Index

Threat Intelligence - MISP

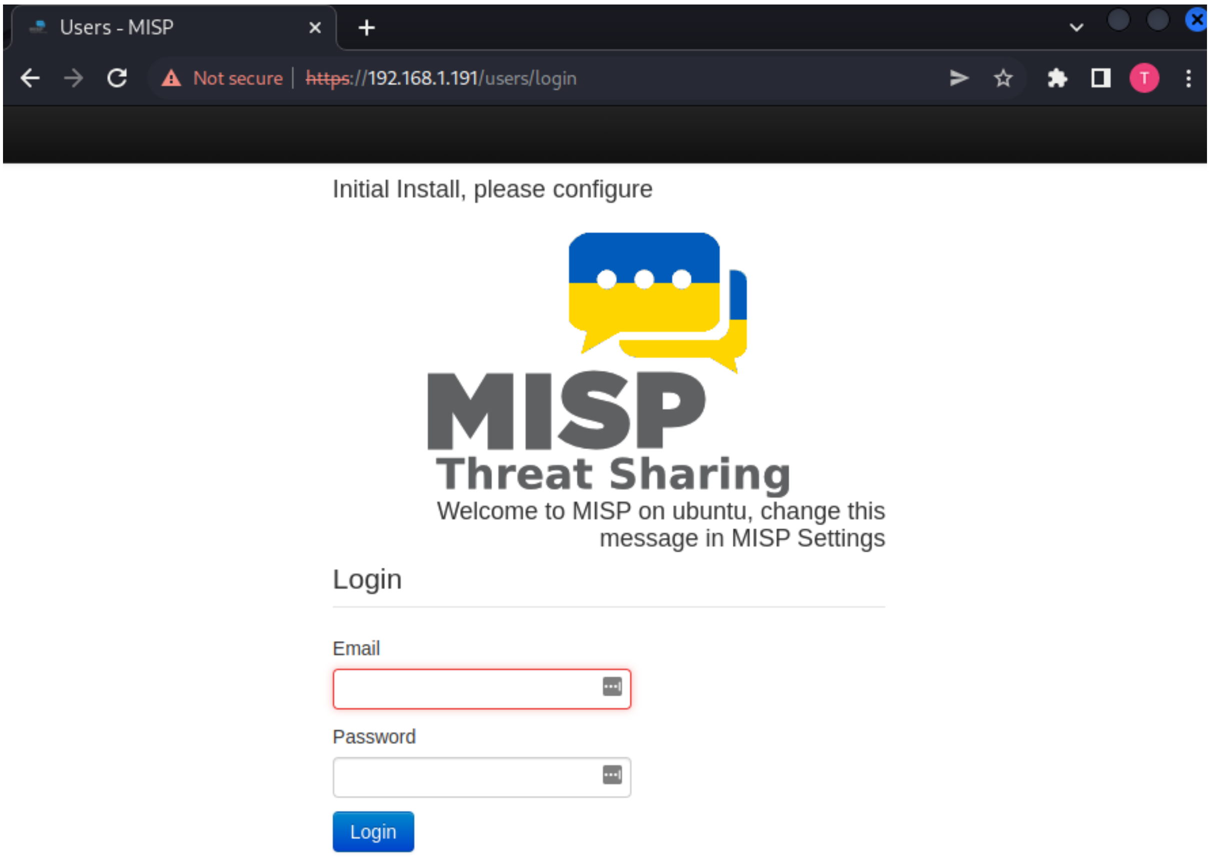
MISP Threat Sharing (Malware Information Sharing Platform) https://www.misp-project.org/

The MISP is an open source software solution for collecting, storing, distributing and sharing cyber security indicators and threats about cyber security. The project is funded by the European Union and the Computer Incident Response Center Luxembourg (CIRCL).

You can download a virtual machine from: https://vm.misp-project.org/latest/ It comes with the following credentials:

```
For the MISP web interface -> admin@admin.test:admin
For the system -> misp:Password1234
```

This virtual machine is not made for production, it’s not secure.



Users - MISP

Not secure | https://192.168.1.191/users/login

Initial Install, please configure

Welcome to MISP on ubuntu, change this message in MISP Settings

Login

Email

Password

Figure 1: "MISP Login"

Set an administrator password for the whole system.

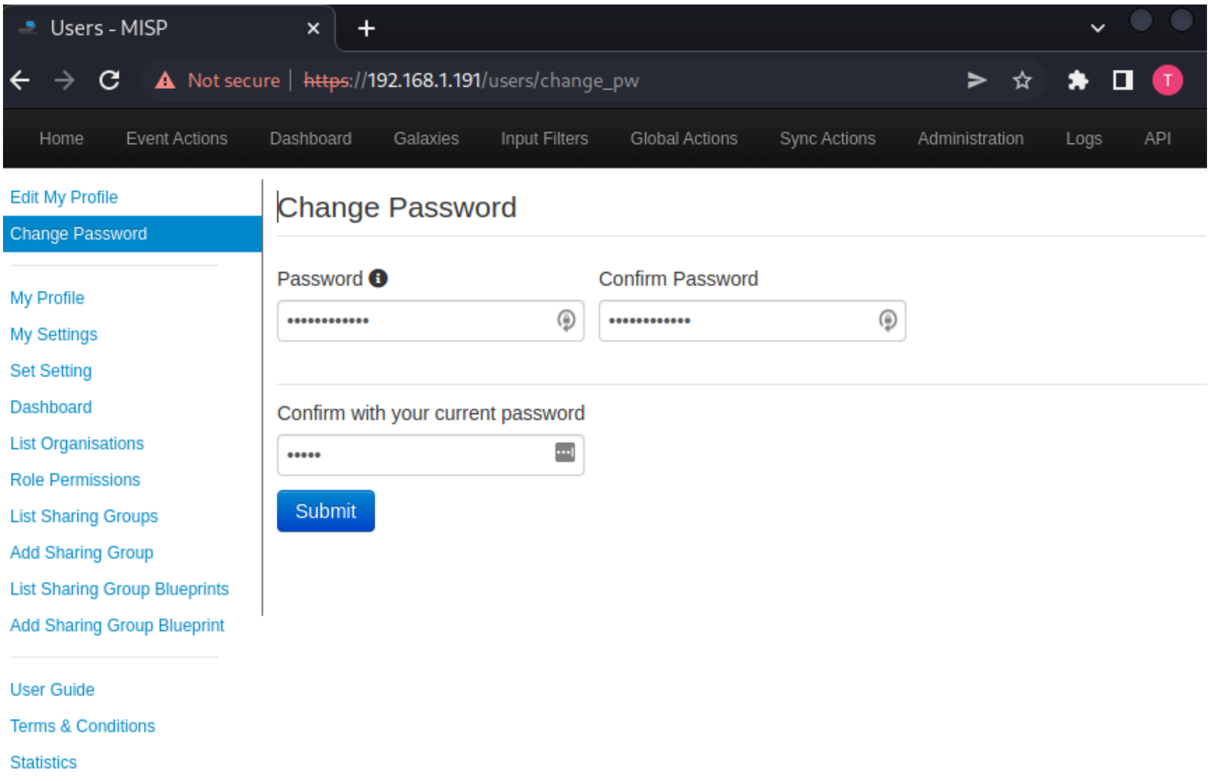
Password Policy:

```
[12]: Ensure that the password is at least 12 characters long

[A-Z]: contains at least one upper-case

[0-9| ]: includes a digit or a special character

[a-z]: at least one lower-case character
```



Change Password

Password: ••••••••••••

Confirm Password: ••••••••••••

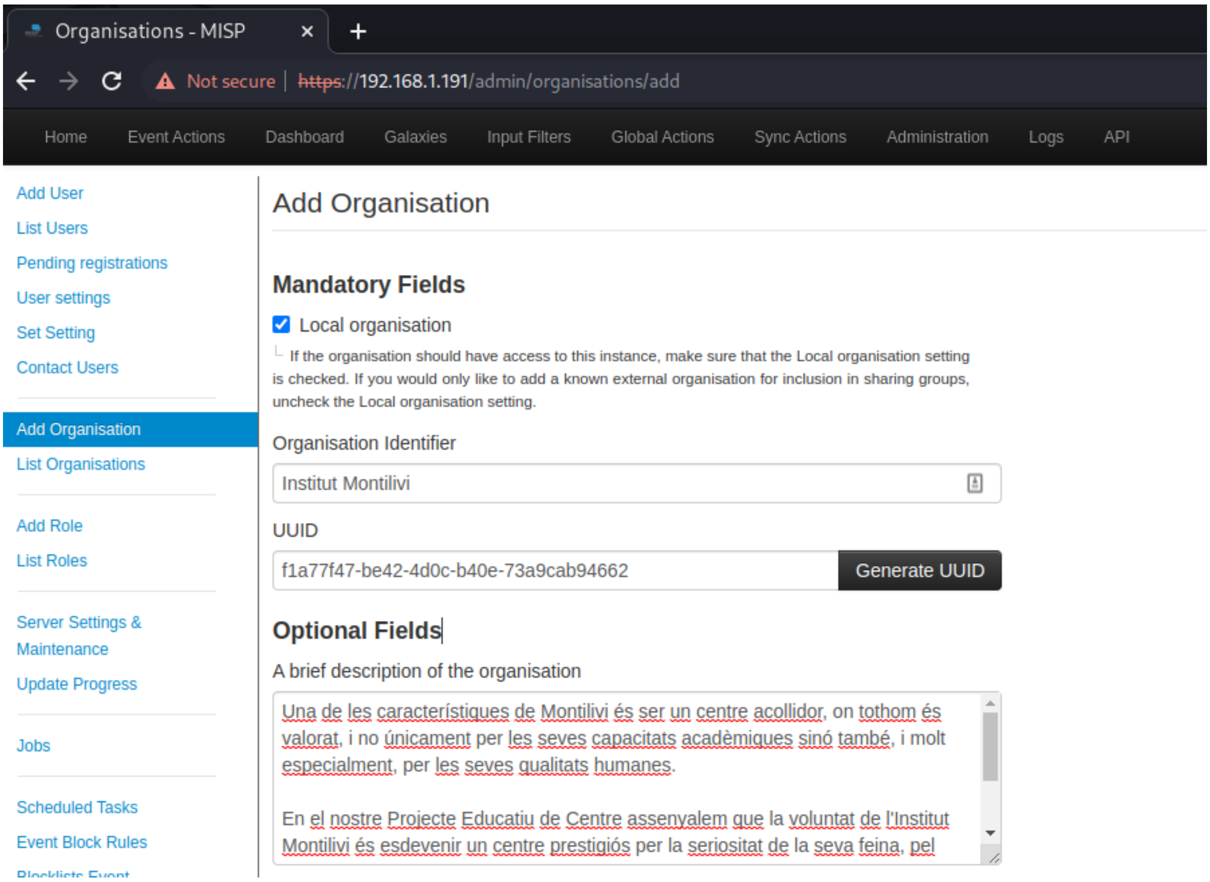
Confirm with your current password: •••••

Figure 2: "Change password"

Define your organization

From the menu bar, select Add Organizations and fill the fields of your own organization.

