:classification="NU"`
nato:Classification="NATO UNCLASSIFIED"

`tlp:amber`

Traffic Light Protocol:(TLP:AMBER) Information exclusively given to an organization; sharing limited within the organization to be effectively acted upon.

namespace 
predicate 
value 



<https://github.com/MISP/misp-taxonomies/>

Ejemplo de JSON con etiquetas triples.

Puede utilizar el validador JSON para asegurarse de que no haya ningún error de sintaxis.

<https://www.circl.lu/doc/misp/taxonomy/#adding-taxonomy-in-misp>

```
{
  "namespace": "sample",
  "description": "Some descriptive words",
  "version": 1,
  "predicates": [
    {
      "value": "my-predicate",
      "expanded": "my-predicate"
    }
  ],
  "values": [
    {
      "predicate": "my-predicate",
      "entry": [
        {
          "value": "a-value",
          "expanded": "A value"
        }
      ]
    }
  ]
}
```

[Home](#)[Event Actions](#)[Galaxies](#)[Input Filters](#)[Global Actions](#)[Syn](#)

Warning: MISP is currently disabled for all users. Enable it in Server Settings (Administr

[List Taxonomies](#)[Update Taxonomies](#)

Taxonomies

[« previous](#)[1](#)[2](#)[3](#)[next »](#)[last »](#)

[Update Taxonomies](#)

Galaxias

[Home](#) [Event Actions](#) [Galaxies](#) [Input Filters](#) [Global Actions](#) [Sync Actions](#) [Administration](#) [Audit](#)

Warning: MISP is currently disabled for all users. Enable it in Server Settings (Administration -> Server Settings -> MISP tab -> live). An update might also be in progress, you

[List Galaxies](#)
[List Cluster Blocklists](#)
[List Relationships](#)

[Update Galaxies](#)
[Force Update Galaxies](#)

[Import Galaxy Clusters](#)

Galaxy index

[« previous](#) [next »](#)

Galaxy Id ↑	Icon	Name	version
-------------	------	------	---------

Tipos de Atributos y sus Categorías

Attribute Categories and Types

Attribute Categories vs. Types

Category	Internal reference	Targeting data	Antivirus detection	Payload delivery	Artifacts dropped	Payload installation	Persistence mechanism	Network activity	Payload type	Attribution	External analysis	Financial fraud	Support Tool	Social network	Person	Other	Category
md5				X	X	X					X						md5
sha1				X	X	X					X						sha1
sha256				X	X	X					X						sha256
filename				X	X	X	X				X						filename
pdb					X												pdb
filename md5				X	X	X					X						filename md5
filename sha1				X	X	X					X						filename sha1
filename sha256				X	X	X					X						filename sha256
ip-src				X				X			X						ip-src
ip-dst				X				X			X						ip-dst
hostname				X				X			X						hostname

Categorías

Categories

Category	Description
Internal reference	Reference used by the publishing party (e.g. ticket number)
Targeting data	Targeting information to include recipient email, infected machines, department, and or locations.
Antivirus detection	List of anti-virus vendors detecting the malware or information on detection performance (e.g. 13/43 or 67%). Attachment with list of detection or link to VirusTotal could be placed here as well.
Payload delivery	Information about the way the malware payload is initially delivered, for example information about the email or web-site, vulnerability used, originating IP etc. Malware sample itself should be attached here.
Artifacts dropped	Any artifact (files, registry keys etc.) dropped by the malware or other modifications to the system
Payload installation	Location where the payload was placed in the system and the way it was installed. For example, a filename md5 type attribute can be added here like this: c:\windows\system32\malicious.exe 41d8cd98f00b204e9800998ecf8427e
Persistence mechanism	Mechanisms used by the malware to start at boot. This could be a registry key, legitimate driver modification, LNK file in startup
Network activity	Information about network traffic generated by the malware
Payload type	Information about the final payload(s). Can contain a function of the payload, e.g. keylogger, RAT, or a name if identified, such as Poison Ivy.
Attribution	Identification of the group, organisation, or country behind the attack
External analysis	Any other result from additional analysis of the malware like tools output Examples: pdf-parser output, automated sandbox analysis, reverse engineering report.
Financial fraud	Financial Fraud indicators, for example: IBAN Numbers, BIC codes, Credit card numbers, etc.
Support Tool	Tools supporting analysis or detection of the event
Social network	Social networks and platforms
Person	A human being - natural person
Other	Attributes that are not part of any other category or are meant to be used as a component in MISP objects in the future

