Introducción a MISP

Compartiendo Información de Inteligencia de Amenazas

Acerca de CIRCL

El Centro de Respuesta ante Emergencias Informáticas de Luxemburgo (CIRCL) es una iniciativa impulsada por el gobierno, diseñada para proveer una respuesta sistemática a incidentes y amenazas de seguridad informática.

CIRCL es el CERT del sector privado, municipios y entidades no gubernamentales en Luxemburgo y es operado por Luxembourg House of Cybersecurity (LHC g.i.e.)

circl.lu
Computer Incident
Response Center
LUXEMBOURG

MISP y CIRCL

CIRCL lidera el desarrollo de MISP, la plataforma de código abierto de inteligencia de amenazas, que es utilizada por muchas comunidades civiles, militares o de inteligencia, fuerzas de seguridad (LEAs), empresas privadas, sector financiero y CERTs nacionales en todo el mundo.

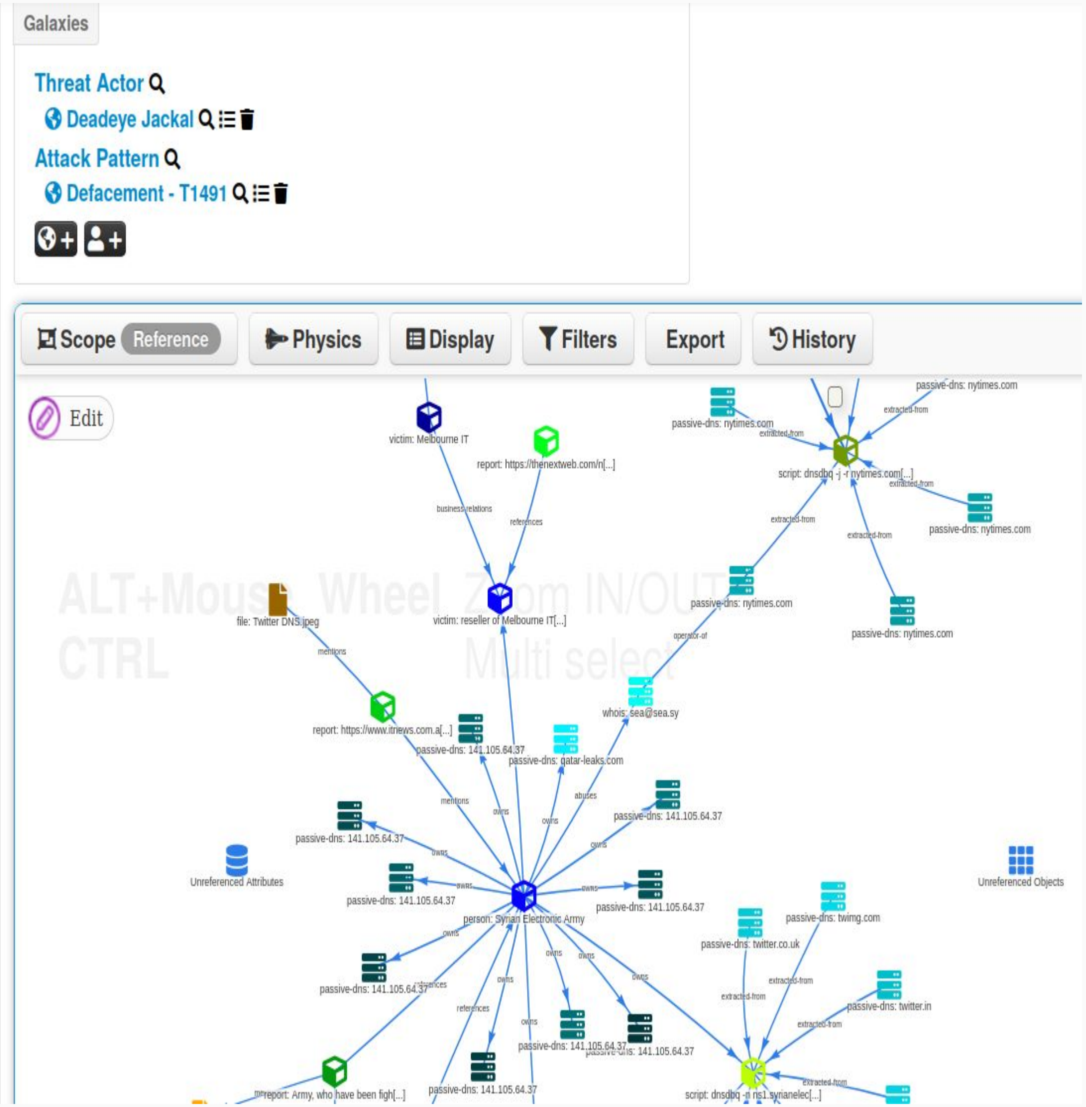
CIRCL opera múltiples comunidades de MISP, que a diario comparten información de inteligencia de amenazas.

Co-financed by the European Union
Connecting Europe Facility

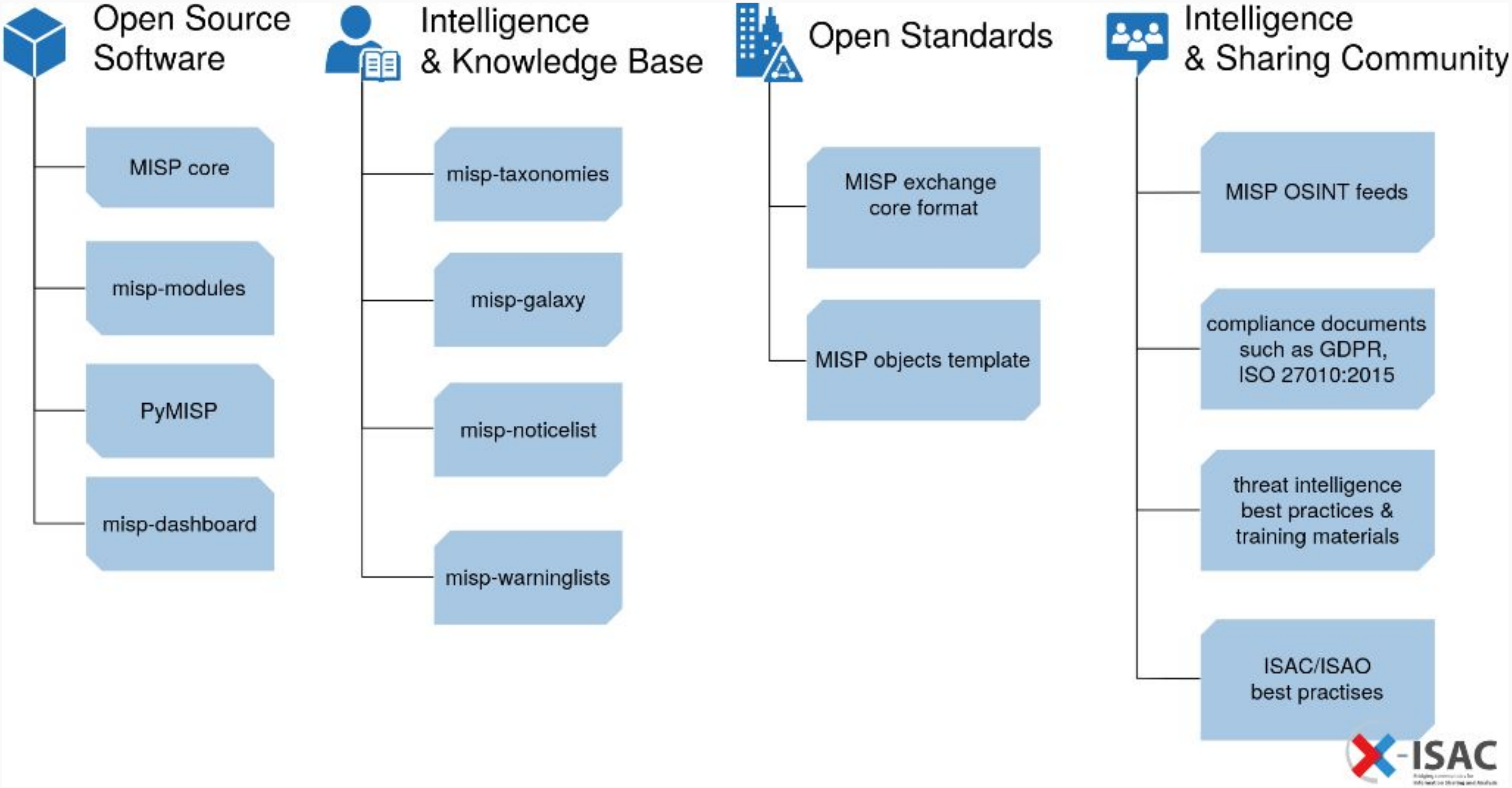
Qué es MISP

- Libre y de código abierto
- Permite compartir Inteligencia de Amenazas
- Normaliza, correlaciona y enriquece información
- Permite colaborar a los diferentes equipos y comunidades
- Alimenta otras herramientas de seguridad
- Da soporte a analistas de seguridad