For this example I created one for our school:



Add Organisation

Mandatory Fields

☑ Local organisation

If the organisation should have access to this instance, make sure that the Local organisation setting is checked. If you would only like to add a known external organisation for inclusion in sharing groups, uncheck the Local organisation setting.

Organisation Identifier: Institut Montilivi

UUID: f1a77f47-be42-4d0c-b40e-73a9cab94662 [Generate UUID]

Optional Fields

A brief description of the organisation

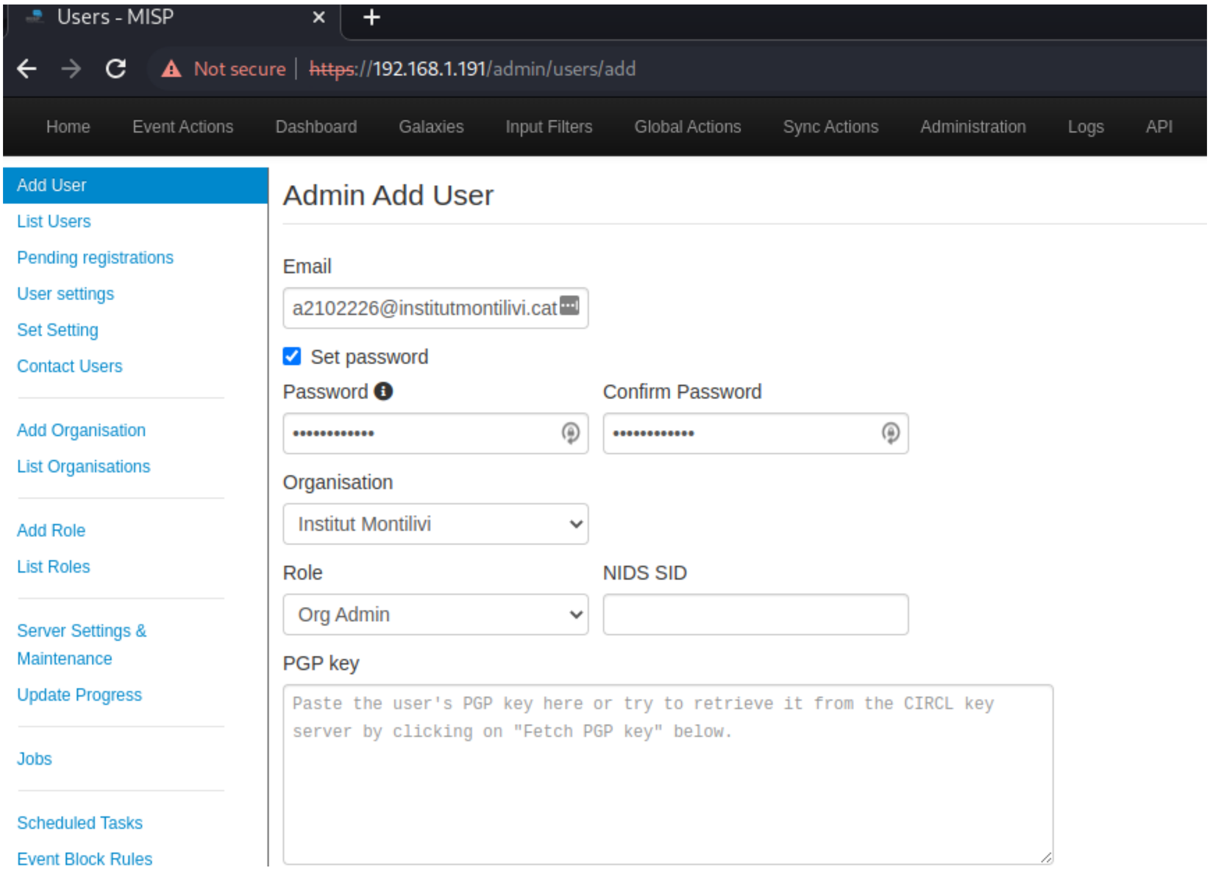
Una de les característiques de Montilivi és ser un centre acollidor, on tothom és valorat, i no únicament per les seves capacitats acadèmiques sinó també, i molt especialment, per les seves qualitats humanes.

En el nostre Projecte Educatiu de Centre assenyalem que la voluntat de l'Institut Montilivi és esdevenir un centre prestigiós per la seriositat de la seva feina, pel

Figure 3: ””

Create a user with *Org admin* permissions on your new organization.

Select *Add User* from the *Administration* menu bar.



Admin Add User

Email
a2102226@institutmontilivi.cat

☑ Set password

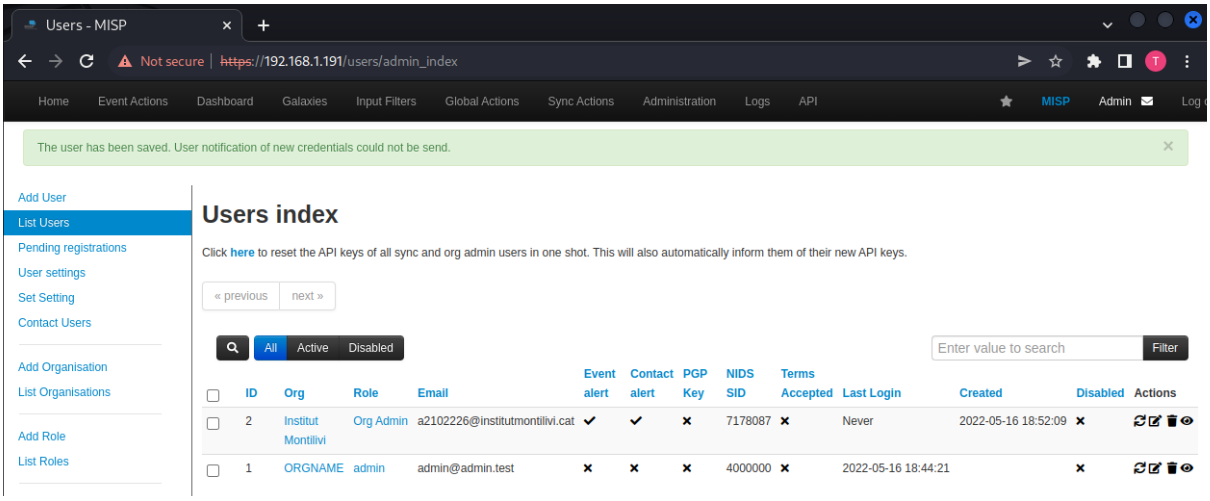
Password	Confirm Password
••••••••••••	••••••••••••

Organisation
Institut Montilivi

Role	NIDS SID
Org Admin	

PGP key
Paste the user's PGP key here or try to retrieve it from the CIRCL key server by clicking on "Fetch PGP key" below.

Figure 4: “Add User”



The user has been saved. User notification of new credentials could not be send.

Users index

Click here to reset the API keys of all sync and org admin users in one shot. This will also automatically inform them of their new API keys.

□	ID	Org	Role	Email	Event alert	Contact alert	PGP Key	NIDS SID	Terms Accepted	Last Login	Created	Disabled	Actions
□	2	Institut Montilivi	Org Admin	a2102226@institutmontilivi.cat	✓	✓	✗	7178087	✗	Never	2022-05-16 18:52:09	✗	
□	1	ORGNAME	admin	admin@admin.test	✗	✗	✗	4000000	✗	2022-05-16 18:44:21		✗	

Figure 5: “List Users”

Key concepts

Event: This is a study case.

Attributes: These are the information elements that shape the event.

Feeds: These are data sources that enrich our events.

Tags: Categories that we put on an event in order to classify it.

Galaxies: These are templates for describing attributes.

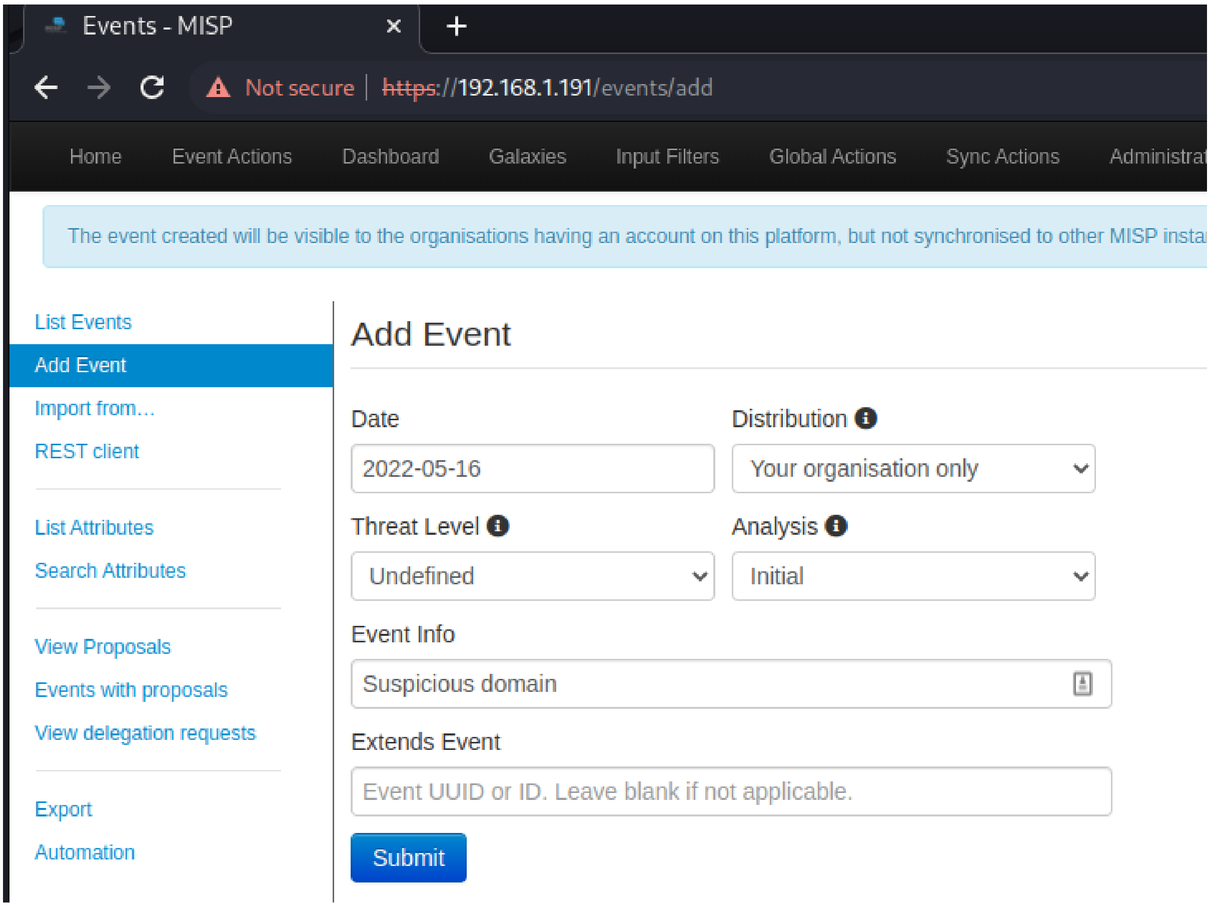
Cluster: Is an instance of a galaxy.

