

Documentacion de MISP

Para realizar la instalacion de misp tendremos que bajarnos un script con la instalacion de misp en un servidor y meterlo en la carpeta tmp

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

Una vez lo tengamos descargado, ejecutaremos el script

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

Nada mas ejecutarlo nos pedira, que modo de instalación de misp queremos realizar

Con la opcion -A nos realizara una instalacion completa y desatendida

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

Tardara un tiempo en instalar pero una vez instalado nos saldra un resumen de todas las contraseñas generadas de los distintos servicios o cuentas.

```
usuario@ubuntu: ~/Downloads/MISP-2.4/INSTALL
File Edit View Search Terminal Help
#####
##### (88%)
#####
Admin (root) DB Password: 4656d556007c015724ee1c607e485f4f1d6b535747b9e97c5273dfa0304c17dd
User (misp) DB Password: b0bcdcf338d28b4abeb197d4795f1abe47a8b233804e78c3e72193f6cfdb9e8cd
Authkey: bWttZv33dWDDZzenpS2VH4157xQbeoe0yJee00cj
-----
MISP Installed, access here:
User: admin@admin.test
Password: admin
-----
The following files were created and need either protection or removal (shred on the CLI)
/home/misp/mysql.txt
Contents:
Admin (root) DB Password: 4656d556007c015724ee1c607e485f4f1d6b535747b9e97c5273dfa0304c17dd
User (misp) DB Password: b0bcdcf338d28b4abeb197d4795f1abe47a8b233804e78c3e72193f6cfdb9e8cd
/home/misp/MISP-authkey.txt
Contents:
Authkey: bWttZv33dWDDZzenpS2VH4157xQbeoe0yJee00cj
-----
The LOCAL system credentials:
User: misp
Password: 0a9e78d264d946923cb1ddf2c9c56fc372e76de8d662508ce9ec44ea12b76705 # Or the password you used of your custom user
-----
GnuPG Passphrase is: 29e7ed5f89c635f2ae5b7a127441a9cae767b0bdf056328279308e8f5ced2d52
-----
To enable outgoing mails via postfix set a permissive SMTP server for the domains you want to contact:
sudo postfix -s localhost -u user1 user1
```

tambien tener en cuenta que se nos generará un usuario de sistema con uid(misp) el cual su contraseña es bastante larga y seria recomendable cambiarla desde dicha cuenta o con sudo passwd misp



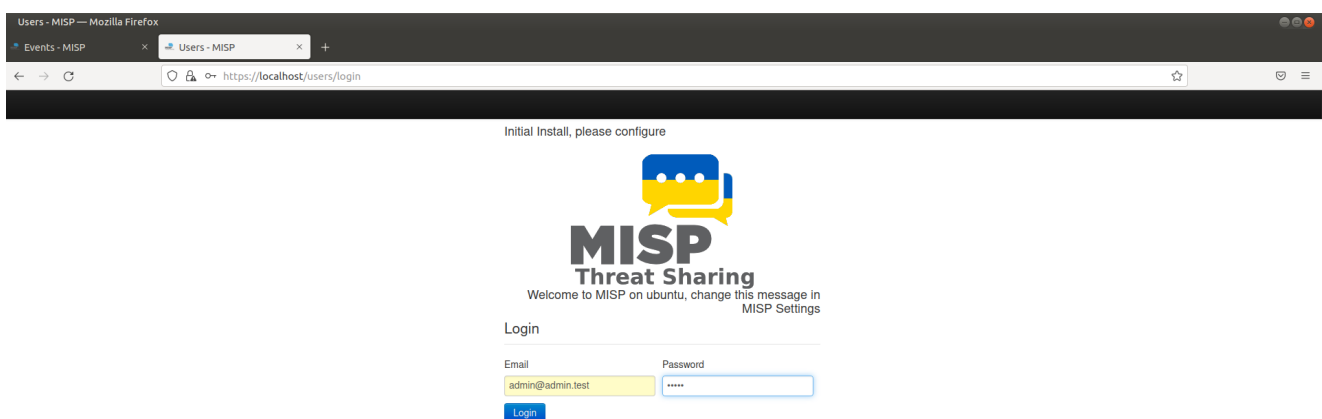
```
Menu
usuario@ubuntu: ~
File Edit View Search Terminal Help
usuario@ubuntu:~$ sudo passwd misp
[sudo] password for usuario:
New password:
Retype new password:
passwd: password updated successfully
usuario@ubuntu:~$
```

Para acceder a MISP una vez instalado, con ip/localhost en un navegador

--- Credenciales: ---

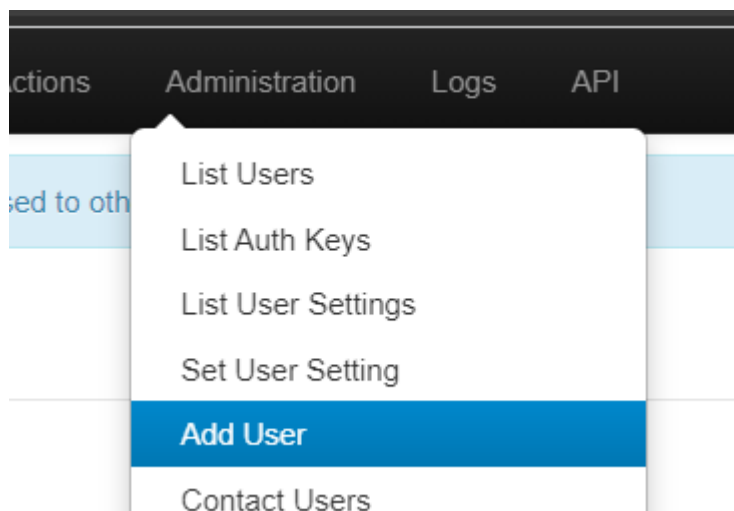
user: admin@admin.test

passowrd: admin



Creacion de usuarios en MISP

Para crear un usuario en MISP sería Administration⇒ Add User



Donde podremos asignar a que tipo de organizacion, email, contraseña y rol va a tener dentro de MISP