https://demo.misp-community.org



Composición de MISP



Open Source Software

- MISP core
- misp-modules
- PyMISP
- misp-dashboard

Intelligence & Knowledge Base

- misp-taxonomies
- misp-galaxy
- misp-noticelist
- misp-warninglists

Open Standards

- MISP exchange core format
- MISP objects template

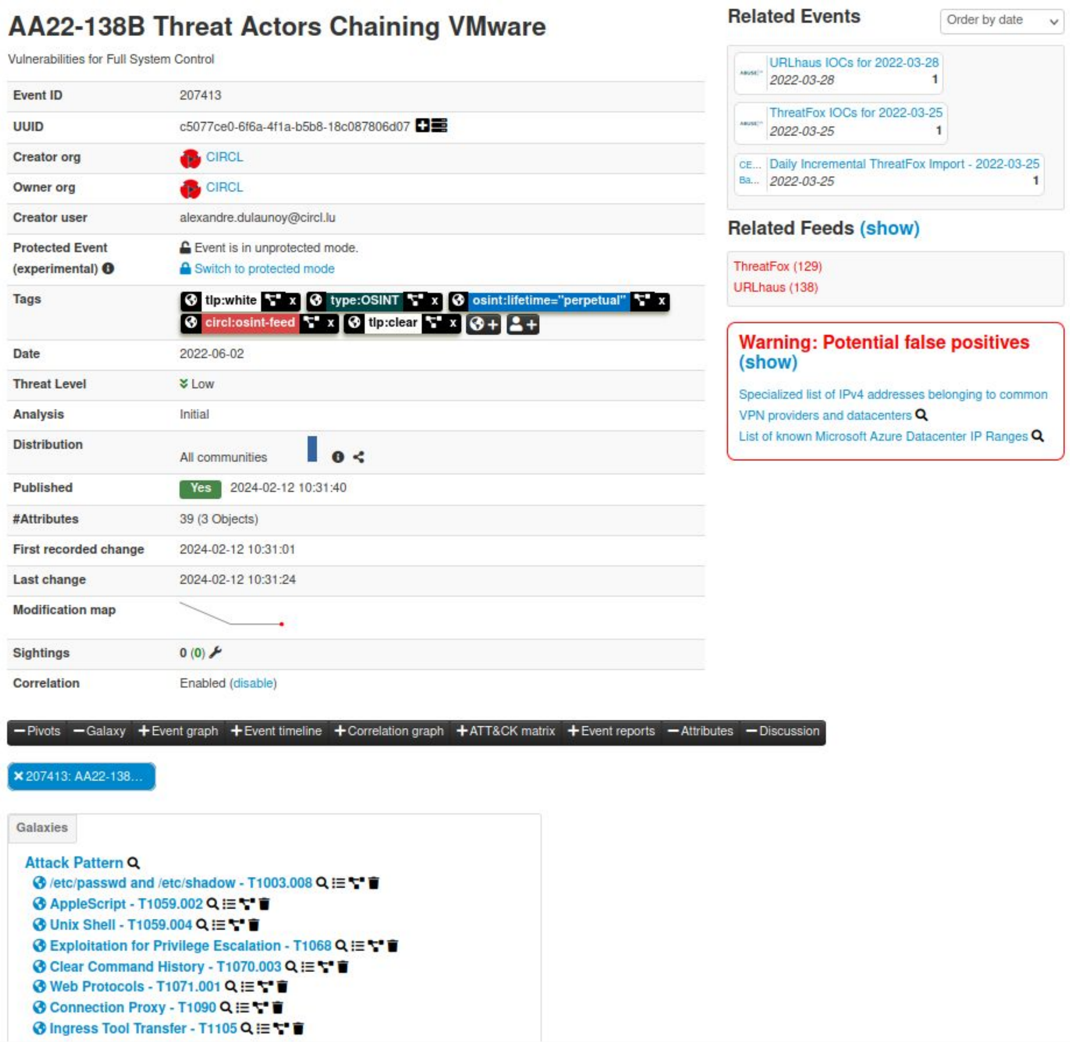
Intelligence & Sharing Community

- MISP OSINT feeds
- compliance documents such as GDPR, ISO 27010:2015
- threat intelligence best practices & training materials
- ISAC/ISAO best practises

MISP 101 - Eventos

- Actúa como el contenedor de toda la información que se comparte en MISP

- Incluye:
  - Metadatos
  - Atributos
  - Objetos
  - Correlaciones
  - Reportes
  - Contexto (tags, galaxies, taxonomies)
  - Sightings
  - Proposals
  - Y más…



AA22-138B Threat Actors Chaining VMware

Vulnerabilities for Full System Control

Event ID	207413
UUID	c5077ce0-6f6a-4f1a-b5b8-18c087806d07
Creator org	CIRCL
Owner org	CIRCL
Creator user	alexandre.dulaunoy@circl.lu
Protected Event (experimental)	Event is in unprotected mode. Switch to protected mode
Tags	tlp:white x · type:OSINT x · osint:lifetime="perpetual" x · circl:osint-feed x · tlp:clear x
Date	2022-06-02
Threat Level	Low
Analysis	Initial
Distribution	All communities
Published	Yes 2024-02-12 10:31:40
#Attributes	39 (3 Objects)
First recorded change	2024-02-12 10:31:01
Last change	2024-02-12 10:31:24
Modification map	
Sightings	0 (0)
Correlation	Enabled (disable)

Related Events

Order by date

	URLhaus IOCs for 2022-03-28 *2022-03-28*	1
	ThreatFox IOCs for 2022-03-25 *2022-03-25*	1
CE… Ba…	Daily Incremental ThreatFox Import - 2022-03-25 *2022-03-25*	1

Related Feeds (show)

ThreatFox (129)
URLhaus (138)

Warning: Potential false positives (show)

