

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

Aquesta màquina virtual no està pensada per posar-la en producció, no és segura.

Defineix un password d'administrador per a tot el sistema

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

Defineix la teva organització

De la barra de menús selecciona *Add Organisations* i omplena els camps de la teva organització. En aquest exemple jo ho he fet pel nostre institut:

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

6cb9516d-90fc-4566-a534-6e24da4b5ef2

Generate UUID

Optional Fields

A brief description of the organisation

A description of the organisation that is purely informational.

Bind user accounts to domains (line separated)

Enter a (list of) domain name(s) to enforce when creating users.

Logo (48×48 PNG or SVG)

[Navega...](#) Logo_Montilivi_2015_negre.png

Nationality

Europe

Sector

Education

Type of organisation

Freetext description of the org.

Contact details

You can add some contact details for the organisation here, if applicable.

Submit

Crea un usuari amb permisos *Org admin* a la nova organització

Selecciona *Add User* de la barra de menús *Administration*.

Admin Add User

Email

☒ Set password

Password ⓘ Confirm Password

Organisation

Role NIDS SID

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.

☒ Receive email alerts when events are published
☒ Receive email alerts from "Contact reporter" requests
☐ Immediately disable this user account
☒ Send credentials automatically

Key concepts

Event: és un cas d'estudi.

Attributes: són els elements d'informació que donen forma a l'event.

Feeds: són fonts de dades que enriqueixen els nostres events.

Tags: són etiquetes que posem a un event per classificar-lo.

Galaxies: són plantilles per descriure elements d'atributs.

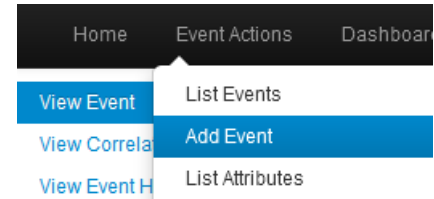
Cluster: és una instància d'una galaxia.

Event

Anem a entendre què és un event mentre en creem un. Suposem que un usuari de la nostra organització rep un correu amb un enllaç sospitós, per exemple: linksys.secureshellz.net

Evidentment, no volem obrir l'enllaç sense saber si aquest domini és lliure de malware.

De la barra de menús selecciona *Event Actions* i *Add Event*.



Omplena'l amb la informació que et demana:

[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

2022-04-22

Distribution ⓘ

Your organisation only ▾

Threat Level ⓘ

Undefined ▾

Analysis ⓘ

Initial ▾

Event Info

Domini sospitós

Extends Event

Event UUID or ID. Leave blank if not applicable.

Submit

Ara, si llistes els events hauries de veure alguna cosa similar a aquesta:

Home

Event Actions

Dashboard

Galaxies

Input Filters

Global Actions

Administration

Logs

API

★

MISP

List Events

Add Event

Import from...

REST client

List Attributes

Search Attributes

View Proposals

Events with proposals

Events

< previous

next >

🔍

Filters: Org: 2 ✕





My Events

Org Events

🏠

Enter value to search

Filter

Published	Creator org	ID	Clusters	Tags	#Attr.	#Corr.	Date	Last modified at ↑	Info	Distribution	Actions
<input type="checkbox"/>	✓		3		1	1	2022-04-26	2022-04-28 17:27:07	URL maliciós	Organisation	  

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

Aquest event tal com està, però, no aporta cap informació. Ara cal posar-li almenys un atribut.

Attributes

Els atributs donen forma i sentit a l'event. En l'exemple que estem definint, un atribut molt clar és el domini que considerem sospitos.

Clica al número d'ID de l'event per veure'n el contingut:

Filters: Org: 2

My Events

Org Events

Filter

Published	Creator org	ID	Clusters	Tags	#Attr.	#Corr.	Date	Last modified at ↑	Info	Distribution	Actions
<input type="checkbox"/>	✓		3		1	1	2022-04-26	2022-04-28 17:27:07	URL maliciós	Organisation	

Tot seguit, afegeix un atribut des del menú de l'esquerra a l'opció *Add Attribute*. Tria una categoria, un tipus, i escriu el valor i la data de recepció de l'enllaç.