Admin Add User

Email

☒ Set password

Password ⓘ

Confirm Password

Organisation

Role

admin

Org Admin

User

Publisher

Sync user

Read Only

NIDS SID

Part of the user's PID key here or try to retrieve it from the CIRCL key server by

Para añadir un evento MISP

Tendremos que ir a home \Rightarrow add event

List Events

Add Event

Import from...

REST client

List Attributes

Search Attributes

View Proposals

Events with proposals

View delegation requests

Export

Automation

Add Event

Date

Distribution ⓘ

2022-03-29

This community only ▾

Threat Level ⓘ

Analysis ⓘ

Low ▾

Ongoing ▾

Event Info

Malicious IPs

Extends Event

Event UUID or ID. Leave blank if not applicable.

Submit

Dentro de añadir un evento, especificando la **distribucion del evento, el nivel de amenaza, y el análisis de la amenaza**

Add attribute

Attribute warning: This event doesn't contain any attribute. It's strongly advised to populate the event with attributes (indicators, observables or information).

« previous next » [view all](#)

Discussion

Para añadir informacion de la amenaza, daremos a "Add attribute"

Dentro de El Atributo, añadiremos la categoría de la información y el tipo, (El nuestro al ser IPs maliciosas)

El tipo de categoría seía **network activity**
y el Tipo, **ip-src**

Tambien podemos añadir, en que fecha se han divisado dicha amenaza

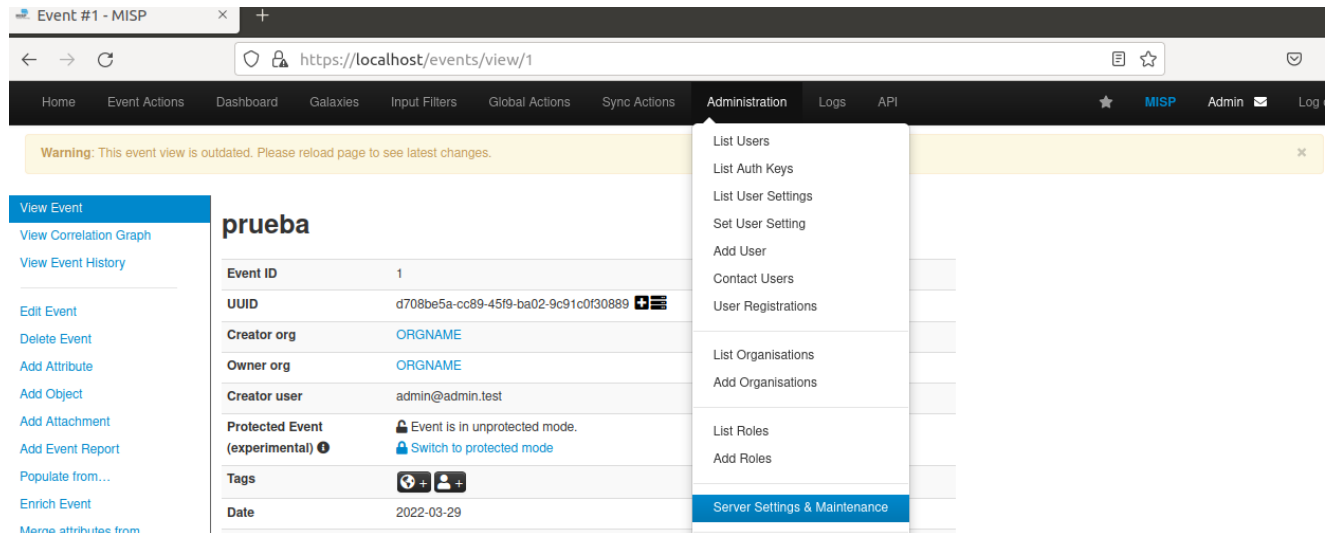
Y como vemos se añadirá.

Scope toggle Deleted Decay score SightingDB Context Related Tags Filtering tool														Enter value to search			
<input type="checkbox"/>	Date ↑	Org	Category	Type	Value	Tags	Galaxies	Comment	Correlate	Related Events	Feed hits	IDB	Distribution	Sightings	Activity	Actions	
<input type="checkbox"/>	2022-03-29		Network activity	ip-dst	160.243.95.154 🔍								Inherit	(0/0)			
<input type="checkbox"/>	2022-03-29		Network activity	ip-dst	192.204.128.198 🔍								Inherit	(0/0)			
<input type="checkbox"/>	2022-03-29		Network activity	ip-dst	36.164.91.203 🔍								Inherit	(0/0)			
<input type="checkbox"/>	2022-03-29		Network activity	ip-dst	141.184.52.126 🔍								Inherit	(0/0)			
<input type="checkbox"/>	2022-03-29		Network activity	ip-dst	126.78.76.60 🔍								Inherit	(0/0)			
<input type="checkbox"/>	2022-03-29		Network activity	ip-dst	65.175.128.132 🔍								Inherit	(0/0)			
<input type="checkbox"/>	2022-03-29		Network activity	ip-dst	172.225.21.16 🔍								Inherit	(0/0)			
<input type="checkbox"/>	2022-03-29		Network activity	ip-dst	0.230.240.118 🔍								Inherit	(0/0)			
<input type="checkbox"/>	2022-03-29		Network activity	ip-dst	116.35.53.133 🔍								Inherit	(0/0)			
<input type="checkbox"/>	2022-03-29		Network activity	ip-dst	79.59.39.81 🔍								Inherit	(0/0)			
<input type="checkbox"/>	2022-03-29		Network activity	ip-src	10.33.110.41 🔍							<input type="checkbox"/>	Inherit	(0/0)			