Event

Let's understand what an event is while creating one. Suppose that a user in our organization receives an email with a suspicious link, for example: linksys.secureshellz.net Obviously, we don't want to open the link without knowing if this domain is malware free.

From the menu bar, select *Event Actions* and *Add Event*.

Fill it with the information requested:



The event created will be visible to the organisations having an account on this platform, but not synchronised to other MISP insta

Add Event

Date: 2022-05-16

Distribution: Your organisation only

Threat Level: Undefined

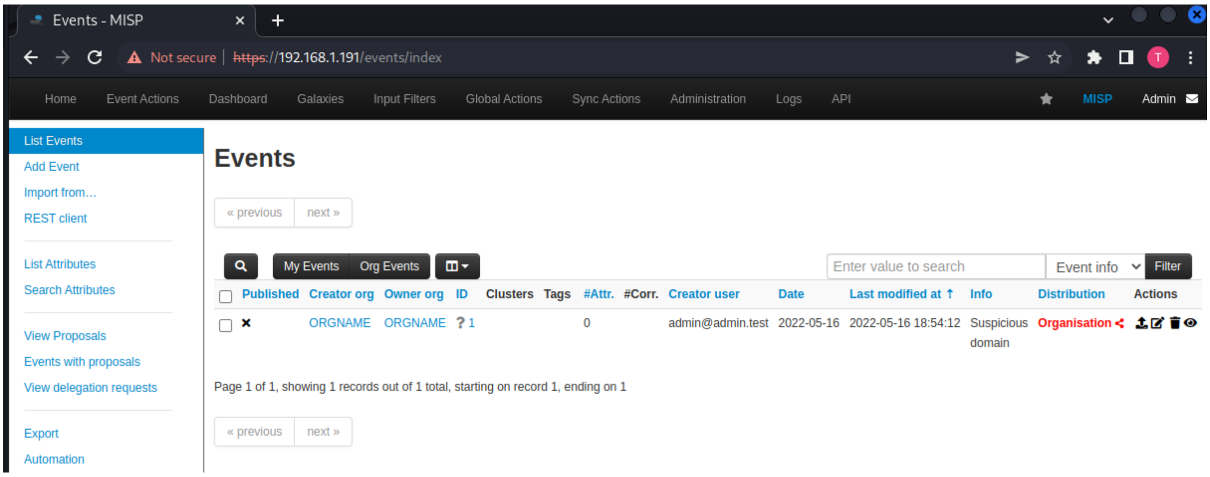
Analysis: Initial

Event Info: Suspicious domain

Extends Event: Event UUID or ID. Leave blank if not applicable.

Figure 6: "Add Event"

Now, if you list the events you should see something like this:



Events

	Published	Creator org	Owner org	ID	Clusters	Tags	#Attr.	#Corr.	Creator user	Date	Last modified at ↑	Info	Distribution	Actions
□	✗	ORGNAME	ORGNAME	? 1			0		admin@admin.test	2022-05-16	2022-05-16 18:54:12	Suspicious domain	Organisation	

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

Figure 7: "List Events"

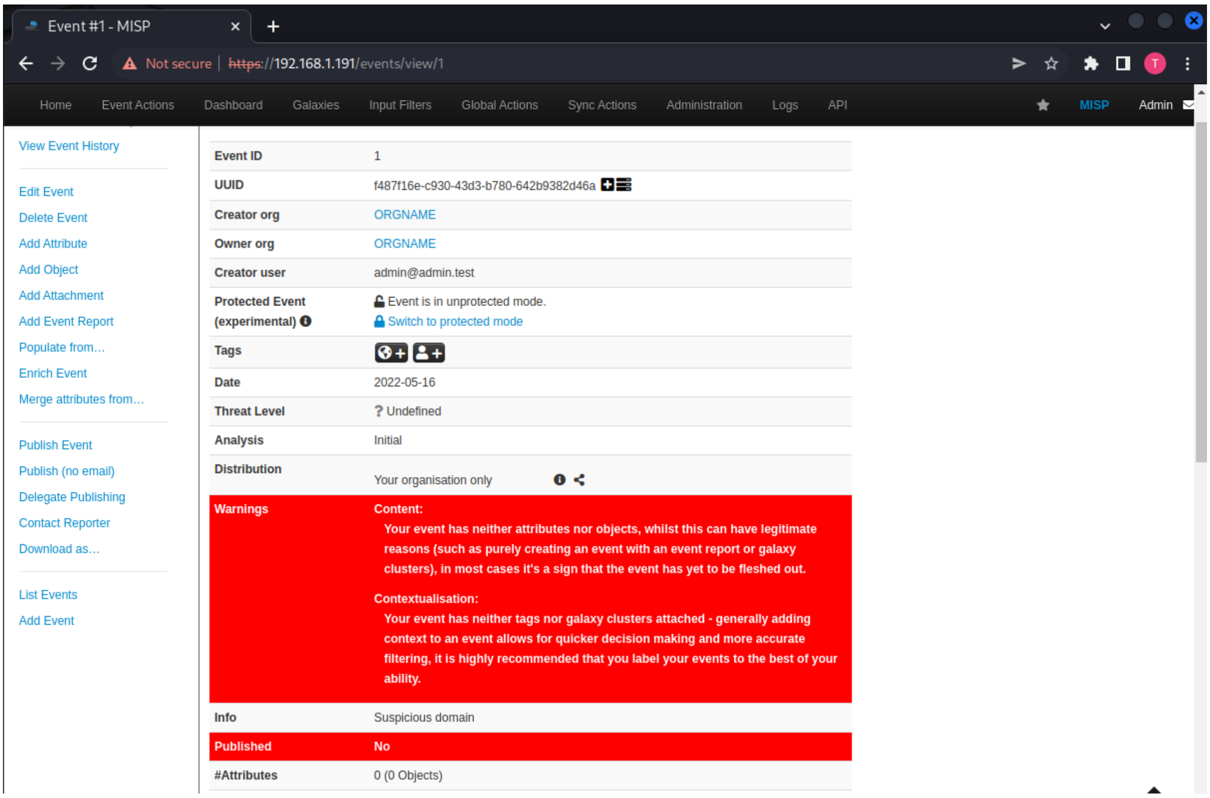
Let's add attributes to this event.

Attributes

Attributes give shape and meaning to the event.

In our example, a very clear attribute is the domain that we consider suspicious.

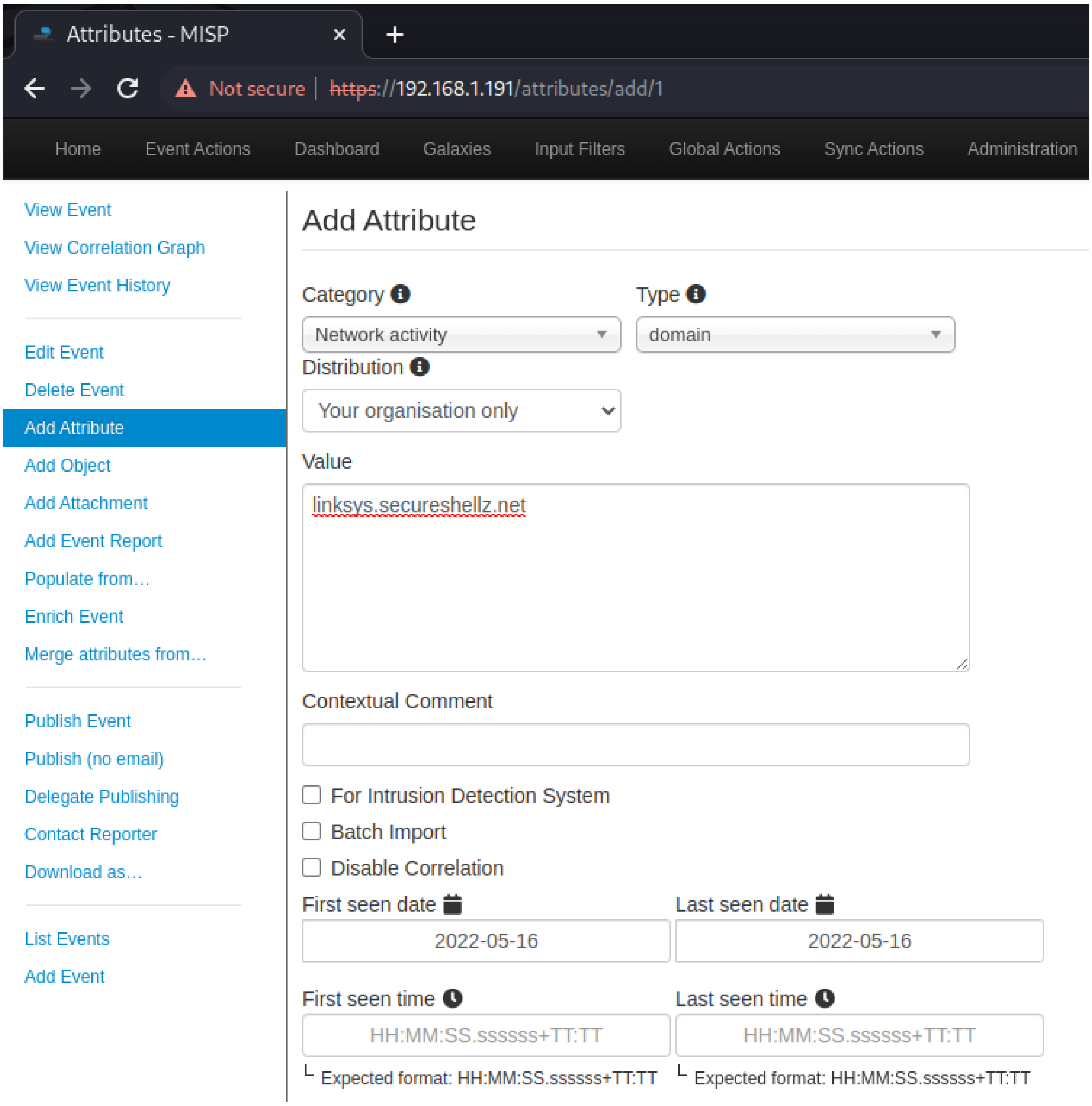
Click on the event ID to see its contents:



Event ID	1
UUID	f487f16e-c930-43d3-b780-642b9382d46a
Creator org	ORGNAME
Owner org	ORGNAME
Creator user	admin@admin.test
Protected Event (experimental)	Event is in unprotected mode. Switch to protected mode
Tags	
Date	2022-05-16
Threat Level	? Undefined
Analysis	Initial
Distribution	Your organisation only
Warnings	Content: Your event has neither attributes nor objects, whilst this can have legitimate reasons (such as purely creating an event with an event report or galaxy clusters), in most cases it's a sign that the event has yet to be fleshed out. 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	Suspicious domain
Published	No
#Attributes	0 (0 Objects)

Figure 8: "Event info"

Then add a new attribute from the menu. Fill the data.