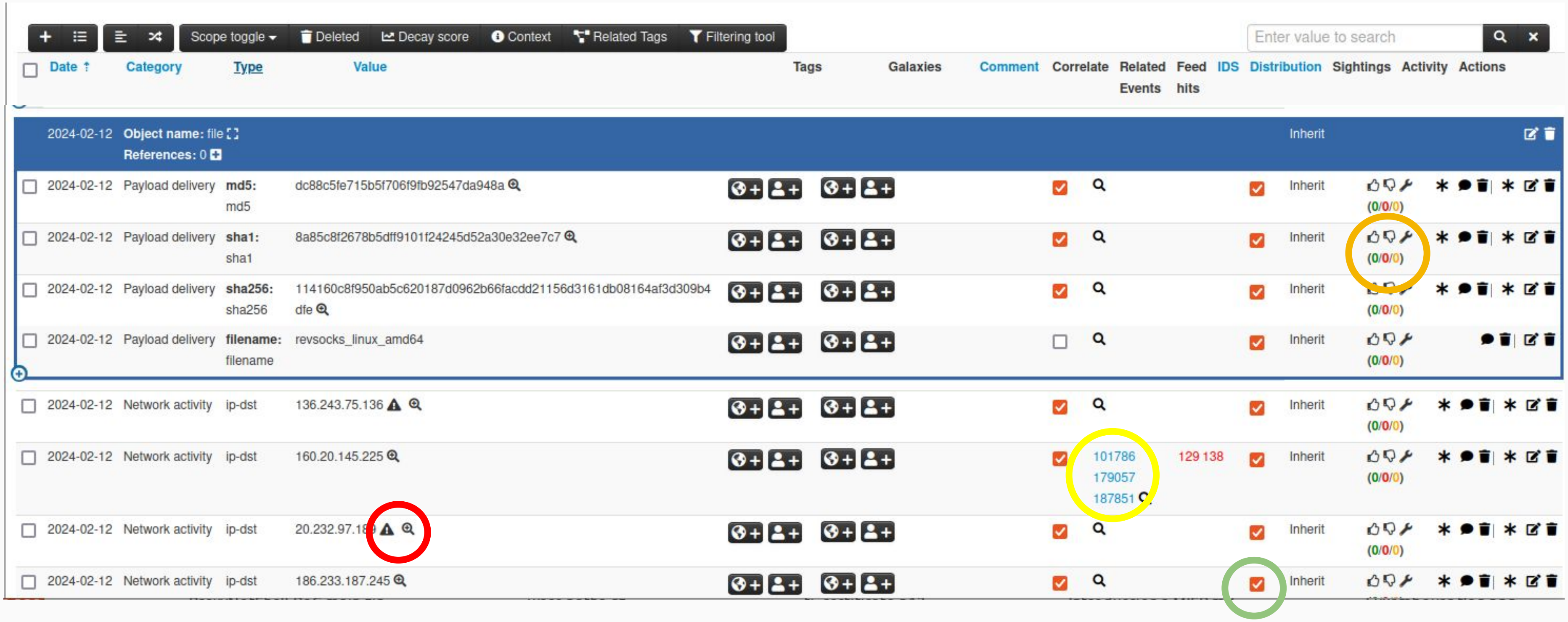
Specialized list of IPv4 addresses belonging to common VPN providers and datacenters
List of known Microsoft Azure Datacenter IP Ranges

Attack Pattern

- /etc/passwd and /etc/shadow - T1003.008
- AppleScript - T1059.002
- Unix Shell - T1059.004
- Exploitation for Privilege Escalation - T1068
- Clear Command History - T1070.003
- Web Protocols - T1071.001
- Connection Proxy - T1090
- Ingress Tool Transfer - T1105

MISP 101 - Atributos, Enriquecimiento y Correlaciones

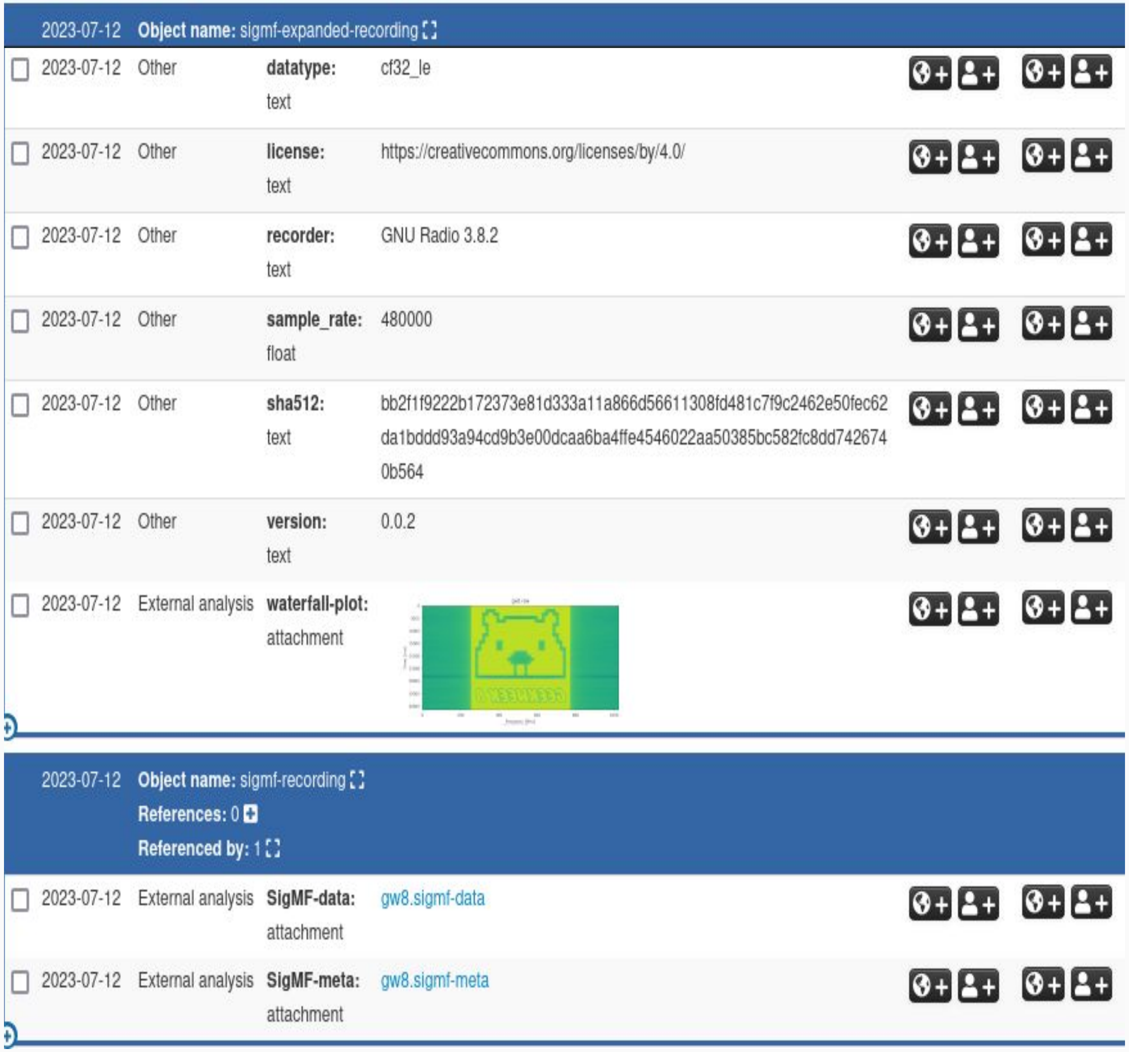
Los atributos son la unidad básica de información, se pueden incorporar metadatos mediante los módulos de enriquecimiento, y además ser correlacionados con otros atributos.



□	Date	Category	Type	Value	Tags	Galaxies	Comment	Correlate	Related Events	Feed hits	IDS	Distribution	Sightings	Activity	Actions
	2024-02-12	**Object name:** file **References:** 0										Inherit			
□	2024-02-12	Payload delivery	**md5:** md5	dc88c5fe715b5f706f9fb92547da948a				☑			☑	Inherit	(0/0/0)		
□	2024-02-12	Payload delivery	**sha1:** sha1	8a85c8f2678b5dff9101f24245d52a30e32ee7c7				☑			☑	Inherit	(0/0/0)		
□	2024-02-12	Payload delivery	**sha256:** sha256	114160c8f950ab5c620187d0962b66facdd21156d3161db08164af3d309b4dfe				☑			☑	Inherit	(0/0/0)		
□	2024-02-12	Payload delivery	**filename:** filename	revsocks_linux_amd64				□			☑	Inherit	(0/0/0)		
□	2024-02-12	Network activity	ip-dst	136.243.75.136 ⚠				☑			☑	Inherit	(0/0/0)		
□	2024-02-12	Network activity	ip-dst	160.20.145.225				☑	101786 179057 187851	129 138	☑	Inherit	(0/0/0)		
□	2024-02-12	Network activity	ip-dst	20.232.97.18 ⚠				☑			☑	Inherit	(0/0/0)		
□	2024-02-12	Network activity	ip-dst	186.233.187.245				☑			☑	Inherit			

MISP 101 - Objetos, Templates y Relaciones

- Permiten modelar entidades compuestas por más de un atributo
- Se pueden crear relaciones entre ellos
- Totalmente customizables mediante templates
- Extensa librería de plantillas objetos ya disponible para ser usada