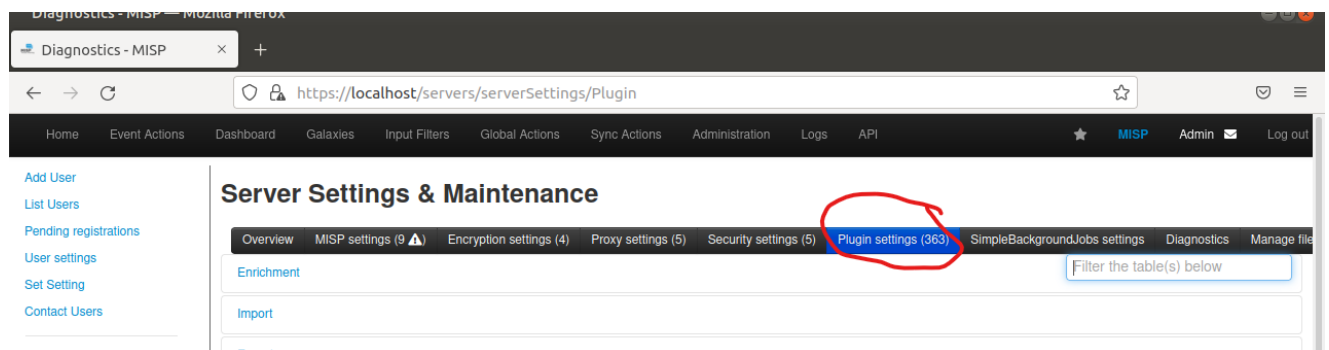
instalacion de pluggins

es interesante recalcar que podemos meter plugins a la plataforma lo cual nos permite hacer desde cosas especificas como relacionar eventos o sus atributos a otros como poder hacer que los eventos se retro-alimenten añadiendo cuando sea necesario nuevos atributos("amenazas"), y se conseguiria de la siguiente manera

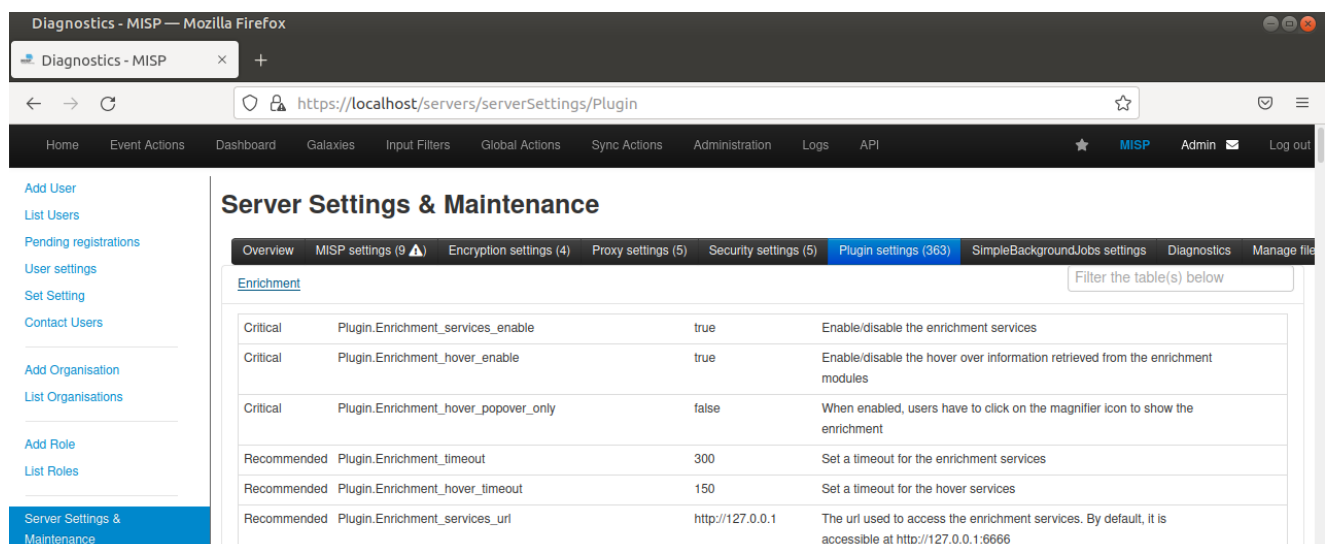
primero nos dirigimos a ajustes de servidor y mantenimiento



luego le damos a ajustes de pluggins



despues clicamos en la primera opcion (enrichment) y nos saldra una lista de las cuales podemos activar las que necesitemos y no sean de pago



en este caso se activaran 2 pluggins los cuales seran:

Recommended	Plugin.Enrichment_dns_enabled	<div> <div>true</div> <div>▼</div> </div>	Enable or disable the dns module.	
Recommended	Plugin.Enrichment_dns_restrict	<div> <div>false</div> <div>▼</div> </div> <div> <div>true</div> <div>▼</div> </div>	Restrict the dns module to the given organisation.	Value not set.