Add Attribute

Category: Network activity

Type: domain

Distribution: Your organisation only

Value: linksys.secureshellz.net

Contextual Comment:

□ For Intrusion Detection System

□ Batch Import

□ Disable Correlation

First seen date: 2022-05-16

Last seen date: 2022-05-16

First seen time: HH:MM:SS.ssssss+TT:TT

└ Expected format: HH:MM:SS.ssssss+TT:TT

Last seen time: HH:MM:SS.ssssss+TT:TT

└ Expected format: HH:MM:SS.ssssss+TT:TT

Figure 9: "Add Attribute"

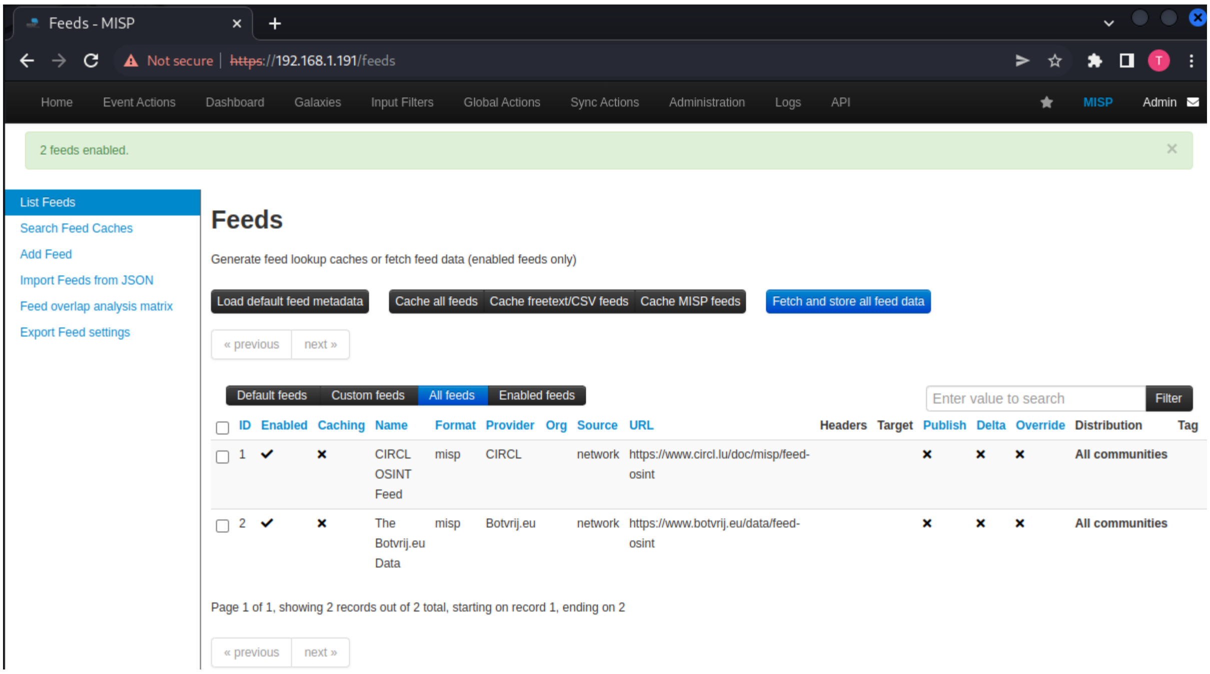
Feeds

In order to find out if someone else has found this link and has already studied it, we will add the feeds, which are serie of OSINT events that we can import.

Select the *List Feeds* option.

By default, the application has two but the are disabled.

Select and enable them.



2 feeds enabled.

Feeds

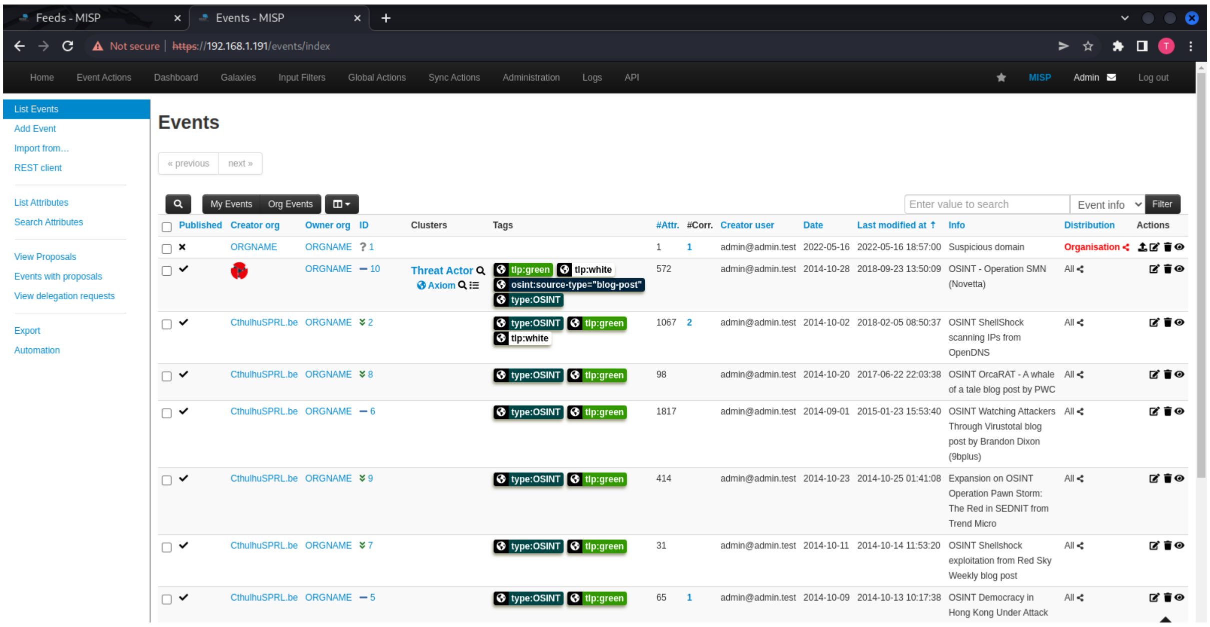
Generate feed lookup caches or fetch feed data (enabled feeds only)

□	ID	Enabled	Caching	Name	Format	Provider	Org	Source	URL	Headers	Target	Publish	Delta	Override	Distribution	Tag
□	1	✓	✗	CIRCL OSINT Feed	misp	CIRCL		network	https://www.circl.lu/doc/misp/feed-osint			✗	✗	✗	All communities	
□	2	✓	✗	The Botvrij.eu Data	misp	Botvrij.eu		network	https://www.botvrij.eu/data/feed-osint			✗	✗	✗	All communities	

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

Figure 10: “List Feeds”

In a short time we will start receiving events created by the two enabled feeds. We can see events listed:



Events

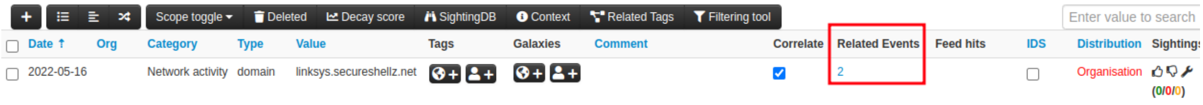
□	Published	Creator org	Owner org	ID	Clusters	Tags	#Attr.	#Corr.	Creator user	Date	Last modified at ↑	Info	Distribution	Actions
□	✗	ORGNAME	ORGNAME	? 1			1	1	admin@admin.test	2022-05-16	2022-05-16 18:57:00	Suspicious domain	Organisation	
□	✓		ORGNAME	— 10	Threat Actor Axiom	tlp:green tlp:white osint:source-type="blog-post" type:OSINT	572		admin@admin.test	2014-10-28	2018-09-23 13:50:09	OSINT - Operation SMN (Novetta)	All	
□	✓	CthulhuSPRL.be	ORGNAME	2		type:OSINT tlp:green tlp:white	1067	2	admin@admin.test	2014-10-02	2018-02-05 08:50:37	OSINT ShellShock scanning IPs from OpenDNS	All	
□	✓	CthulhuSPRL.be	ORGNAME	8		type:OSINT tlp:green	98		admin@admin.test	2014-10-20	2017-06-22 22:03:38	OSINT OrcaRAT - A whale of a tale blog post by PWC	All	
□	✓	CthulhuSPRL.be	ORGNAME	— 6		type:OSINT tlp:green	1817		admin@admin.test	2014-09-01	2015-01-23 15:53:40	OSINT Watching Attackers Through Virustotal blog post by Brandon Dixon (9bplus)	All	
□	✓	CthulhuSPRL.be	ORGNAME	9		type:OSINT tlp:green	414		admin@admin.test	2014-10-23	2014-10-25 01:41:08	Expansion on OSINT Operation Pawn Storm: The Red in SEDNIT from Trend Micro	All	
□	✓	CthulhuSPRL.be	ORGNAME	7		type:OSINT tlp:green	31		admin@admin.test	2014-10-11	2014-10-14 11:53:20	OSINT Shellshock exploitation from Red Sky Weekly blog post	All	
□	✓	CthulhuSPRL.be	ORGNAME	— 5		type:OSINT tlp:green	65	1	admin@admin.test	2014-10-09	2014-10-13 10:17:38	OSINT Democracy in Hong Kong Under Attack	All	

Figure 11: “Events created”

Automatic enrichment

Now, the part that interests us is in our event. Click the event to display its content and go to its attribute.