2023-07-12 **Object name:** sigmf-expanded-recording

□	2023-07-12	Other	**datatype:** text	cf32_le
□	2023-07-12	Other	**license:** text	https://creativecommons.org/licenses/by/4.0/
□	2023-07-12	Other	**recorder:** text	GNU Radio 3.8.2
□	2023-07-12	Other	**sample_rate:** float	480000
□	2023-07-12	Other	**sha512:** text	bb2f1f9222b172373e81d333a11a866d56611308fd481c7f9c2462e50fec62da1bddd93a94cd9b3e00dcaa6ba4ffe4546022aa50385bc582fc8dd7426740b564
□	2023-07-12	Other	**version:** text	0.0.2
□	2023-07-12	External analysis	**waterfall-plot:** attachment	

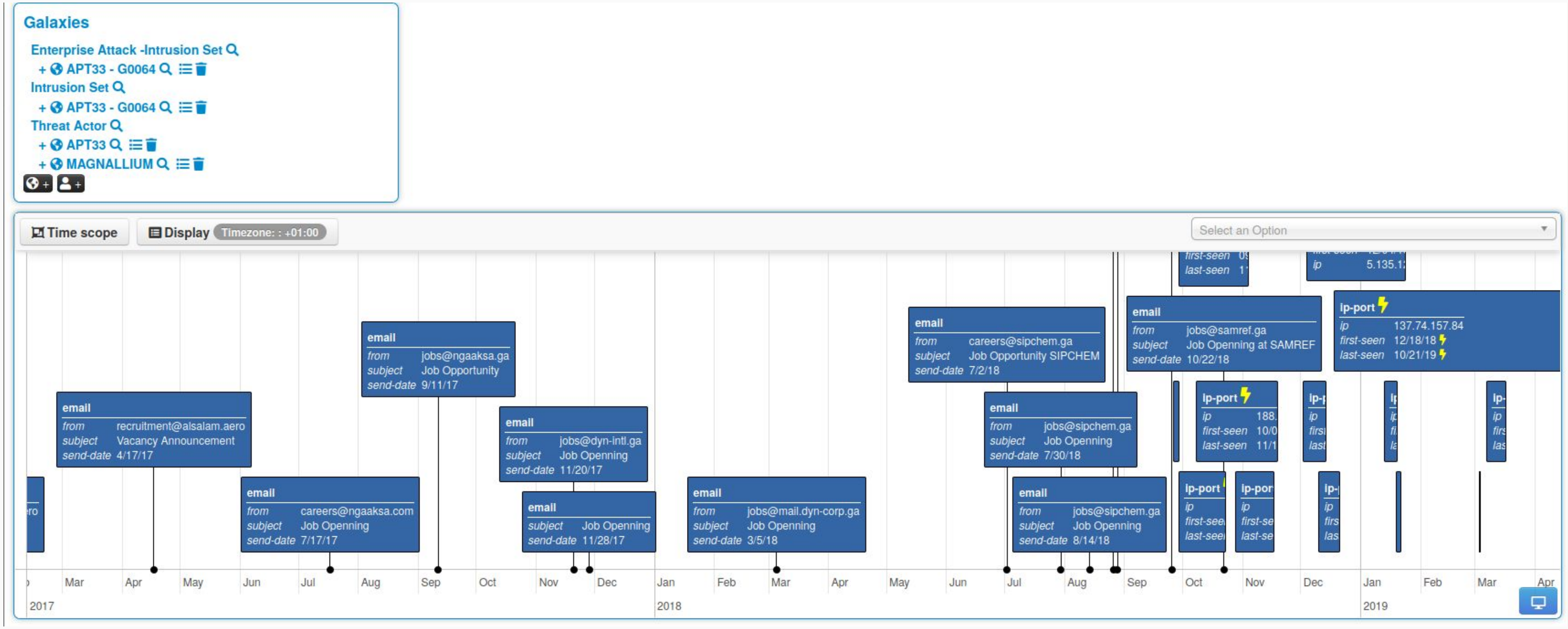
2023-07-12 **Object name:** sigmf-recording

References: 0

Referenced by: 1

□	2023-07-12	External analysis	**SigMF-data:** attachment	gw8.sigmf-data
□	2023-07-12	External analysis	**SigMF-meta:** attachment	gw8.sigmf-meta

MISP 101 - Línea de tiempos / Timeline



Galaxies

Enterprise Attack -Intrusion Set
- APT33 - G0064

Intrusion Set
- APT33 - G0064

Threat Actor
- APT33
- MAGNALLIUM

Time scope | Display | Timezone: : +01:00

Select an Option

email
from recruitment@alsalam.aero
subject Vacancy Announcement
send-date 4/17/17

email
from careers@ngaaksa.com
subject Job Openning
send-date 7/17/17

email
from jobs@ngaaksa.ga
subject Job Opportunity
send-date 9/11/17

email
from jobs@dyn-intl.ga
subject Job Openning
send-date 11/20/17

email
subject Job Openning
send-date 11/28/17

email
from jobs@mail.dyn-corp.ga
subject Job Openning
send-date 3/5/18

email
from careers@sipchem.ga
subject Job Opportunity SIPCHEM
send-date 7/2/18

email
from jobs@sipchem.ga
subject Job Openning
send-date 7/30/18

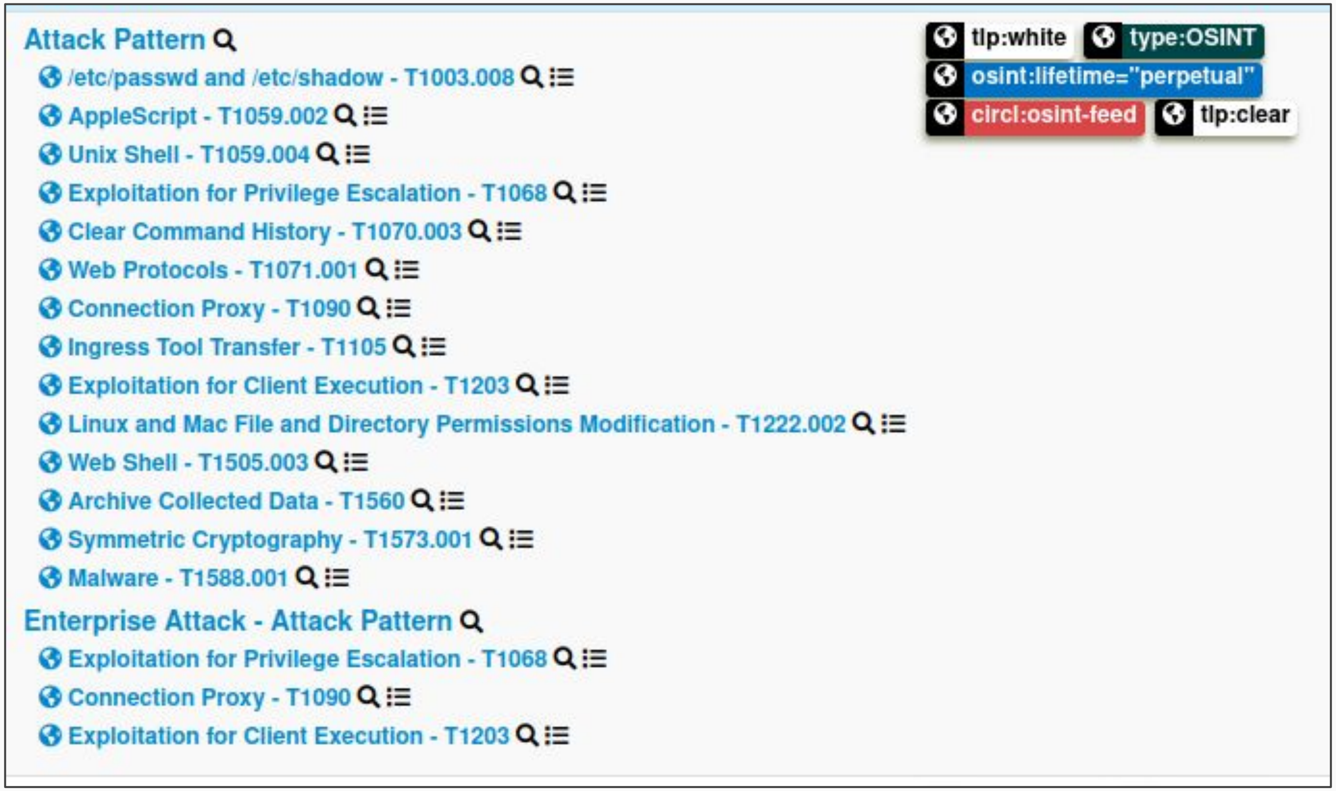
email
from jobs@sipchem.ga
subject Job Openning
send-date 8/14/18

email
from jobs@samref.ga
subject Job Openning at SAMREF
send-date 10/22/18

ip-port
ip 137.74.157.84
first-seen 12/18/18
last-seen 10/21/19

MISP 101 - Contextualización / Metadata

- Tags
  - Custom
- Galaxies
  - Threat Actors
  - Countries
  - Ransomware
- Taxonomies
  - MITRE ATT&CK
  - TLP
  - OSINT
  - Phishing