Recommended	Plugin.Enrichment_uriscan_enabled	<div> <div>true</div> <div>▼</div> </div>	Enable or disable the uriscan module.	
Recommended	Plugin.Enrichment_uriscan_restrict	<div> <div>No organisation</div> <div>▼</div> </div> <div> <div>✓</div> <div>✕</div> </div>	Restrict the uriscan module to the given organisation.	Value not set.

estos plugins nos permitiran por ejemplo en el caso de un evento, añadir un nombre de dominio como atributo y que su ip se añada automaticamente o en el caso del segundo pluggin que cuando lo utilizemos nos avisaria de todas las url relacionadas con dicho atributo. asi en seleccion del usuario se podria abarcar un amplio abanico de posibilidades.

un ejemplo de esto seria:

The screenshot shows the MISP (Malware Incident Response System) interface. At the top is a navigation bar with links like Home, Event Actions, Dashboard, Galaxies, Input Filters, Global Actions, Sync Actions, Administration, Logs, and API. Below this is a header for an event page with buttons for « previous, next », and view all. A toolbar contains icons for adding, deleting, and filtering. A table lists various attributes with columns: Date, Org, Category, Type, Value, Tags, Galaxies, Comment, Correlate, Related Events, Feed hits, IDS, and Distribution. A red warning banner states: "Attribute warning: This event doesn't contain any attribute. It's strongly advised to populate the event with attributes (indicators, observables or information) to provide a meaningful event." Below the table is a discussion section with buttons for Quote, Event, Thread, Link, and Code.