[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 \(no email\)](#)
[Delegate Publishing](#)
[Contact Reporter](#)
[Download as...](#)

[List Events](#)
[Add Event](#)

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 📅
2022-04-22

Last seen date 📅
2022-04-22

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

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

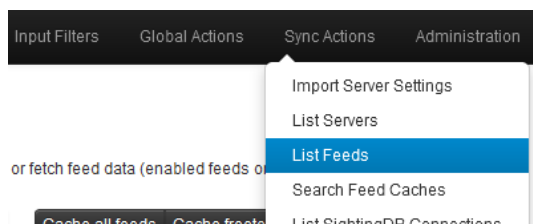
Expected format: HH:MM:SS.ssssss+TT:TT

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

Submit

Feeds

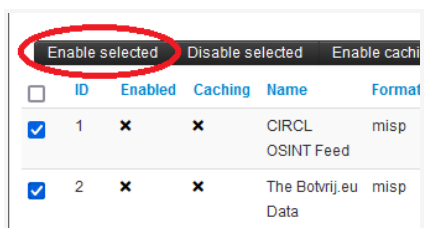
Per tal de saber si algú més s'ha trobat amb aquest enllaç i ja el té estudiat hem d'afegir el *feeds*, que són conjunts d'events OSINT que es poden importar. Amb l'usuari *admin@admin.test* podràs veure l'opció *Sync Actions* de la barra de menús. Selecciona l'opció *List Feeds*.



Per defecte l'aplicació en porta dos però estan desactivats.

Default feeds Custom feeds All feeds Enabled feeds															Enter value to search 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	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	CIRCL OSINT Feed	misp	CIRCL		network	https://www.circl.lu/doc/misp/feed-osint		Feed not enabled	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	All communities		<input checked="" type="checkbox"/>	Not cached	
<input type="checkbox"/>	2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	The Botvrij.eu Data	misp	Botvrij.eu		network	https://www.botvrij.eu/data/feed-osint		Feed not enabled	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	All communities		<input checked="" type="checkbox"/>	Not cached	

Selecciona'ls i clica *Enable selected*.







En poca estona començaràs a rebre events creats pels dos feeds que has activat. Si ara tries l'opció *llistar events* els podràs veure:

A screenshot of the 'Events' page in the application. The left sidebar shows navigation options like 'List Events', 'Add Event', 'Import from...', 'REST client', 'List Attributes', 'Search Attributes', 'View Proposals', 'Events with proposals', 'View delegation requests', 'Export', and 'Automation'. The main area displays a table of events with columns for 'Published', 'Creator org', 'Owner org', 'ID', 'Clusters', 'Tags', '#Att.', '#Corr.', 'Creator user', and 'Date'. Three events are visible, each with a red status icon and a list of associated threat intelligence sources like 'Enterprise Attack - Intrusion Set', 'Intrusion Set', 'Threat Actor', 'Attack Pattern', etc.

Automatic enrichment

Ara, la part que ens interessa és al nostre event. Clica l'event per desplegar el seu contingut i vés al seu atribut.

<input type="text" value="Q"/>	Filters: Org: 2	My Events	Org Events	<input type="text" value="Enter value to search"/>	Filter						
Published	Creator org	ID	Clusters	Tags	#Attr.	#Corr.	Date	Last modified at	Info	Distribution	Actions
<input type="checkbox"/>	<input checked="" type="checkbox"/>		<div><div></div><div>- 3</div></div>		1	1	2022-04-26	2022-04-28 17:27:07	URL maliciós	Organisation	  

Veuràs que a la columna *Related Events* hi ha un event relacionat. Clica'l.

<div><div><div><div><div></div><div></div><div></div><div></div></div></div><div><div>Scope toggle</div><div>Deleted</div><div>Decay score</div><div>SightingDB</div><div>Context</div><div>Related Tags</div><div>Filtering tool</div></div></div><div>Enter value to search</div></div>														
<input type="checkbox"/>	Date ↑	Org	Category	Type	Value	Tags	Galaxies	Comment	Correlate	Related Events	Feed hits	IDS	Distribution	Sighti
<input type="checkbox"/>	2022-04-28		Network activity	domain	linksys.secureshellz.net	<div><div><div></div><div></div></div><div><div></div><div></div></div></div>	<div><div><div></div><div></div></div><div><div></div><div></div></div></div>		<input checked="" type="checkbox"/>	6		<input type="checkbox"/>	Organisation	<div><div></div><div></div><div></div></div>

Aquest event està creat per l'organització CthulhuSPRL.be amb data de 2014 i conté 1067 atributs.