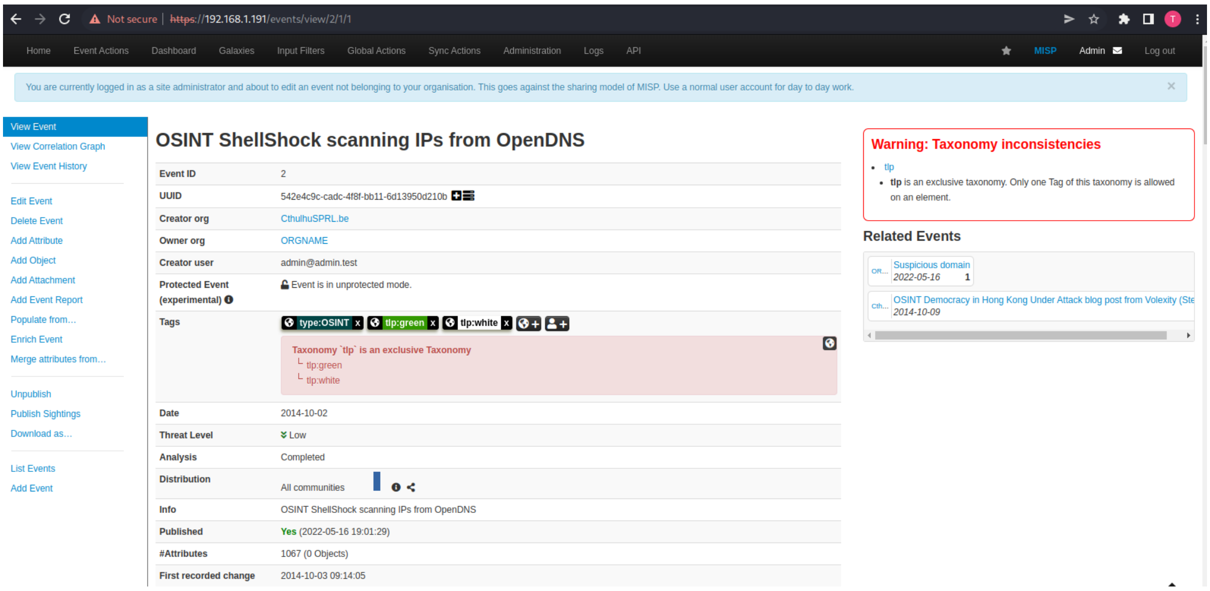
We can see in the *Related Events* column our related event. Click it.



□	Date ↑	Org	Category	Type	Value	Tags	Galaxies	Comment	Correlate	Related Events	Feed hits	IDS	Distribution	Sighting
□	2022-05-16		Network activity	domain	linksys.secureshellz.net				☑	2		□	Organisation	(0/0/0)

Figure 12: “Related Events”

This event is created by the CthulhuSPRL.be organization with data from 2014 and contains 1067 attributes.



You are currently logged in as a site administrator and about to edit an event not belonging to your organisation. This goes against the sharing model of MISP. Use a normal user account for day to day work.

OSINT ShellShock scanning IPs from OpenDNS

Event ID	2
UUID	542e4c9c-cadc-4f8f-bb11-6d13950d210b
Creator org	CthulhuSPRL.be
Owner org	ORGNAME
Creator user	admin@admin.test
Protected Event (experimental)	Event is in unprotected mode.
Tags	type:OSINT x tlp:green x tlp:white x Taxonomy `tlp` is an exclusive Taxonomy └ tlp:green └ tlp:white
Date	2014-10-02
Threat Level	Low
Analysis	Completed
Distribution	All communities
Info	OSINT ShellShock scanning IPs from OpenDNS
Published	Yes (2022-05-16 19:01:29)
#Attributes	1067 (0 Objects)
First recorded change	2014-10-03 09:14:05

Warning: Taxonomy inconsistencies

- tlp
  - **tlp** is an exclusive taxonomy. Only one Tag of this taxonomy is allowed on an element.

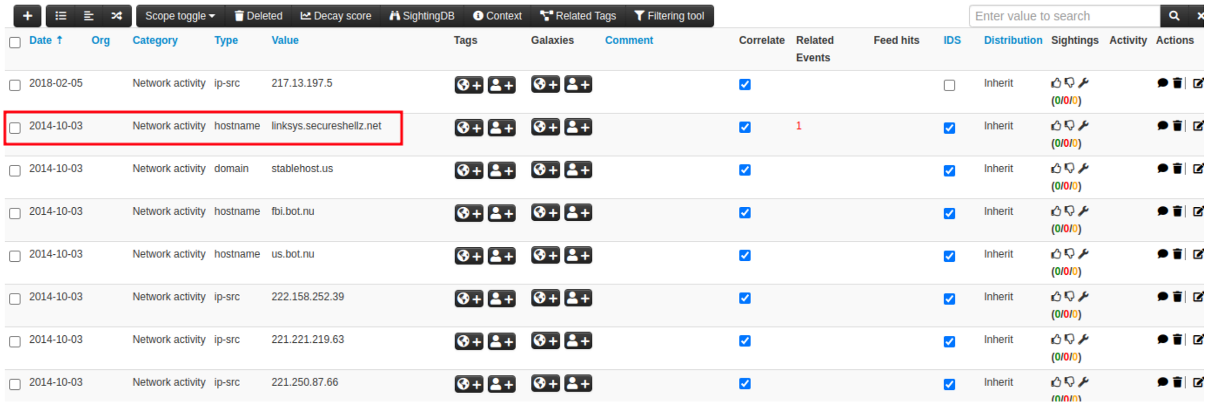
Related Events

OR… Suspicious domain *2022-05-16* **1**

Cth… OSINT Democracy in Hong Kong Under Attack blog post from Volexity (Ste *2014-10-09*

Figure 13: “View Event”

Below the description we can see the list of all its attributes, one of which we are interested in:



□	Date ↑	Org	Category	Type	Value	Tags	Galaxies	Comment	Correlate	Related Events	Feed hits	IDS	Distribution	Sightings	Activity	Actions
□	2018-02-05		Network activity	ip-src	217.13.197.5				☑			□	Inherit	(0/0/0)		
□	2014-10-03		Network activity	hostname	linksys.secureshellz.net				☑	1		☑	Inherit	(0/0/0)		
□	2014-10-03		Network activity	domain	stablehost.us				☑			☑	Inherit	(0/0/0)		
□	2014-10-03		Network activity	hostname	fbi.bot.nu				☑			☑	Inherit	(0/0/0)		
□	2014-10-03		Network activity	hostname	us.bot.nu				☑			☑	Inherit	(0/0/0)		
□	2014-10-03		Network activity	ip-src	222.158.252.39				☑			☑	Inherit	(0/0/0)		
□	2014-10-03		Network activity	ip-src	221.221.219.63				☑			☑	Inherit	(0/0/0)		
□	2014-10-03		Network activity	ip-src	221.250.87.66				☑			☑	Inherit	(0/0/0)		

Figure 14: “List Attributes”

So, yes, this link is already classified as ***OSINT ShellShock scanning IPs from OpenDNS***.

Tags

Tags are used to classify and add information to an event. This is the link where MISP has collected all tags and taxonomies:

https://www.misp-project.org/taxonomies.html

From this list we will work with one type: the TLP taconomy.

TLP (Traggic Light Protocol) is designed to classify event information depending on the data protection and reputation of the company.

They have defined the following tags:

- Red
- Amber
- Green
- White

Activity 1

According to the information given the taxonomies by MISP, explain briefly what involves each color in an event.

- **Red**

For information that is limited to selected persons and its disclosure could have a negative impact on operations.

It can be distributed only to designated persons.

- **Amber**

For internal information that with its misuse or distribution would cause privacy risks affecting reputation and operations.

It can be distributed only with the members of the organization who are authorized to have knowledge of the information.

- **Green**

For all the information that can be shared in the organization and with third parties.

It can be distributed to partner organizations, but not by public means.

- **White**

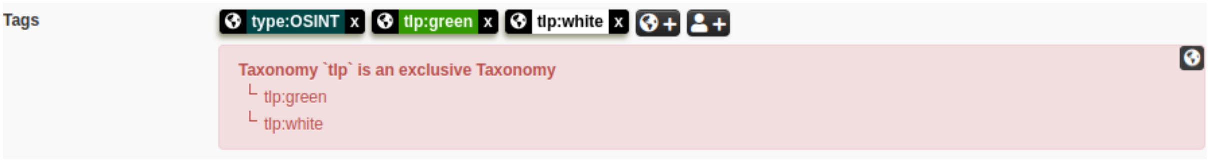
For information that can be used without causing any risk in case it's misused.

Information can be shared publicly in accordance with the law.

Activity 2

When the event is captured in the previous page, there is a warning in the *Tags* section.

What is the warning telling us?



Tags

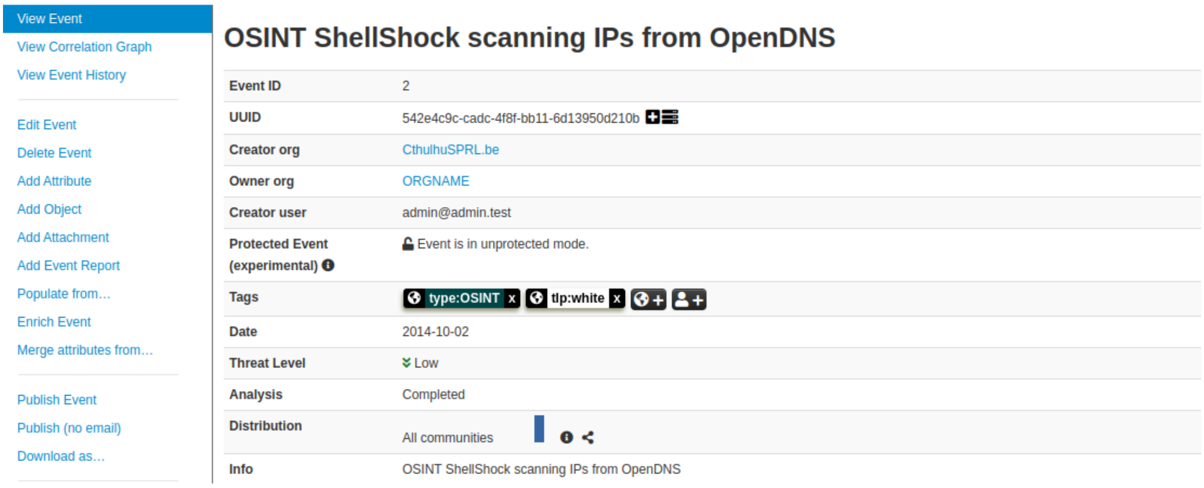
type:OSINT x · tlp:green x · tlp:white x

Taxonomy `tlp` is an exclusive Taxonomy
└ tlp:green
└ tlp:white

Figure 15: "Warning"

It's saying that this taxonomy is exclusive, therefore it only makes sense to have one tls color.