añadiría ahora el dns de google.com

Add Attribute

Category ⓘ

Network activity

▼

Type ⓘ

domain

▼

Distribution ⓘ

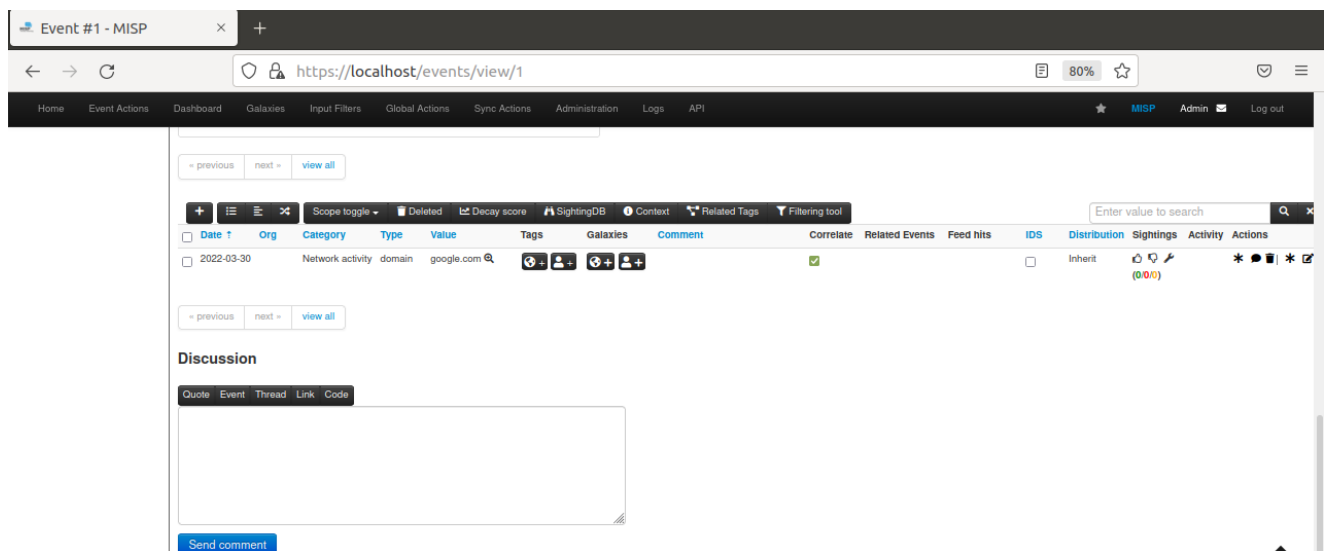
Inherit event

▼

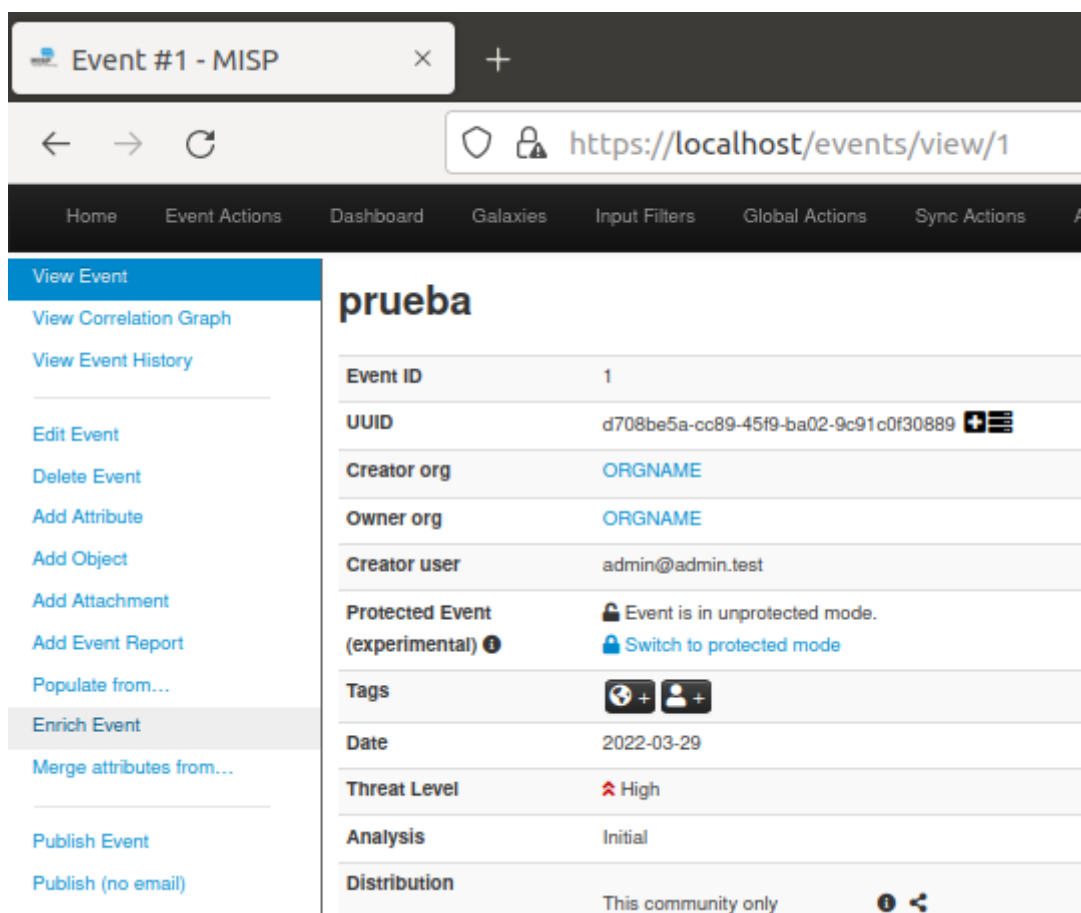
Value

google.com

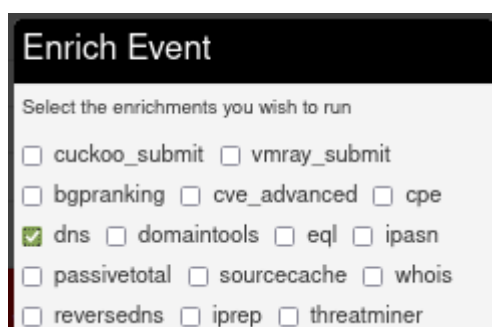
una vez añadido se mostraria solo en dns



iríamos a la parte de arriba del evento y clicariamos a la izquierda en enrich event



entonces saltaria una ventana la cual nos muestra todos los pluggins instalados en este caso hay mas de los necesarios pero solo daremos clic a dns:



despues de darle y aceptar refrescamos la pagina y se puede apreciar la aparicion de otro atributo el cual es una ip y pertenece al dominio agregado anteriormente

Event #1 - MISP

Attributes saved.

Enrichment task queued for background processing. Check back later to see the results.

View Event

View Correlation Graph

View Event History

Edit Event

Delete Event

Add Attribute

Add Object

Add Attachment

Add Event Report

Populate from...

prueba

Event ID 1

UUID d708be5a-cc89-45f9-ba02-9c91c0f30889

Creator org ORGNAME

Owner org ORGNAME

Creator user admin@admin.test

Protected Event (experimental) Event is in unprotected mode. Switch to protected mode

Tags

Download: PGP public key

This is an initial install Powered by MISP 2.4.157 Please configure and harden accordingly - 2022-03-30 01:31:16

Event #1 - MISP — Mozilla Firefox

Event #1 - MISP

« previous next » view all

Scope toggle Deleted Decay score SightingDB Context Related Tags Filtering tool

Date	Org	Category	Type	Value	Tags	Galaxies	Comment	Correlate	Related Events	Feed hits	IDS
2022-03-30		Network activity	ip-src	142.250.200.78			Attribute #7 enriched by dns.	✓			
2022-03-30		Network activity	domain	google.com				✓			

« previous next » view all

Discussion

Una vez tengamos un lista de ips podremos guardar el evento y publicarlo

Publish Event

Publish (no email)

Contact Reporter

Download as...

List Events

Add Event

Y si nos vamos a la home, tendremos nuestro evento publicado

Events

« previous next »

My Events Org Events

Published	Creator org	Owner org	ID	Clusters	Tags	#Attr	#Corr	Creator user	Date	Last modified at	Info
✓	ORGNAME	ORGNAME	1		osint:source-type=block-or-filter-list	11		admin@admin.test	2022-03-29	2022-03-29 03:06:53	IPs maliciosas

Exportar / Importar eventos

para exportar eventos lo recomendable es descargar el evento que queremos exportar en este caso uno de prueba que contiene 4 atributos simples

Events

« previous next »

Filters: Org: 1 x My Events Org Events

Enter value to search Filter

	Published	Creator org	Owner org	ID	Clusters	Tags	#Attr	#Corr	Creator user	Date	Last modified at	Info	Distribution	Actions
<input type="checkbox"/>	x	ORGNAME	ORGNAME	1			2		admin@admin.test	2022-03-29	2022-03-30 01:27:07	prueba	Community	+ - x o

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

al entrar al evento podemos apreciar un menu a la izquierda el cual tiene la opcion de descargar el evento ("download as....")

Event #1 - MISP — Mozilla Firefox

Event #1 - MISP

https://localhost/events/view/1

View Event

View Correlation Graph

View Event History

Edit Event

Delete Event

Add Attribute

Add Object

Add Attachment

Add Event Report

Populate from...

Enrich Event

Merge attributes from...

Publish Event

Publish (no email)

Contact Reporter

Download as...