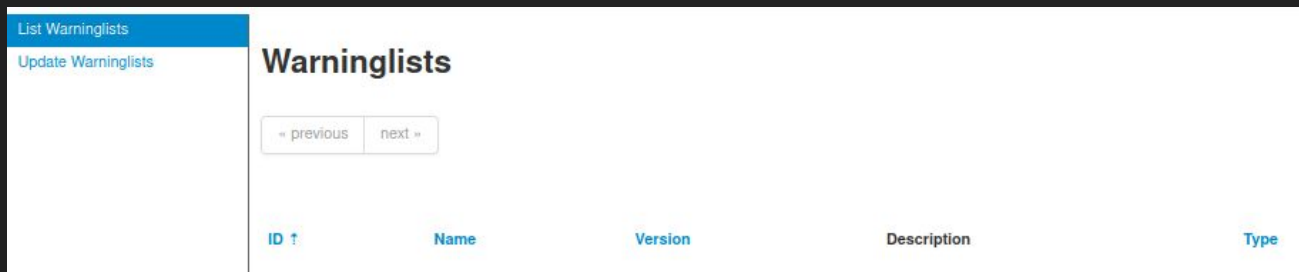
Tipos

Types

Type	Description
md5	You are encouraged to use filename md5 instead. A checksum in md5 format, only use this if you don't know the correct filename
sha1	You are encouraged to use filename sha1 instead. A checksum in sha1 format, only use this if you don't know the correct filename
sha256	You are encouraged to use filename sha256 instead. A checksum in sha256 format, only use this if you don't know the correct filename
filename	Filename
pdb	Microsoft Program database (PDB) path information
filename md5	A filename and an md5 hash separated by a (no spaces)
filename sha1	A filename and an sha1 hash separated by a (no spaces)
filename sha256	A filename and an sha256 hash separated by a (no spaces)
ip-src	A source IP address of the attacker
ip-dst	A destination IP address of the attacker or C&C server. Also set the IDS flag on when this IP is hardcoded in malware
hostname	A full host/dnsname of an attacker. Also set the IDS flag on when this hostname is hardcoded in malware
domain	A domain name used in the malware. Use this instead of hostname when the upper domain is important or can be used to create links between events.
domain ip	A domain name and its IP address (as found in DNS lookup) separated by a (no spaces)
email	An e-mail address
email-src	The source email address. Used to describe the sender when describing an e-mail.
eppn	eduPersonPrincipalName - eppn - the NetId of the person for the purposes of inter-institutional authentication. Should be stored in the form of user@univ.edu, where univ.edu is the name of the local security domain.
email-dst	The destination email address. Used to describe the recipient when describing an e-mail.
email-subject	The subject of the email

Falsos positivos

Las listas de advertencias erróneas son listas de indicadores bien conocidos que pueden asociarse a posibles falsos positivos, errores o equivocaciones.



The screenshot shows the MISP Warninglists management interface. On the left is a sidebar with 'List Warninglists' (active) and 'Update Warninglists'. The main area is titled 'Warninglists' and contains navigation buttons for '« previous' and 'next »'. Below these is a table with the following headers: ID (with a sort icon), Name, Version, Description, and Type.

ID ↑	Name	Version	Description	Type
------	------	---------	-------------	------

Están integradas en MISP para mostrar un cuadro de información/advertencia a nivel de evento y atributo si dichos indicadores están disponibles en una de las listas. Las listas también se utilizan para filtrar posibles falsos positivos a nivel de API. La lista se puede habilitar o deshabilitar globalmente en MISP siguiendo las prácticas de la organización.

<https://github.com/MISP/misp-warninglists>

TLP

Traffic Light Protocol (TLP) es un esquema creado para fomentar un mejor intercambio de información sensible (pero no clasificada) en el ámbito de la seguridad de la información.

<https://www.circl.lu/pub/traffic-light-protocol/>

<https://www.incibe-cert.es/tlp>

TLP

Código	Cuándo utilizarlo	Cómo compartirlo	Color	Fondo
TLP:RED	Se debe utilizar TLP:RED cuando la información está limitada a personas concretas, y podría tener impacto en la privacidad, reputación u operaciones si es mal utilizada.	Los receptores no deben compartir información designada como TLP:RED con ningún tercero fuera del ámbito donde fue expuesta originalmente.	#ff0033	#000000
TLP:AMBER	Se debe utilizar TLP:AMBER cuando la información requiere ser distribuida de forma limitada, pero supone un riesgo para la privacidad, reputación u operaciones si es compartida fuera de la organización.	Los receptores pueden compartir información indicada como TLP:AMBER únicamente con miembros de su propia organización que necesitan conocerla, y con clientes, proveedores o asociados que necesitan conocerla para protegerse a sí mismos o evitar daños. El emisor puede especificar restricciones adicionales para compartir esta información.	#ffc000	#000000
TLP:GREEN	Se debe utilizar TLP:GREEN cuando la información es útil para todas las organizaciones que participan, así como con terceros de la comunidad o el sector.	Los receptores pueden compartir la información indicada como TLP:GREEN con organizaciones afiliadas o miembros del mismo sector, pero nunca a través de canales públicos.	#33ff00	#000000
TLP:WHITE	Se debe utilizar TLP:WHITE cuando la información no supone ningún riesgo de mal uso, dentro de las reglas y procedimientos establecidos para su difusión pública.	La información TLP:WHITE puede ser distribuida sin restricciones, sujeta a controles de Copyright.	#ffffff	#000000

Feeds

Proporcionan una manera de intercambio de información a través de cualquier mecanismo de transporte (HTTP, TLS, USB, etc.)