Attack Pattern

- /etc/passwd and /etc/shadow - T1003.008
- AppleScript - T1059.002
- Unix Shell - T1059.004
- Exploitation for Privilege Escalation - T1068
- Clear Command History - T1070.003
- Web Protocols - T1071.001
- Connection Proxy - T1090
- Ingress Tool Transfer - T1105
- Exploitation for Client Execution - T1203
- Linux and Mac File and Directory Permissions Modification - T1222.002
- Web Shell - T1505.003
- Archive Collected Data - T1560
- Symmetric Cryptography - T1573.001
- Malware - T1588.001

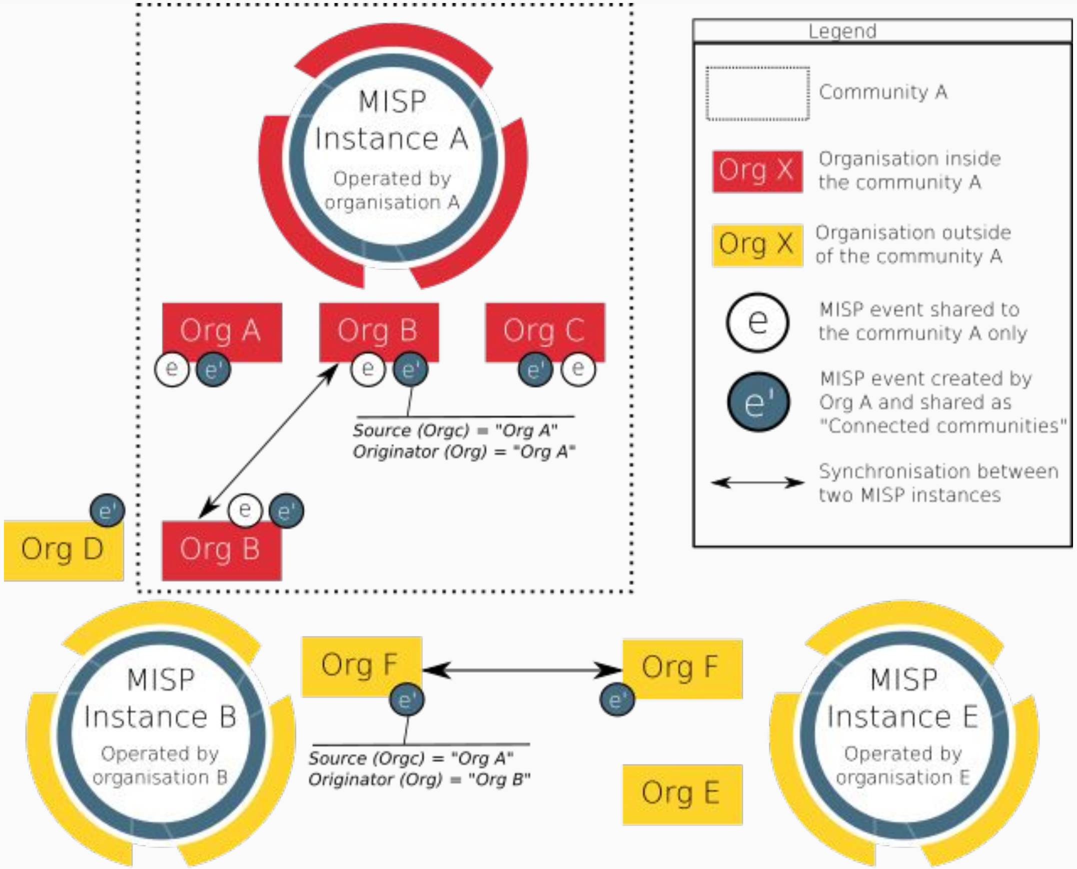
Enterprise Attack - Attack Pattern

- Exploitation for Privilege Escalation - T1068
- Connection Proxy - T1090
- Exploitation for Client Execution - T1203

tlp:white type:OSINT
osint:lifetime="perpetual"
circl:osint-feed tlp:clear

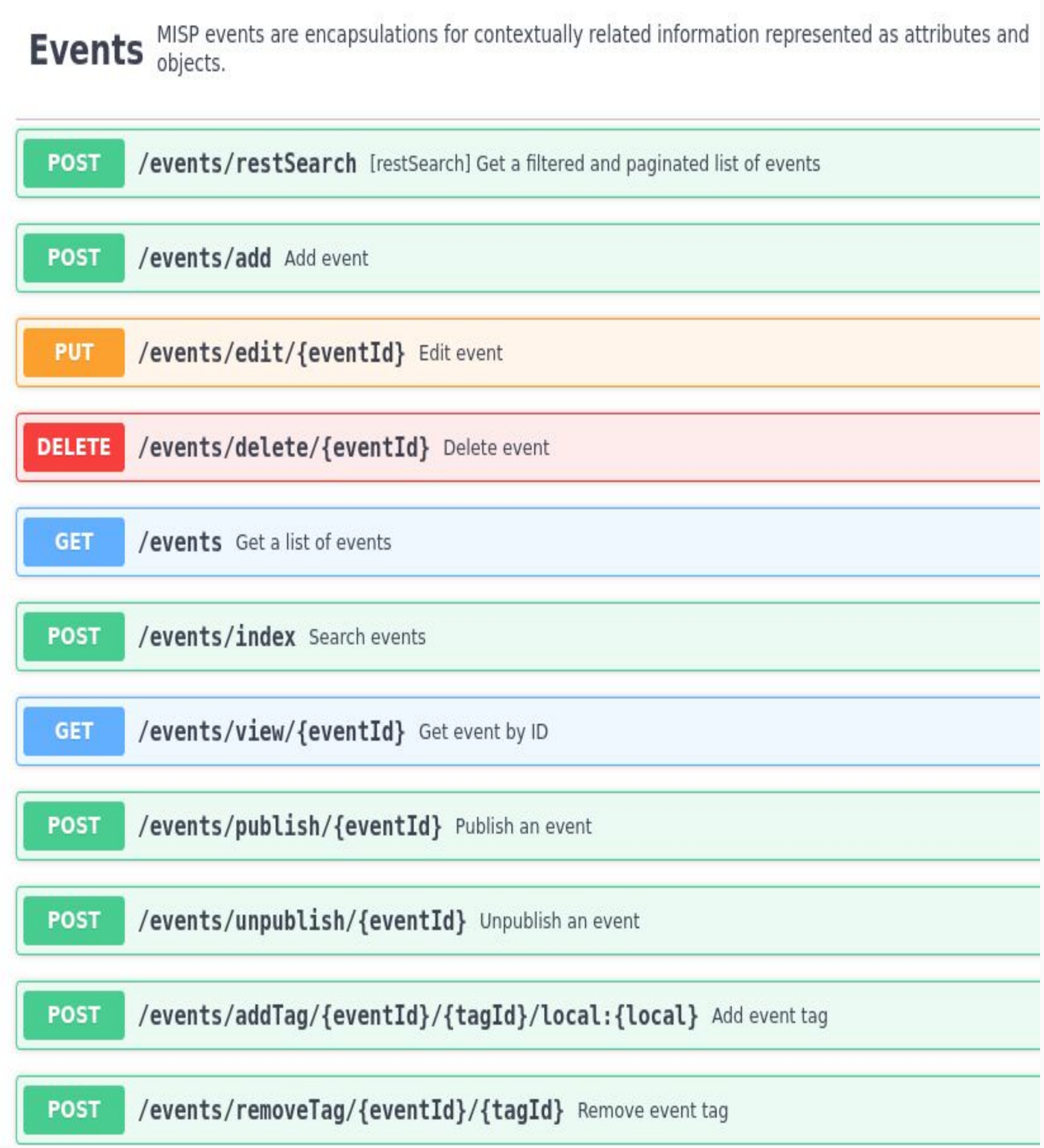
MISP 101 - Sincronización

- Servidores remotos
- Niveles de distribución configurables
- Grupos de Confianza (Sharing Groups)
- Comunidades
- Feeds