If we remove one of the colors we will no longer see the warning.



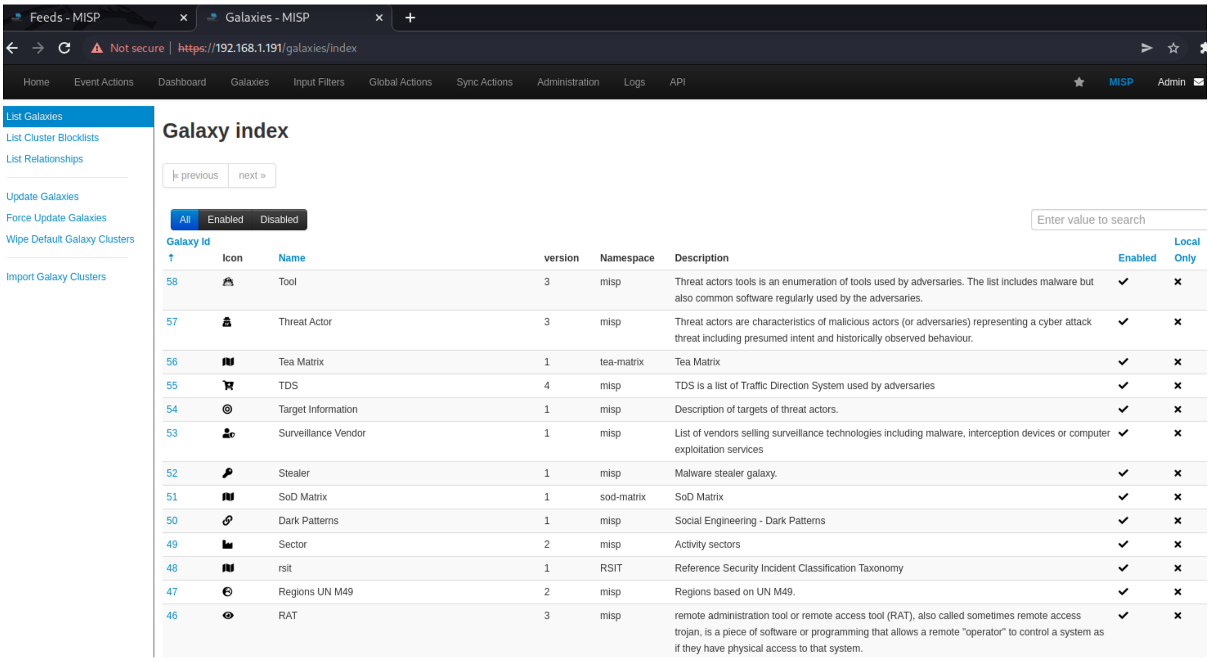
OSINT ShellShock scanning IPs from OpenDNS

Event ID	2
UUID	542e4c9c-cadc-4f8f-bb11-6d13950d210b
Creator org	CthulhuSPRL.be
Owner org	ORGNAME
Creator user	admin@admin.test
Protected Event (experimental)	Event is in unprotected mode.
Tags	type:OSINT x · tlp:white x
Date	2014-10-02
Threat Level	Low
Analysis	Completed
Distribution	All communities
Info	OSINT ShellShock scanning IPs from OpenDNS

Figure 16: "Warning corrected"

Galaxies

Galaxies are templates for describing more information about an event or attribute. To list them we go to *List Galaxies* from the *Galaxies* menu bar.

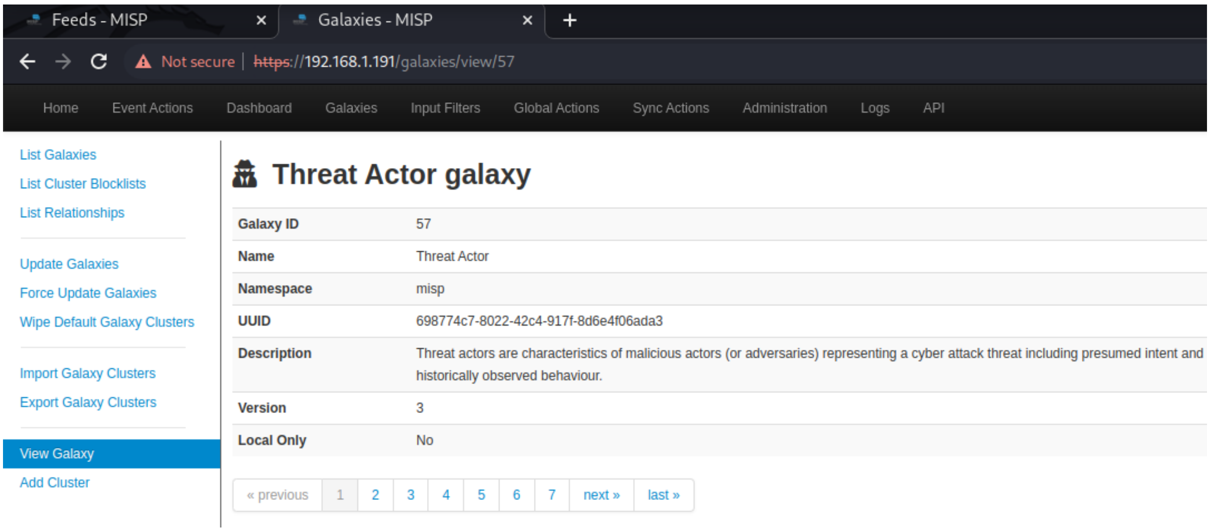


Galaxy index

Galaxy Id ↑	Icon	Name	version	Namespace	Description	Enabled	Local Only
58		Tool	3	misp	Threat actors tools is an enumeration of tools used by adversaries. The list includes malware but also common software regularly used by the adversaries.	✓	✗
57		Threat Actor	3	misp	Threat actors are characteristics of malicious actors (or adversaries) representing a cyber attack threat including presumed intent and historically observed behaviour.	✓	✗
56		Tea Matrix	1	tea-matrix	Tea Matrix	✓	✗
55		TDS	4	misp	TDS is a list of Traffic Direction System used by adversaries	✓	✗
54		Target Information	1	misp	Description of targets of threat actors.	✓	✗
53		Surveillance Vendor	1	misp	List of vendors selling surveillance technologies including malware, interception devices or computer exploitation services	✓	✗
52		Stealer	1	misp	Malware stealer galaxy.	✓	✗
51		SoD Matrix	1	sod-matrix	SoD Matrix	✓	✗
50		Dark Patterns	1	misp	Social Engineering - Dark Patterns	✓	✗
49		Sector	2	misp	Activity sectors	✓	✗
48		rsit	1	RSIT	Reference Security Incident Classification Taxonomy	✓	✗
47		Regions UN M49	2	misp	Regions based on UN M49.	✓	✗
46		RAT	3	misp	remote administration tool or remote access tool (RAT), also called sometimes remote access trojan, is a piece of software or programming that allows a remote "operator" to control a system as if they have physical access to that system.	✓	✗

Figure 17: "List Galaxies"

Let's look at one: *Threat Actor*

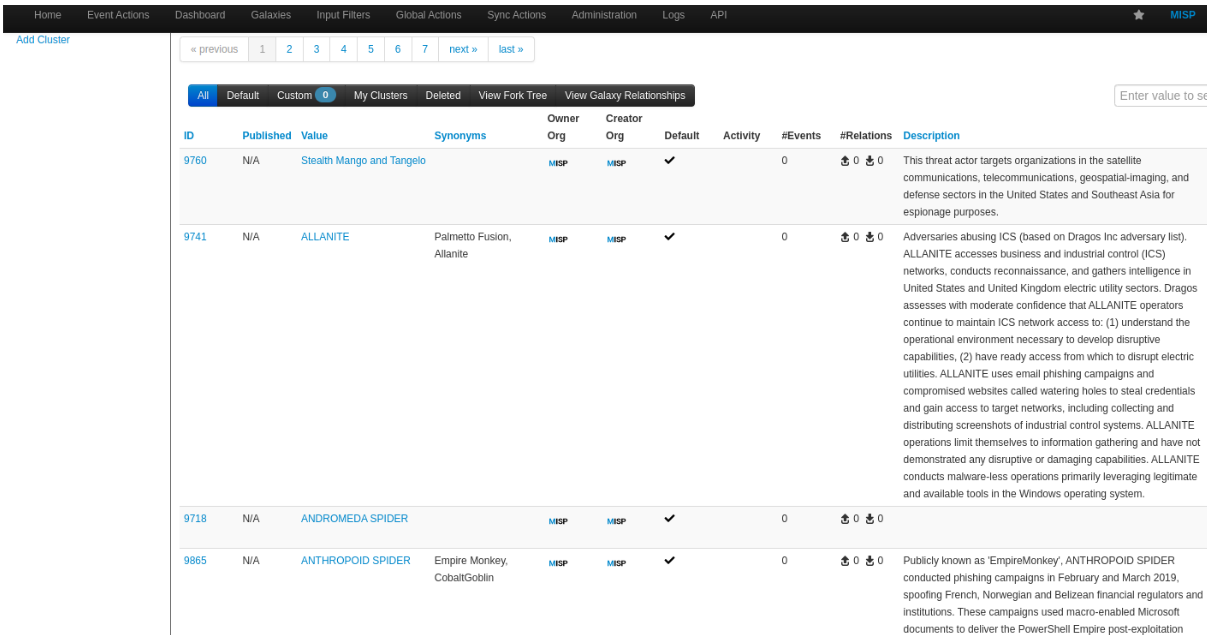


Threat Actor galaxy

Galaxy ID	57
Name	Threat Actor
Namespace	misp
UUID	698774c7-8022-42c4-917f-8d6e4f06ada3
Description	Threat actors are characteristics of malicious actors (or adversaries) representing a cyber attack threat including presumed intent and historically observed behaviour.
Version	3
Local Only	No

Figure 18: ""