List Events

Add Event

prueba

Event ID	1
UUID	d708be5a-cc89-45f9-ba02-9c91c0f30889
Creator org	ORGNAME
Owner org	ORGNAME
Creator user	admin@admin.test
Protected Event (experimental)	Event is in unprotected mode. Switch to protected mode
Tags	+ - x o
Date	2022-03-29
Threat Level	High
Analysis	Initial
Distribution	This community only
Warnings	Contextualisation: Your event has neither tags nor galaxy clusters attached - generally adding context to an event allows for quicker decision making and more accurate filtering, it is highly recommended that you label your events to the best of your ability.
Info	prueba
Published	No
#Attributes	2 (0 Objects)

si clicamos en el el nos mostrara varias opciones

Choose the format that you wish to download the event in

MISP XML (metadata + all attributes)	Encode Attachments <input checked="" type="checkbox"/>
MISP JSON (metadata + all attributes)	Encode Attachments <input checked="" type="checkbox"/>
OpenIOC (all indicators marked to IDS)	
CSV (event not published, IDS flag ignored)	
CSV with additional context	Include non-IDS marked attributes <input type="checkbox"/>
STIX 1 XML (metadata + all attributes)	Encode Attachments <input type="checkbox"/>
STIX 1 JSON (metadata + all attributes)	Encode Attachments <input type="checkbox"/>
STIX 2	Encode Attachments <input type="checkbox"/>
RPZ Zone file	
Download Suricata rules	
Download Snort rules	
Download Bro rules	

Cancel

la que nos interesaria para poder pasar eventos desde un modo practico seria en formato JSON. Aunque tambien se puede usar otros formatos como csv que se podrian implementar con otros servicios o plataformas como ELK que veremos mas adelante.....

una vez seleccionada la opcion se descargaria con el formato seleccionado por ejemplo en el caso de JSON:

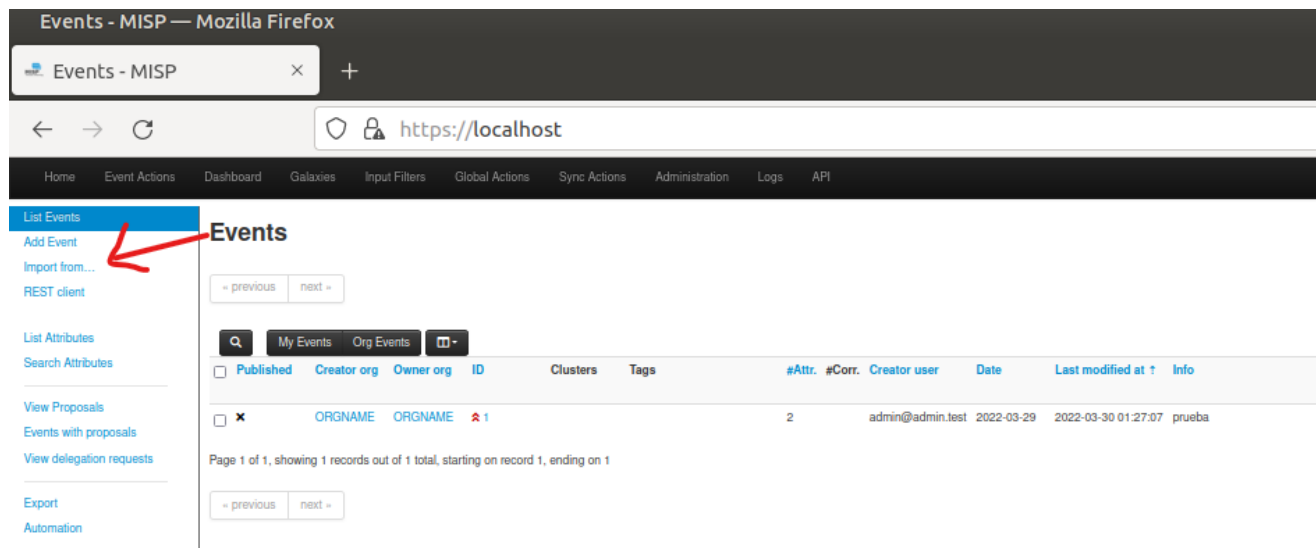
A screenshot of a Pluma text editor window. The title bar reads "misp.event.1.json (~/.Downloads) - Pluma". The menu bar includes "File", "Edit", "View", "Search", "Tools", "Documents", and "Help". The toolbar contains icons for file operations (Open, Save, Print), editing (Undo, Cut, Copy, Paste), and search (Find, Replace). The active tab is "misp.event.1.json". The editor content shows a JSON file with the following structure:

```
1 {"response": [{"Event":  
  {"id": "1", "orgc_id": "1", "org_id": "1", "date": "2022-03-29", "threat_level":  
    "cc89-45f9-ba02-9c91c0f30889", "attribute_count": "2", "analysis": "0", "timestamp": "  
    {"id": "1", "name": "ORGNAME", "uuid": "162592d3-6433-4a8b-8f2b-76da4d3c5c  
    {"id": "1", "name": "ORGNAME", "uuid": "162592d3-6433-4a8b-8f2b-76da4d3c5c  
    [{"id": "7", "type": "domain", "category": "Network  
    activity", "to_ids": false, "uuid": "5d811c16-6f5a-4906-  
    a2e1-0fc80e3ae86a", "event_id": "1", "distribution": "5", "timestamp": "164  
    [], "ShadowAttribute": []}, {"id": "8", "type": "ip-  
    src", "category": "Network  
    activity", "to_ids": false, "uuid": "1728c8da-4b45-4b74-  
    be41-4732389b6248", "event_id": "1", "distribution": "5", "timestamp": "164  
    #7 enriched by  
    dns.", "sharing_group_id": "0", "deleted": false, "disable_correlation": fa  
    [], "ShadowAttribute": []}], "ShadowAttribute": [], "RelatedEvent":  
    [], "Galaxy": [], "Object": [], "EventReport": [], "CryptographicKey":  
    []}]}
```