- Vista previa de eventos junto con sus atributos, objetos
- Seleccionar e importar eventos

Ventajas:

- Funcionan sin necesidad de sincronización MISP
- Pueden producirse sin una instancia MISP

Feeds

Warning: MISP is currently disabled for all users. Enable it in Server Settings (Administration -> Server Settings -> MISP tab -> live). An update might also be in progress, you can see the progress in [Update Progress](#)

List Feeds

[Search Feed Caches](#)

[Add Feed](#)

[Import Feeds from JSON](#)

[Feed overlap analysis matrix](#)

[Export Feed settings](#)

Feeds

Generate feed lookup caches or fetch feed data (enabled feeds only)

[Load default feed metadata](#) [Cache all feeds](#) [Cache freetext/CSV feeds](#) [Cache MISP feeds](#) [Fetch and store all feed data](#)

[← previous](#) [next →](#)

[Default feeds](#) [Custom feeds](#) [All feeds](#) [Enabled feeds](#)

[Filter](#)

<input type="checkbox"/>	Id	Enabled	Caching	Name	Format	Provider	Org	Source	URL	Headers	Target	Publish	Delta	Override	Distribution	Tag	Visible	Caching	Actions
<input type="checkbox"/>	1	✗	✗	CIRCL OSINT Feed	misp	CIRCL		network	https://www.circl.lu/doc/misp/feed-osint		Feed not enabled	✗	✗	✗	All communities		✗	Not cached	🔍 📄 🗑️
<input type="checkbox"/>	2	✗	✗	The Botvrij.eu Data	misp	Botvrij.eu		network	https://www.botvrij.eu/data/feed-osint		Feed not enabled	✗	✗	✗	All communities		✗	Not cached	🔍 📄 🗑️

Page 1 of 1, showing 2 records out of 2 total, starting on record 1, ending on 2

[← previous](#) [next →](#)

Dashboard

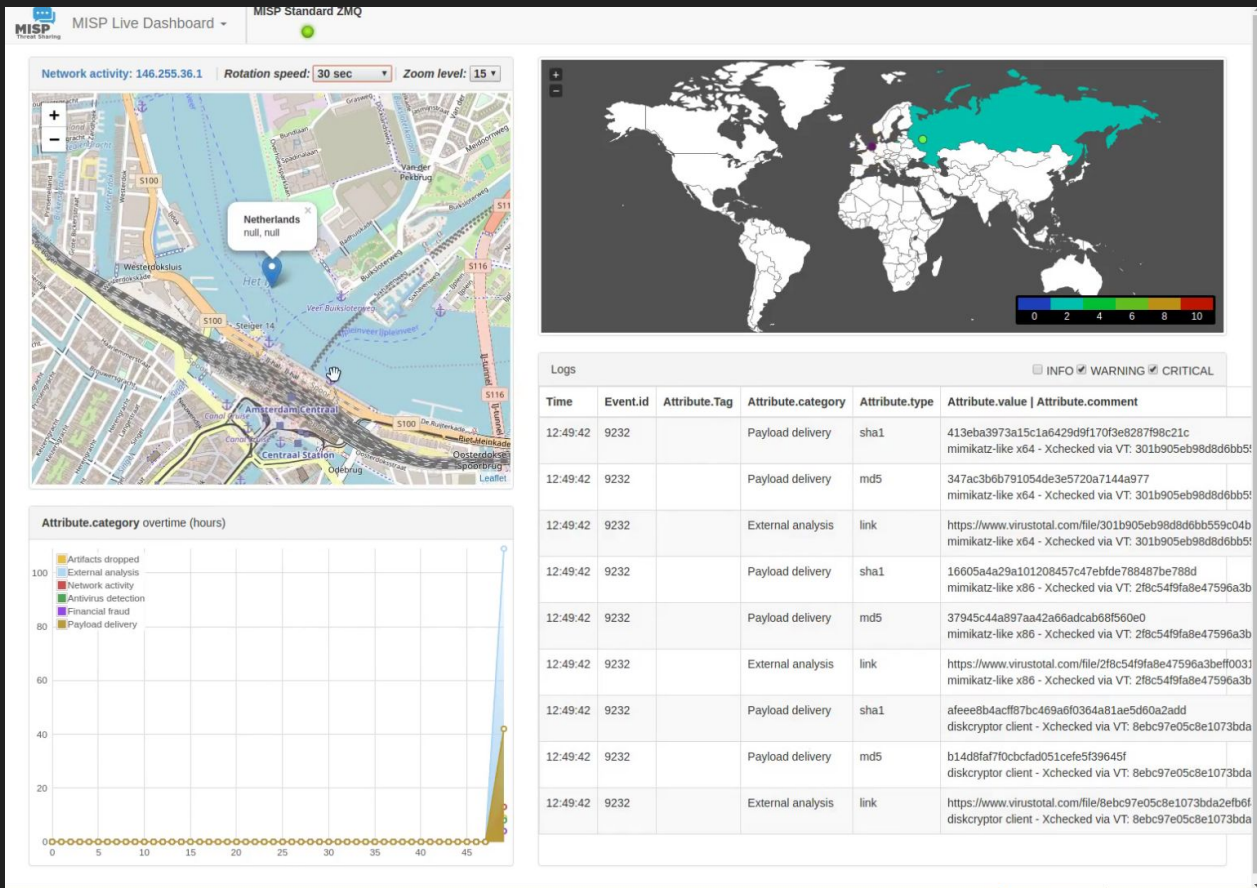
MISP tiene un módulo que permite ver datos de eventos, de uso y participación de forma gráfica.