MISP Instance A
Operated by organisation A
Org A
Org B
Org C
e
e'
Source (Orgc) = "Org A"
Originator (Org) = "Org A"
Org D
Org B
MISP Instance B
Operated by organisation B
Org F
Source (Orgc) = "Org A"
Originator (Org) = "Org B"
Org F
Org E
MISP Instance E
Operated by organisation E
Legend
Community A
Org X
Organisation inside the community A
Org X
Organisation outside of the community A
e
MISP event shared to the community A only
e'
MISP event created by Org A and shared as "Connected communities"
Synchronisation between two MISP instances

MISP 101 - Automatización: API

- Permite automatizar tareas
- Facilita la interconexión con otros sistemas y herramientas de seguridad
- Permite actuar en tiempo real
- Facilita tareas administrativas, como creación de usuarios, etc.



Events MISP events are encapsulations for contextually related information represented as attributes and objects.

POST /events/restSearch [restSearch] Get a filtered and paginated list of events

POST /events/add Add event

PUT /events/edit/{eventId} Edit event

DELETE /events/delete/{eventId} Delete event

GET /events Get a list of events

POST /events/index Search events

GET /events/view/{eventId} Get event by ID

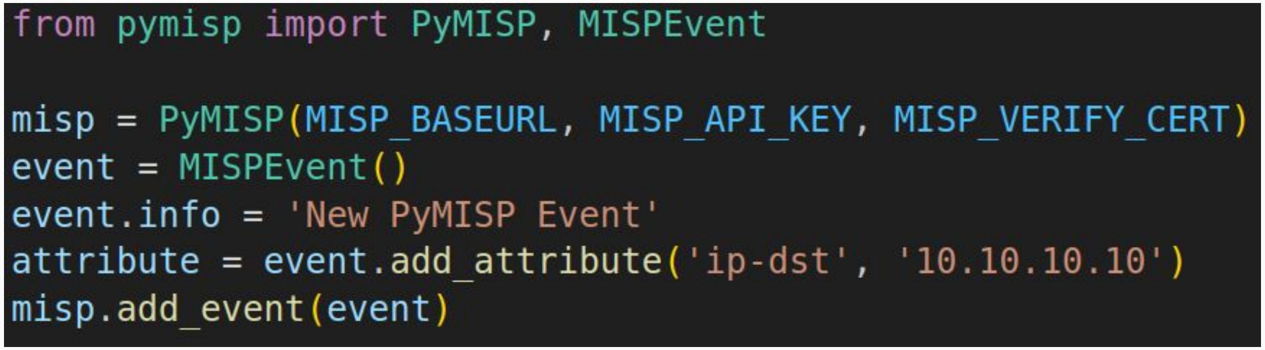
POST /events/publish/{eventId} Publish an event

POST /events/unpublish/{eventId} Unpublish an event

POST /events/addTag/{eventId}/{tagId}/local:{local} Add event tag

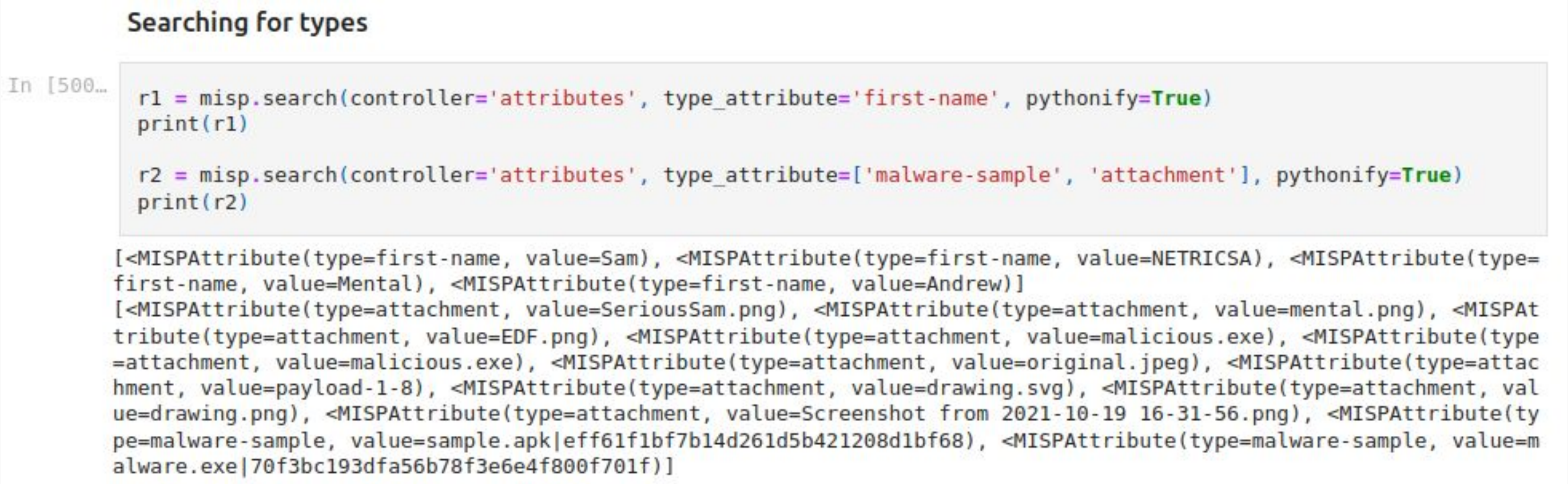
POST /events/removeTag/{eventId}/{tagId} Remove event tag

MISP 101 - Automatización: PyMISP, Jupyter Notebooks



```python
from pymisp import PyMISP, MISPEvent

misp = PyMISP(MISP_BASEURL, MISP_API_KEY, MISP_VERIFY_CERT)
event = MISPEvent()
event.info = 'New PyMISP Event'
attribute = event.add_attribute('ip-dst', '10.10.10.10')
misp.add_event(event)
```