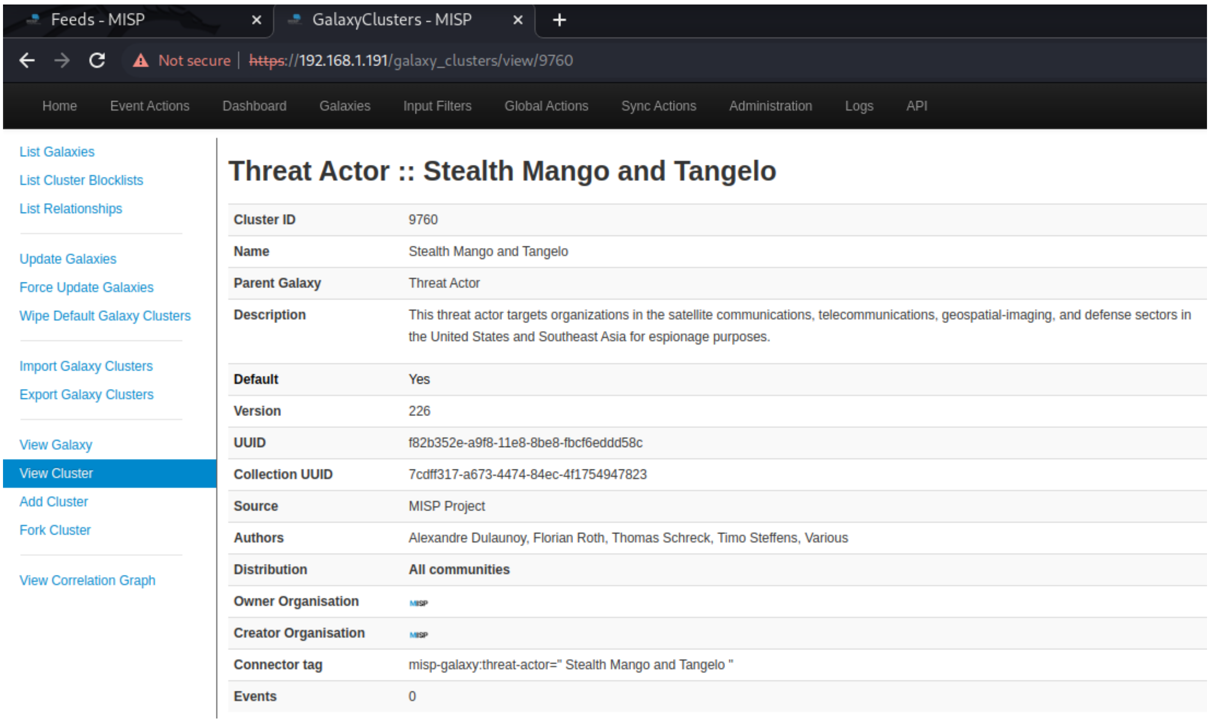
This is a fairly simple case, we got only a name and a description. We can see all the published instances of this galaxy:



ID	Published	Value	Synonyms	Owner Org	Creator Org	Default	Activity	#Events	#Relations	Description
9760	N/A	Stealth Mango and Tangelo		MISP	MISP	✓		0	⬆ 0 ⬇ 0	This threat actor targets organizations in the satellite communications, telecommunications, geospatial-imaging, and defense sectors in the United States and Southeast Asia for espionage purposes.
9741	N/A	ALLANITE	Palmetto Fusion, Allanite	MISP	MISP	✓		0	⬆ 0 ⬇ 0	Adversaries abusing ICS (based on Dragos Inc adversary list). ALLANITE accesses business and industrial control (ICS) networks, conducts reconnaissance, and gathers intelligence in United States and United Kingdom electric utility sectors. Dragos assesses with moderate confidence that ALLANITE operators continue to maintain ICS network access to: (1) understand the operational environment necessary to develop disruptive capabilities, (2) have ready access from which to disrupt electric utilities. ALLANITE uses email phishing campaigns and compromised websites called watering holes to steal credentials and gain access to target networks, including collecting and distributing screenshots of industrial control systems. ALLANITE operations limit themselves to information gathering and have not demonstrated any disruptive or damaging capabilities. ALLANITE conducts malware-less operations primarily leveraging legitimate and available tools in the Windows operating system.
9718	N/A	ANDROMEDA SPIDER		MISP	MISP	✓		0	⬆ 0 ⬇ 0	
9865	N/A	ANTHROPOID SPIDER	Empire Monkey, CobaltGoblin	MISP	MISP	✓		0	⬆ 0 ⬇ 0	Publicly known as 'EmpireMonkey', ANTHROPOID SPIDER conducted phishing campaigns in February and March 2019, spoofing French, Norwegian and Belizean financial regulators and institutions. These campaigns used macro-enabled Microsoft documents to deliver the PowerShell Empire post-exploitation

Figure 19: “Threat Actor galaxy”

We select one to see its history:



Threat Actor :: Stealth Mango and Tangelo

Cluster ID	9760
Name	Stealth Mango and Tangelo
Parent Galaxy	Threat Actor
Description	This threat actor targets organizations in the satellite communications, telecommunications, geospatial-imaging, and defense sectors in the United States and Southeast Asia for espionage purposes.
Default	Yes
Version	226
UUID	f82b352e-a9f8-11e8-8be8-fbcf6eddd58c
Collection UUID	7cdff317-a673-4474-84ec-4f1754947823
Source	MISP Project
Authors	Alexandre Dulaunoy, Florian Roth, Thomas Schreck, Timo Steffens, Various
Distribution	All communities
Owner Organisation	MISP
Creator Organisation	MISP
Connector tag	misp-galaxy:threat-actor=" Stealth Mango and Tangelo "
Events	0

Figure 20: “Instances of the galaxy”

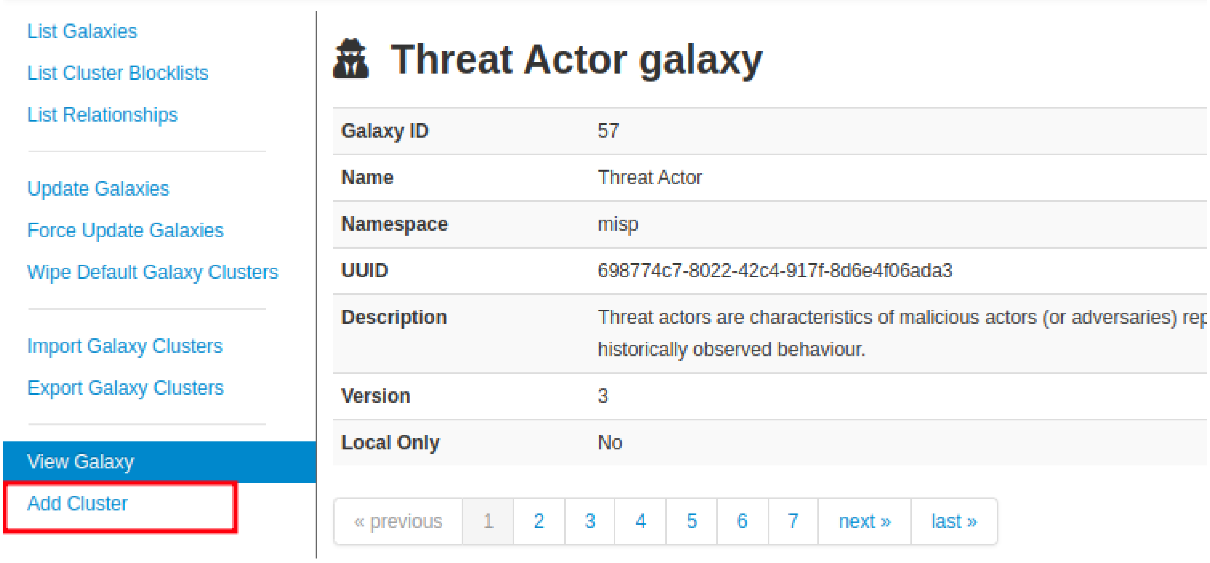
Cluster

Clusters are simply an instance of a galaxy.

Activity 3

Create a cluster as an instance of the *Threat Actor* galaxy, defining the attacker "Estudiant del curs de ciberseguretat Montilivi".

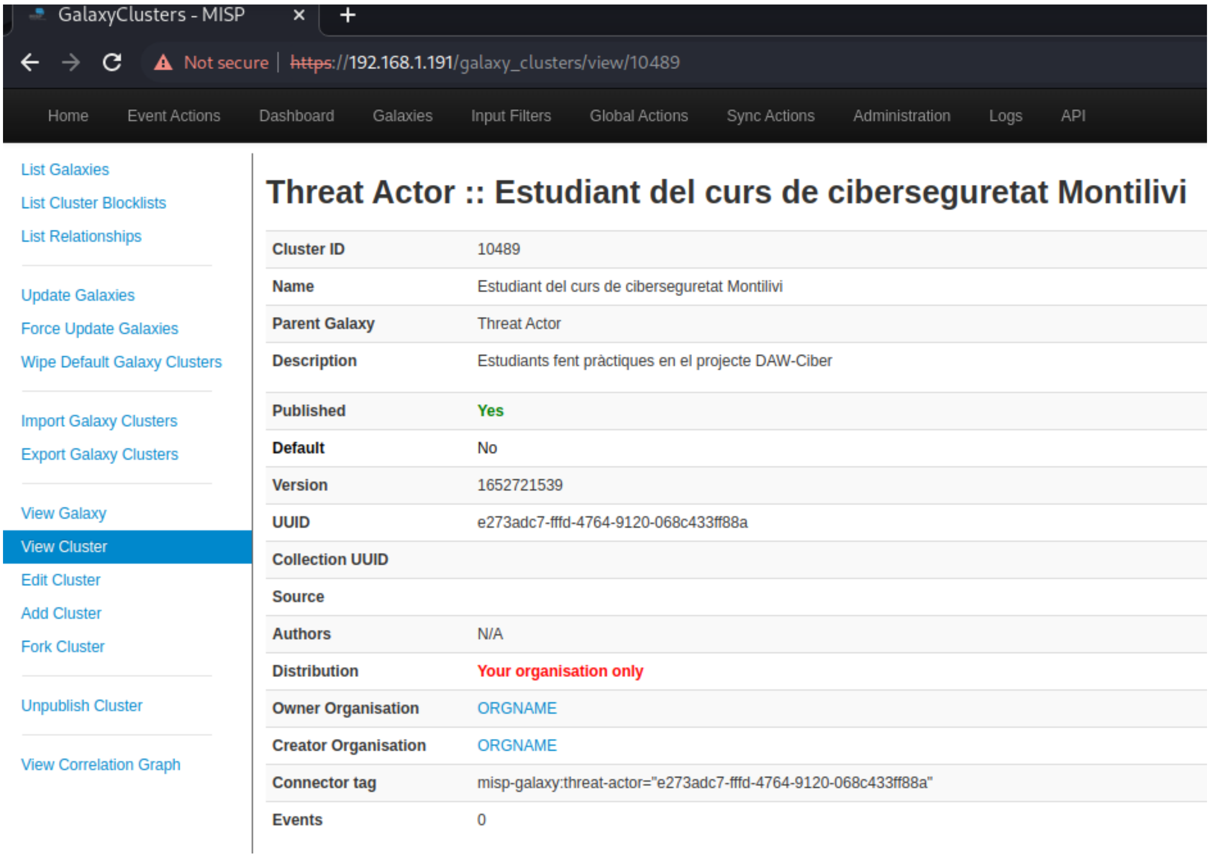
Attach a screenshot of your new cluster.