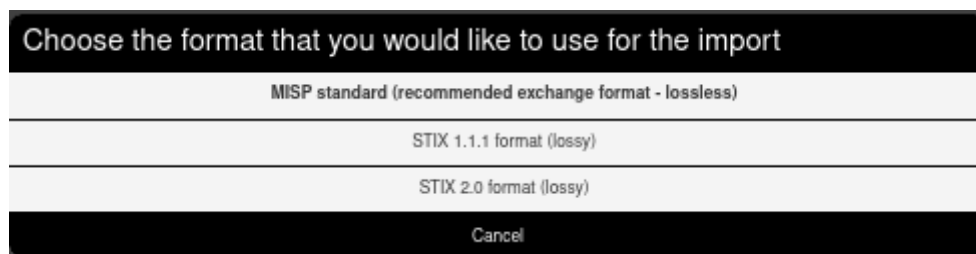
The status bar at the bottom shows a green progress bar.

para importar eventos tenemos que tener en cuenta una cosa y es que los archivos/eventos a importar tienen que tener un formato xml o json. y se realizaria de la siguiente manera:

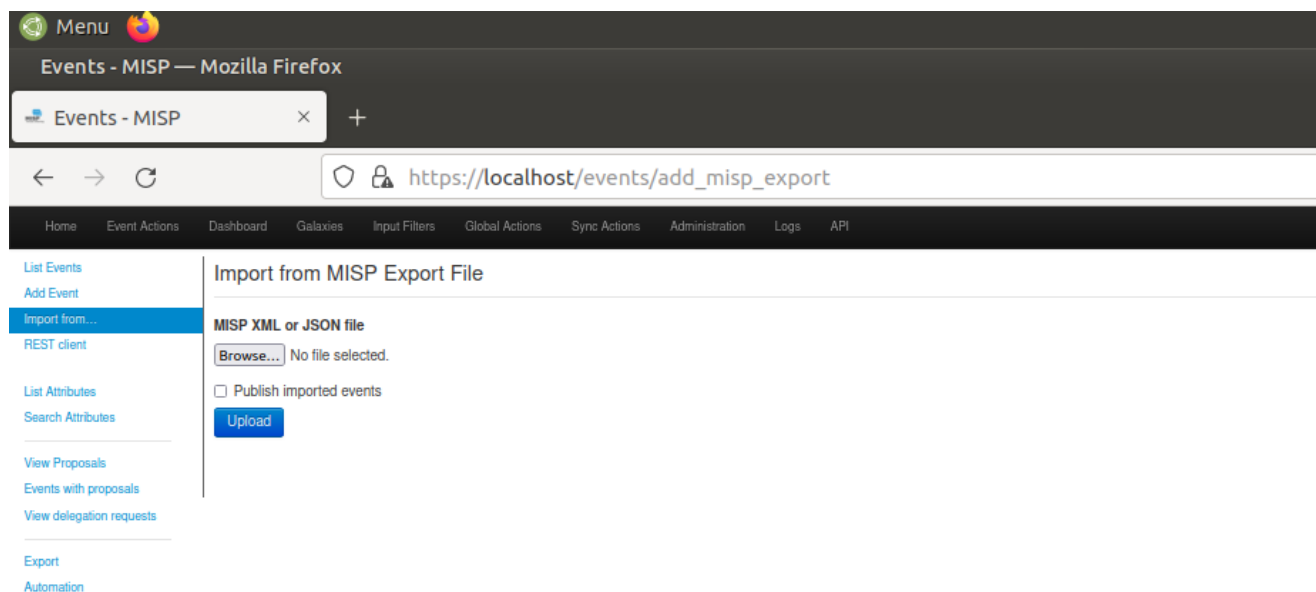
desde el home de misp veremos la opcion de import from("importar desde")



cuando le demos nos pedira un formato

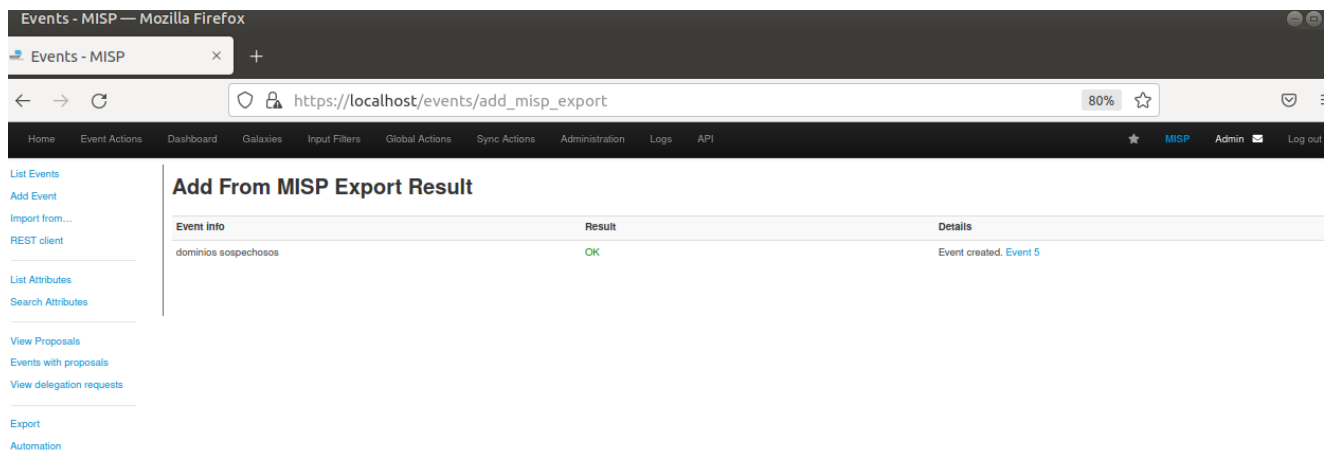


en este caso vamos a probar a seleccionar el formato MISP que se basa en xml/json