Searching for types

In [500…

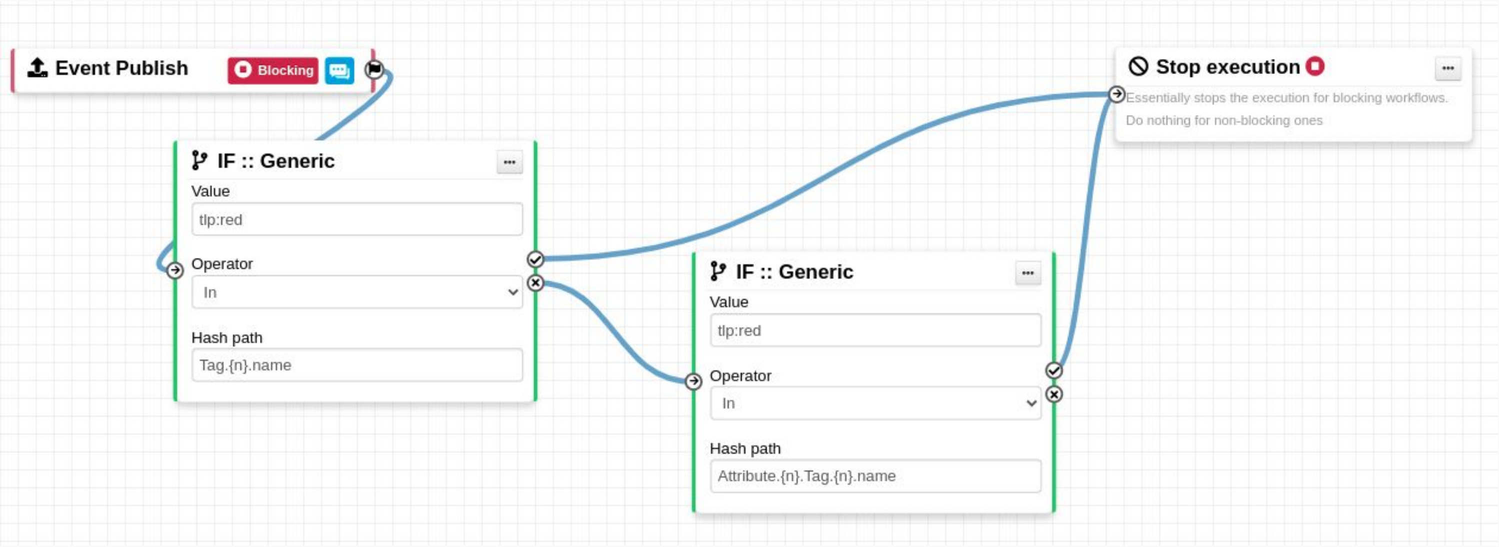
```python
r1 = misp.search(controller='attributes', type_attribute='first-name', pythonify=True)
print(r1)

r2 = misp.search(controller='attributes', type_attribute=['malware-sample', 'attachment'], pythonify=True)
print(r2)
```

```
[<MISPAttribute(type=first-name, value=Sam), <MISPAttribute(type=first-name, value=NETRICSA), <MISPAttribute(type=
first-name, value=Mental), <MISPAttribute(type=first-name, value=Andrew)]
[<MISPAttribute(type=attachment, value=SeriousSam.png), <MISPAttribute(type=attachment, value=mental.png), <MISPAt
tribute(type=attachment, value=EDF.png), <MISPAttribute(type=attachment, value=malicious.exe), <MISPAttribute(type
=attachment, value=malicious.exe), <MISPAttribute(type=attachment, value=original.jpeg), <MISPAttribute(type=attac
hment, value=payload-1-8), <MISPAttribute(type=attachment, value=drawing.svg), <MISPAttribute(type=attachment, val
ue=drawing.png), <MISPAttribute(type=attachment, value=Screenshot from 2021-10-19 16-31-56.png), <MISPAttribute(ty
pe=malware-sample, value=sample.apk|eff61f1bf7b14d261d5b421208d1bf68), <MISPAttribute(type=malware-sample, value=m
alware.exe|70f3bc193dfa56b78f3e6e4f800f701f)]
```

MISP 101 - Automatización: Workflows

- Interfaz gráfica intuitiva (Drag & Drop)
- Sistema flexible (Plug & Play)
- Facilita tareas repetitivas
- Puede interactuar con aplicaciones third-party



Event Publish Blocking

IF :: Generic

Value: tlp:red

Operator: In

Hash path: Tag.{n}.name

IF :: Generic

Value: tlp:red

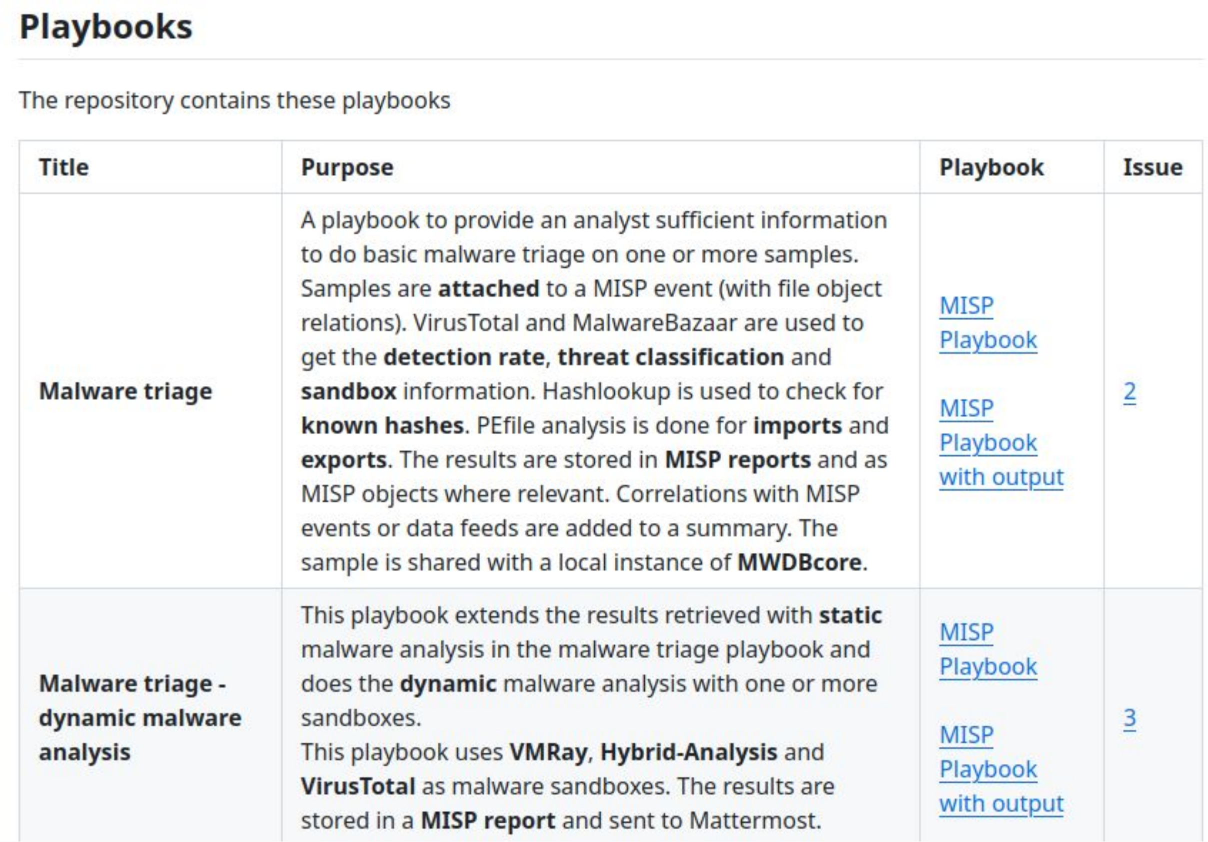
Operator: In

Hash path: Attribute.{n}.Tag.{n}.name

Stop execution

Essentially stops the execution for blocking workflows.
Do nothing for non-blocking ones