Threat Actor galaxy

Galaxy ID	57
Name	Threat Actor
Namespace	misp
UUID	698774c7-8022-42c4-917f-8d6e4f06ada3
Description	Threat actors are characteristics of malicious actors (or adversaries) rep historically observed behaviour.
Version	3
Local Only	No

Figure 21: "Add Cluster"



Threat Actor :: Estudiant del curs de ciberseguretat Montilivi

Cluster ID	10489
Name	Estudiant del curs de ciberseguretat Montilivi
Parent Galaxy	Threat Actor
Description	Estudiants fent pràctiques en el projecte DAW-Ciber
Published	Yes
Default	No
Version	1652721539
UUID	e273adc7-fffd-4764-9120-068c433ff88a
Collection UUID	
Source	
Authors	N/A
Distribution	Your organisation only
Owner Organisation	ORGNAME
Creator Organisation	ORGNAME
Connector tag	misp-galaxy:threat-actor="e273adc7-fffd-4764-9120-068c433ff88a"
Events	0

Figure 22: "Our new Cluster"

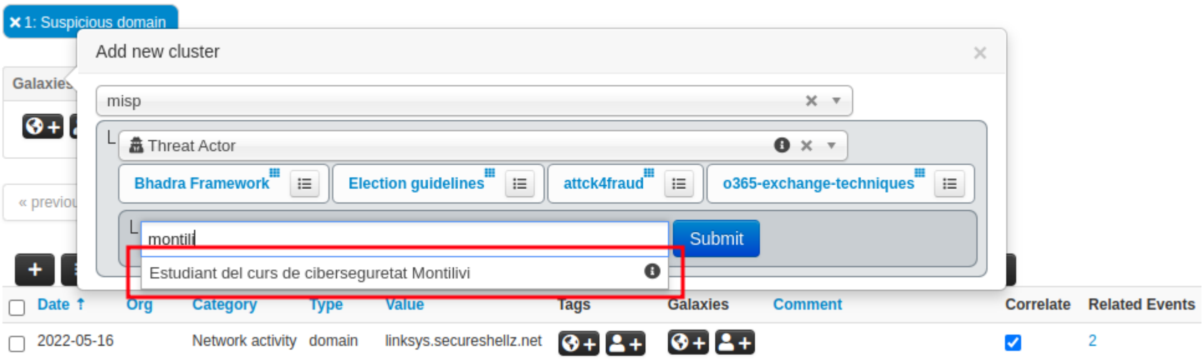
In order to use this new custer, we must publish it.

Publish is not a immediate action, it may take a few minutes.

Now, we add this cluster to the created event. List events, select yours and edit it. Add a cluster MISP, *Threat Actor*, and then start typing the name of your cluster until you see it.

Activity 4

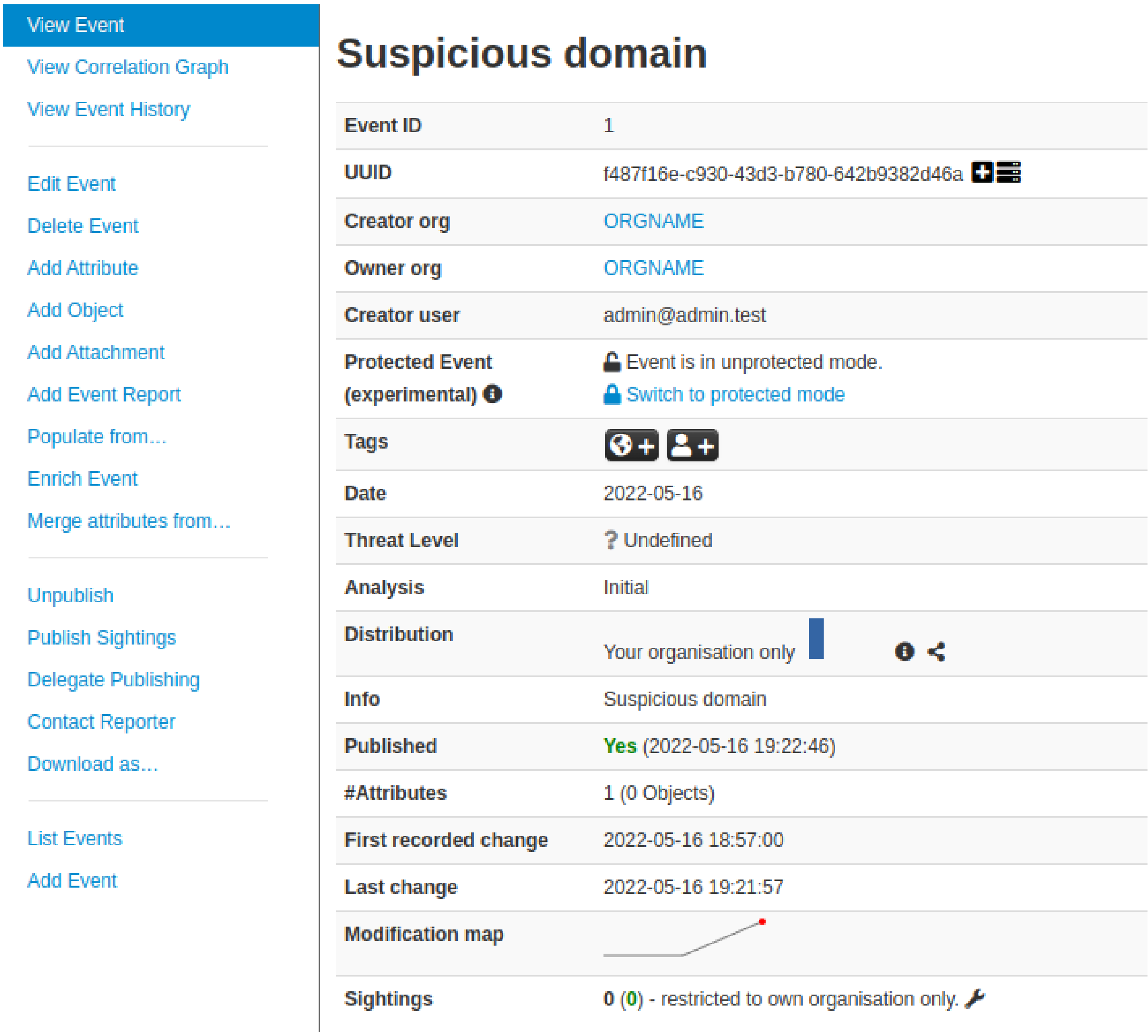
Attach a screenshot of your event from Montilivi's cluster that you just created.



□	Date ↑	Org	Category	Type	Value	Tags	Galaxies	Comment	Correlate	Related Events
□	2022-05-16		Network activity	domain	linksys.secureshellz.net				☑	2

Figure 23: "Add new cluster"

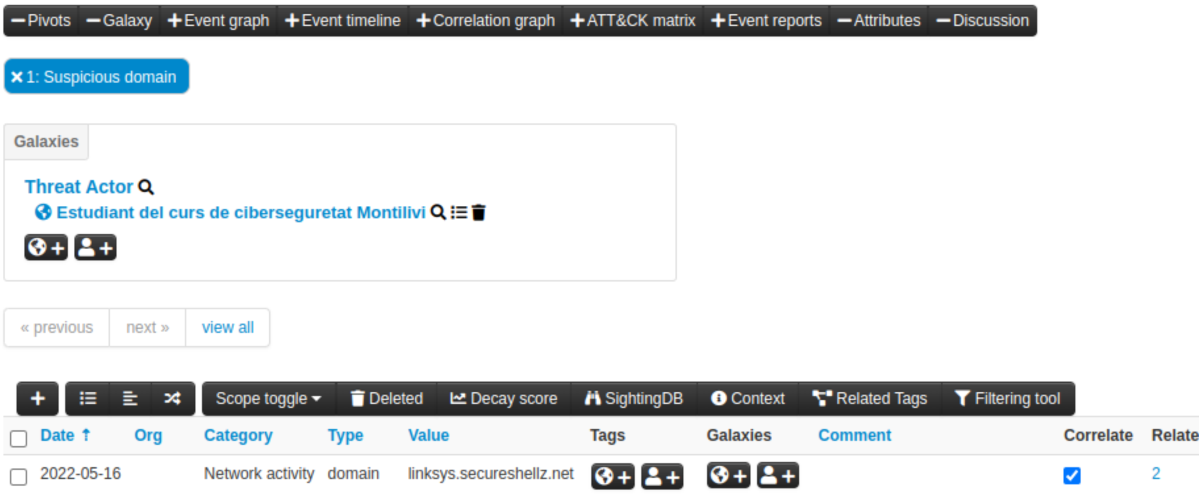
Publish the event.



Suspicious domain

Event ID	1
UUID	f487f16e-c930-43d3-b780-642b9382d46a
Creator org	ORGNAME
Owner org	ORGNAME
Creator user	admin@admin.test
Protected Event (experimental)	Event is in unprotected mode. Switch to protected mode
Tags	
Date	2022-05-16
Threat Level	? Undefined
Analysis	Initial
Distribution	Your organisation only
Info	Suspicious domain
Published	Yes (2022-05-16 19:22:46)
#Attributes	1 (0 Objects)
First recorded change	2022-05-16 18:57:00
Last change	2022-05-16 19:21:57
Modification map	
Sightings	0 (0) - restricted to own organisation only.

Figure 24: “Published event 1”



Galaxies

Threat Actor
Estudiant del curs de ciberseguretat Montilivi

□	Date ↑	Org	Category	Type	Value	Tags	Galaxies	Comment	Correlate	Relate
□	2022-05-16		Network activity	domain	linksys.secureshellz.net				☑	2

Figure 25: “Published event 2”