Está deshabilitado en la instalación standard debido a algunos bugs.

Podemos instalarlo de forma independiente.

Durante los ejercicios cibernéticos para realizar un seguimiento de lo que se está procesando en sus diversas instancias de MISP.

<https://github.com/MISP/misp-dashboard>



Sizer

Dimensionamiento de los Servidores
en MISP

<https://misp-project.org/MISP-sizer/>

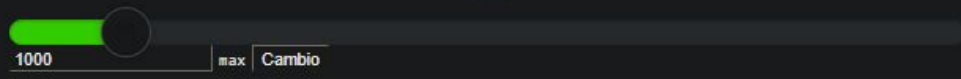
GRAIL CYBER TECH



Medidor de hardware MISP (calculadora)

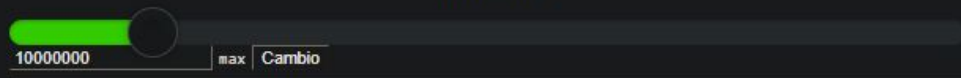
Número de usuarios:

100



Número de atributos (= valores de campo):

1300000



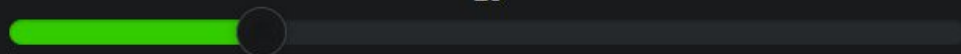
Porcentaje de atributos que se correlacionan / superponen:

0%: atributos de texto libre de OSINT sin posibilidad de que dos atributos en la base de datos tengan el mismo valor.

50%: un campo de atributo dado tendrá el mismo valor en el 50% de los eventos (ya es un caso de gran valor, raro y costoso).

Si se desconoce, déjelo al 25%, que actualmente es un buen promedio.

25



RAM resultante: 20

GB

DISCO resultante: 1314

GB

CPU resultante: 3

* Núcleo (s) de vCPU (nivel Intel Xeon)

[README.txt](#) - [Página de GitHub](#) - [GitHub MISP](#) - [Página principal del proyecto](#)

Instalación

Servidor Ubuntu 18.04

Please check the installer options first to make the best choice for your install

```
wget -O /tmp/INSTALL.sh https://raw.githubusercontent.com/MISP/MISP/2.4/INSTALL/INSTALL.sh
```

```
bash /tmp/INSTALL.sh
```

This will install MISP Core

```
wget -O /tmp/INSTALL.sh https://raw.githubusercontent.com/MISP/MISP/2.4/INSTALL/INSTALL.sh
```

```
bash /tmp/INSTALL.sh -c
```

<https://misp.github.io/MISP/INSTALL.ubuntu1804>

Hardening

Medidas genéricas:

- Seguridad física
- Seguridad de red: Server Proxy, Firewall, IDS/IPS, ACLs, etc.
- SSL/TLS.
- Uso de certificados.

Backups

- **Archivos de configuración de MISP:** /var/www/MISP/app/Config/*
- **Claves de cifrado:** /var/www/MISP/.gnupg
- **Configuración de Apache:** /etc/apache2/sites-enabled/misp-ssl
- **Apache PHP config:** /etc/php5/apache2/php.ini
- **Certificados SSL:** /etc/ssl/private/*
- **Dump de BBDD:** mysqldump -u misp -p misp > misp_db_bkp.sql.dump
- Información de personalización:
 - /var/www/MISP/app/webroot/img/orgs
 - /var/www/MISP/app/webroot/img/custom
 - /var/www/MISP/app/files