OSINT ShellShock scanning IPs from OpenDNS

Event ID	6
UUID	542e4c9c-cadc-4f8f-bb11-6d13950d210b
Creator org	CthulhuSPRL.be
Owner org	Institut Montilivi
Creator user	admin@admin.test
Tags	type:OSINT tip:green tip:white
	Taxonomy 'tip' is an exclusive Taxonomy └ tip:green └ tip:white
Date	2014-10-02
Threat Level	✓ Low
Analysis	Completed
Distribution	All communities
Info	OSINT ShellShock scanning IPs from OpenDNS
Published	Yes (2022-04-28 17:32:48)
#Attributes	1067 (0 Objects)
First recorded change	2014-10-03 09:14:05
Last change	2018-02-05 08:50:37

A continuació d'aquesta descripció pots veure la llista de tots els seus atributs, dels quals ens n'interessa un:

<input type="checkbox"/>	2014-10-03	Network activity	hostname	linksys.secureshellz.net	
--------------------------	------------	------------------	----------	--------------------------	--

Per tant, sí, aquest enllaç ja està classificat com a **OSINT ShellShock scanning IPs from OpenDNS**.

Tags

Les etiquetes ens serveixen per classificar i afegir informació a un event. Aquest és l'enllaç on MISP té recollits totes les etiquetes i taxonomies:

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

D'aquesta llista en treballarem un tipus: la taxonomia TLP.

La taxonomia TLP (Traffic Light Protocol) està pensada per classificar la informació d'un event en funció de la protecció de dades i reputació de l'empresa, així doncs, han definit les següents etiquetes:

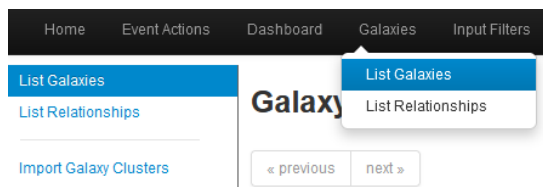
- Red
- Amber
- Green
- White

Activitat 1: Segons la informació donada a les taxonomies per MISP, explica breument què implica cada color en un event.

Activitat 2: A la captura de l'event de la pàgina anterior, a l'apartat *Tags* hi ha un advertiment. De què ens està avisant?

Galaxies

Les galaxies són plantilles per descriure més informació sobre un event o atribut. Per llistar-les vés a *List Galaxies* de la barra de menús *Galaxies*.



Veuràs la següent llista:

All Enabled Disabled							Enter value to search	Filter X
Galaxy Id 1	Icon	Name	version	Namespace	Description	Enabled	Local Only	Actions
56		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.	✓	x	
55		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.	✓	x	
54		Tea Matrix	1	tea-matrix	Tea Matrix	✓	x	
53		TDS	4	misp	TDS is a list of Traffic Direction System used by adversaries	✓	x	
52		Target Information	1	misp	Description of targets of threat actors.	✓	x	
51		Surveillance Vendor	1	misp	List of vendors selling surveillance technologies including malware, interception devices or computer exploitation services	✓	x	
50		Stealer	1	misp	Malware stealer galaxy.	✓	x	
49		SoD Matrix	1	sod-matrix	SoD Matrix	✓	x	
48		Dark Patterns	1	misp	Social Engineering - Dark Patterns	✓	x	
47		Sector	2	misp	Activity sectors	✓	x	
46		rsit	1	RSIT	Reference Security Incident Classification Taxonomy	✓	x	
45		Regions UN M49	2	misp	Regions based on UN M49.	✓	x	
44		RAT	3	misp	remote administration tool or remote access tool (RAT), also called sometimes remote access trojan, is a piece of software or	✓	x	

Anem a examinar-ne una: *Threat Actor*

Threat Actor galaxy

Galaxy ID	55
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

Aquest cas és bastant senzill, pràcticament només es compona d'un nom i una descripció. A sota però hi podem veure totes les instàncies publicades d'aquesta galàxia:

ID	Published	Value	Synonyms	Creator Org	Default	Activity	#Events	#Relations	Description	Distribution	Ac
9823	N/A	Stealth Mango and Tangelo		MISP	✓		0	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.	All communities	
9604	N/A	ALLANITE	Palmetto Fusion, Allanite	MISP	✓		0	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.	All communities	
9581	N/A	ANDROMEDA SPIDER		MISP	✓		0	0 0 0		All communities	
9728	N/A	ANTHROPOID SPIDER	Empire Monkey, CobaltGoblin	MISP	✓		0	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 framework. ANTHROPOID SPIDER likely enabled a breach that allegedly involved fraudulent transfers over the SWIFT network.	All communities	
9446	N/A	APT 16	APT16, SVCMONDR	MISP	✓		0	0 0 0	Between November 26, 2015, and December 1, 2015, known and suspected China-based APT groups launched several spear-phishing attacks targeting Japanese and Taiwanese organizations in the high-tech, government services, media and financial services industries. Each campaign delivered a malicious Microsoft Word document exploiting the aforementioned EPS dict copy use-after-free vulnerability, and the local Windows privilege escalation vulnerability CVE-2015-1701. The successful exploitation of both vulnerabilities led to the delivery of either a downloader that we refer to as IRONHALO, or a backdoor that we refer to as ELMER.	All communities	
9559	N/A	APT 22	APT22, BRONZE OLIVE	MISP	✓		0	0 0 0		All communities	

Selecciona'n una i podràs veure el seu historial:

Threat Actor :: ALLANITE

Cluster ID	9604
Name	ALLANITE
Parent Galaxy	Threat Actor
Description	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.
Default	Yes
Version	214
UUID	a9000eaf-2b75-4ec7-8dcf-fe1bb5c77470
Collection UUID	7cdf317-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="ALLANITE"
Events	0

Cluster

Els clusters són el que acabes de veure, una instància d'una galàxia.

Activitat 3: Crea un cluster com a instància de la galàxia *Threat Actor* definint l'atacant "Estudiant del curs de ciberseguretat Montilivi". Adjunta una captura del teu nou cluster.

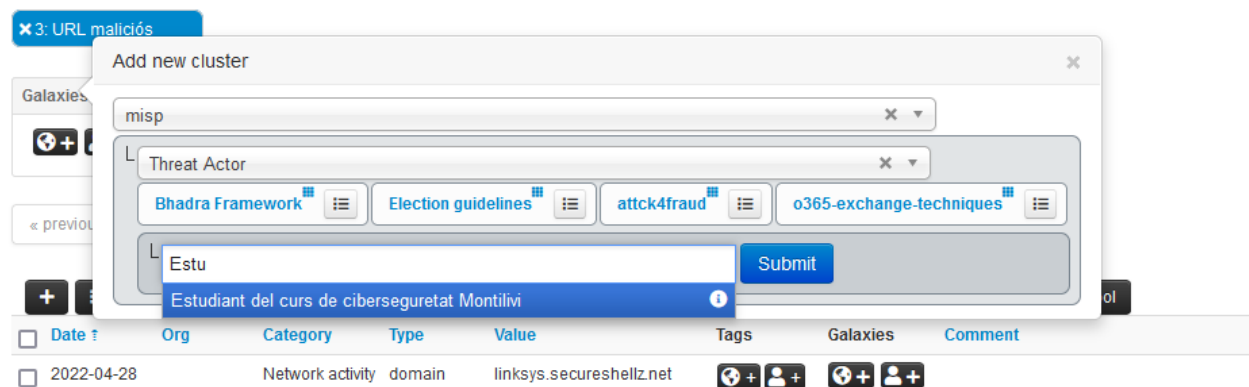
Per poder utilitzar aquest nou cluster l'has de publicar. Per fer-ho, visualitza el cluster i tria l'opció *Publish Cluster* de la barra de menús de l'esquerra:



Threat Actor :: Estudiant del curs de ciberseguretat Montilivi	
Cluster ID	10338
Name	Estudiant del curs de ciberseguretat Montilivi
Parent Galaxy	Threat Actor
Description	Estudiants fent pràctiques en el projecte DAW-Ciber
Published	No
Default	No
Version	1651572901
UUID	2d81640f-1e66-477d-bfbc-45b4fd6fefad
Collection UUID	
Source	

La publicació no és immediata, pot ser que trigui uns minuts.

Ara, afegeix aquest cluster a l'event que vas crear. Llista els events, selecciona el teu i edita'l. Afegeix un cluster *misp*, *Threat Actor*, i tot seguit comences a escriure el nom del teu cluster fins que el vegis.



Date	Org	Category	Type	Value	Tags	Galaxies	Comment
2022-04-28		Network activity	domain	linksys.secureshellz.net			

Activitat 4: mostra una captura del teu event amb el clúster Montilivi que acabes de crear.