MISP 101 - Automatización: Playbooks



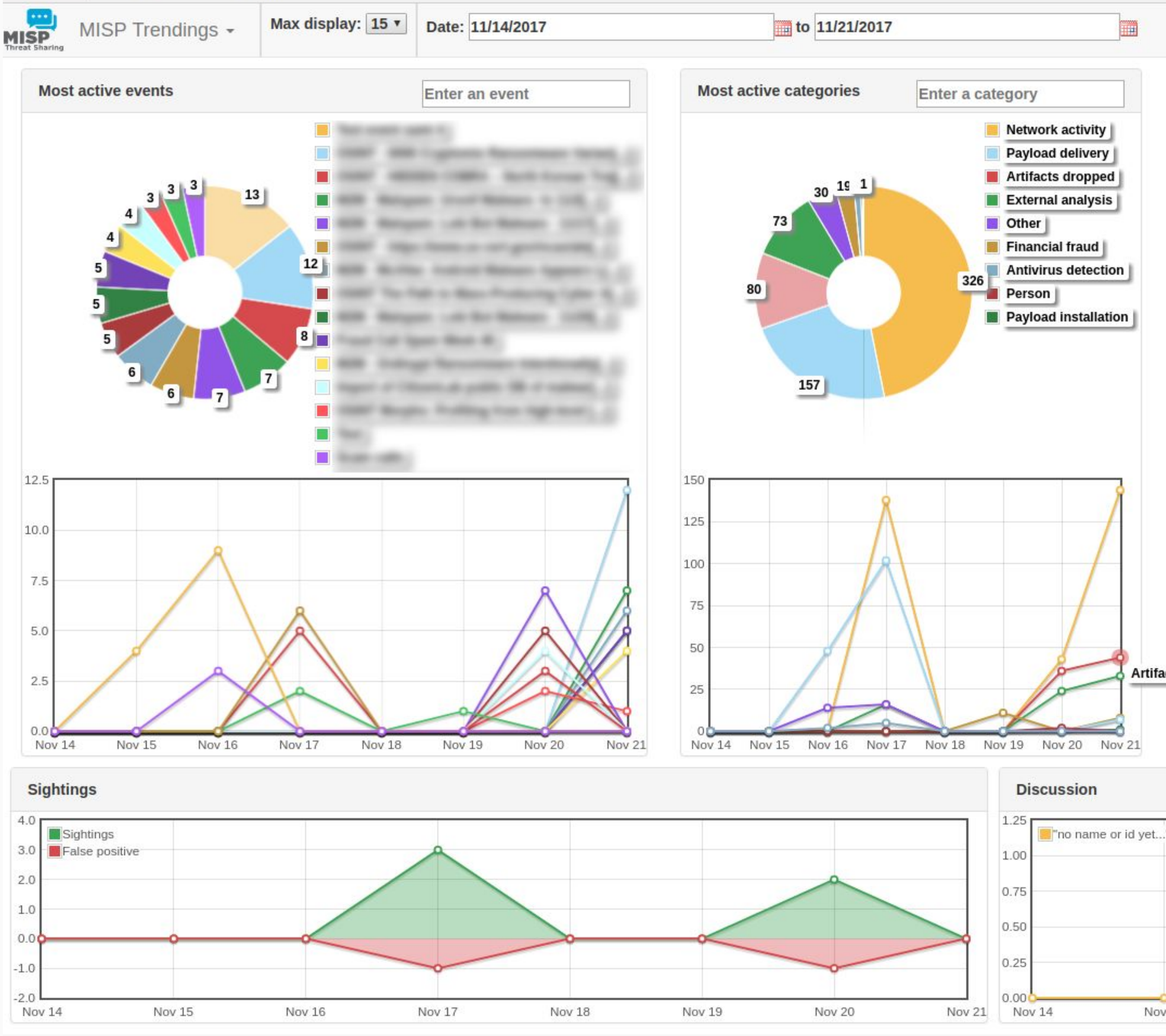
Playbooks

The repository contains these playbooks

Title	Purpose	Playbook	Issue
Malware triage	A playbook to provide an analyst sufficient information to do basic malware triage on one or more samples. Samples are **attached** to a MISP event (with file object relations). VirusTotal and MalwareBazaar are used to get the **detection rate**, **threat classification** and **sandbox** information. Hashlookup is used to check for **known hashes**. PEfile analysis is done for **imports** and **exports**. The results are stored in **MISP reports** and as MISP objects where relevant. Correlations with MISP events or data feeds are added to a summary. The sample is shared with a local instance of **MWDBcore**.	MISP Playbook MISP Playbook with output	2
Malware triage - dynamic malware analysis	This playbook extends the results retrieved with **static** malware analysis in the malware triage playbook and does the **dynamic** malware analysis with one or more sandboxes. This playbook uses **VMRay**, **Hybrid-Analysis** and **VirusTotal** as malware sandboxes. The results are stored in a **MISP report** and sent to Mattermost.	MISP Playbook MISP Playbook with output	3

MISP 101 - Otras funcionalidades

- Dashboard
- STIX / TAXII
- Event Reports
- Analysts Notes
- Sightings
- Warninglists
- Y mucho más…



MISP Trendings

Max display: 15

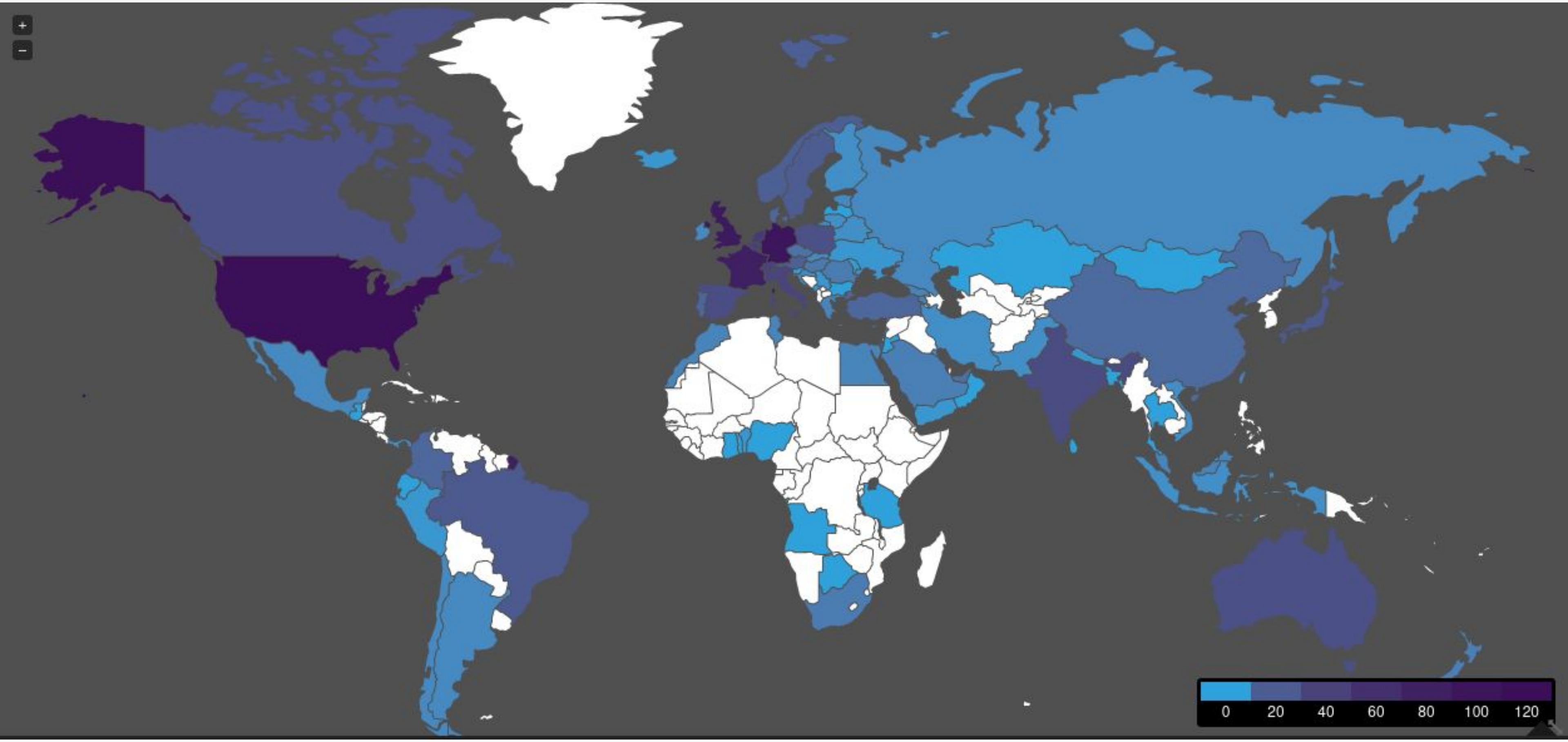
Date: 11/14/2017 to 11/21/2017

MISP 101 - Integraciones con otras herramientas

- Elastic
- Microsoft Sentinel
- CrowdStrike
- Wazuh
- Splunk
- OpenCTI
- Cuckoo Sandbox
- EclecticIQ
- IntelMQ
- ...

Más en: https://www.misp-project.org/tools/

MISP - MISPPriv Community



+1700 organizaciones, +4800 usuarios, +200K eventos, +74M indicadores

CIRCL - Otros servicios (gratuitos)

- Respuesta a Incidentes para el sector privado de Luxemburgo

Servicios Online:

- Passive DNS
- Passive SSL
- https://pandora.circl.lu
- https://lookyloo.circl.lu
- https://hashlookup.circl.lu

Más en:
https://www.circl.lu/services/
info@circl.lu
team@circl.lu
luciano.righetti@circl.lu

Recursos

- https://github.com/MISP/MISP
- https://www.circl.lu/
- https://www.misp-project.org/
- https://github.com/MISP/misp-training
- https://www.youtube.com/@CIRCLLuxembourg
- https://github.com/MISP/PyMISP
- https://github.com/MISP/misp-playbooks