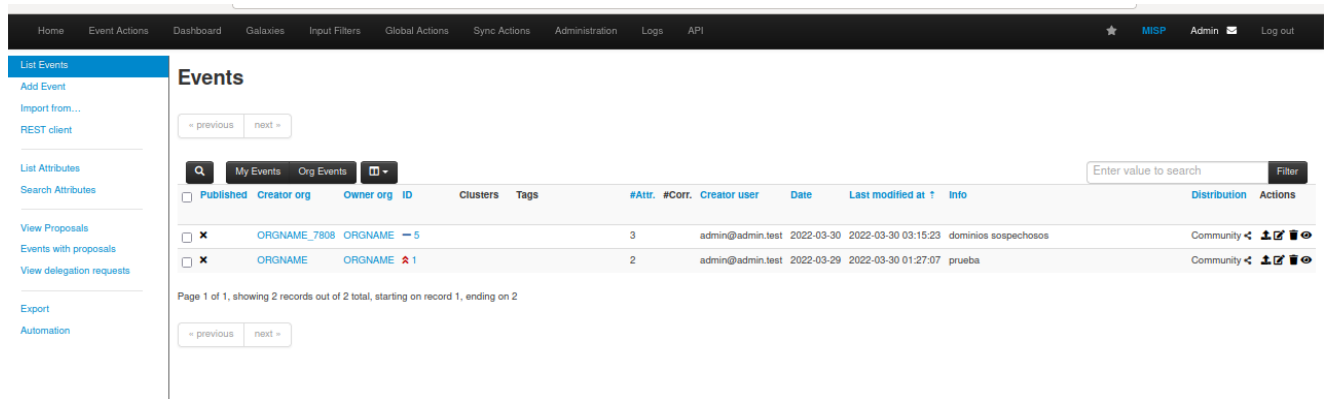


se puede ver que tambien se puede publicar a la hora de importar

una vez le demos a upload nos mostrara los eventos importados



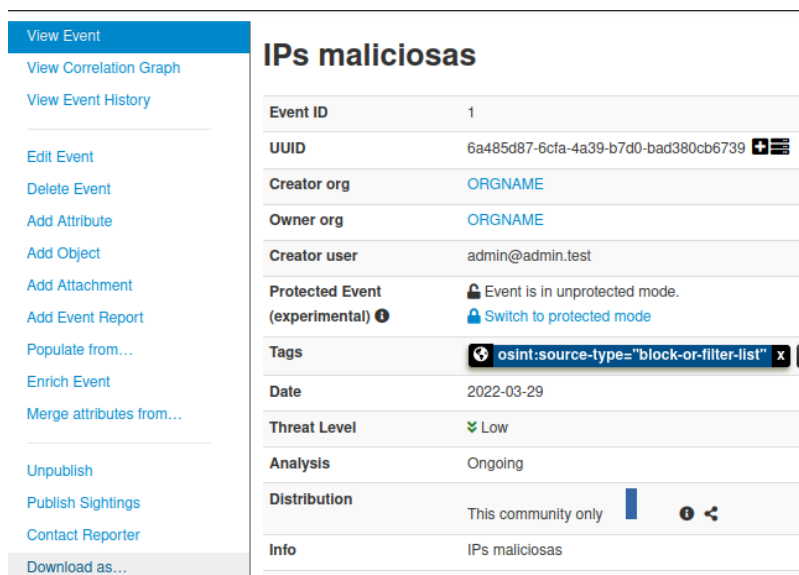
luego al dar a home veremos que se han creado correctamente



Implementar MISP a ELK

Para poder implementar MISP a ELK tendremos que descargarnos un evento en forma de CSV y aplicarlo con logstash

Para ello, **dentro de un evento** tendremos que irnos a la parte de "download as"



Y crearnos un pipeline para meter los datos de CSV

```
input {
  file {
    path => "ruta al fichero de csv"
    start_position => beginning
    sincedb_path => "/dev/null"
    mode => read
    exit_after_read => true
  }
}

filter {
  csv {
    columns => ["columnas creadas en la platilla del index"]
  }
  mutate {
    remove_field => ["columnas a eliminar"]
  }
}

output {
  stdout { }
  elasticsearch {
    index => "nombre del index creado(ipsmaliciosas en este caso)"
  }
}
```

Y relizar un logstash

```
sudo /usr/share/logstash/bin/logstash -f '/home/usuario/Desktop/pipeline.conf'
```

Posibles usos de misp

visto todo lo anterior misp podria tener diferentes implementaciones gracias a su versatilidad y su adaptacion al uso que le queremos dar. Existen usos como la implementacion de eventos a un firewall en el cual se irian añadiendo bloqueos a ips no deseadas de forma automatica. por ejemplo, tambien existe la posibilidad de un dns automatizado con la implementacion de un evento autosuficiente o se podria usar como una herramienta de aprendizaje donde los usuarios o equipo de seguridad se informen de nuevas amenazas, debilidades y fortalezas.