



MISP - User Guide

A Threat Sharing Platform

A collaborative effort from the MISP community

Table of Contents

Introduction	1.1
Book Convention	1.2
Quick Start	1.3
Requirements	1.4
Get Your Instance	1.5
General Layout	1.6
General Concepts	1.7
User Management and Global Actions	1.8
Using the System	1.9
Delegation of Event	1.10
Extending Events	1.11
Administration	1.12
Managing Feeds	1.13
Updating Python dependencies	1.14
Automation and MISP API	1.15
PyMISP - Python Library to Access MISP	1.16
Create an Event Based on a Report	1.17
Taxonomies	1.18
Galaxies	1.19
MISP Objects	1.20
Sightings	1.21
Warning lists	1.22
Notice lists	1.23
Categories and Types	1.24
Synchronisation/Sharing	1.25
External Connectors	1.26
Modules	1.27
ZeroMQ - MISP publish-subscribe	1.28
Keyboard shortcuts	1.29
Translations - i18n & l10n	1.30
FAQ	1.31
Dev FAQ	1.32
Best Practices	1.33
User stories	1.34
User personas	1.35

Last modified: Tue Apr 13 2021 14:18:34 GMT+0200 (Central European Summer Time)

Introduction





User guide for MISP - The Open Source Threat Intelligence Sharing Platform. This user guide is intended for ICT professionals such as security analysts, security incident handlers, or malware reverse engineers who share threat intelligence using MISP or integrate MISP into other security monitoring tools. The user guide includes day-to-day usage of the MISP's graphical user interface along with its automated interfaces ([API](#)), in order to integrate MISP within a security environment and operate one or more MISP instances.

Acknowledgement

The MISP user guide is a collaborative effort between all the contributors to [MISP](#) including:

- Belgian Ministry of Defence (CERT)
- [CIRCL Computer Incident Response Center Luxembourg](#)
- Iklody IT Solutions
- [NATO NCIRC](#)
- Cthulhu Solutions
- [CERT-EU](#)

and many other contributors especially the ones during the [MISP hackathons](#).

Contributing

We welcome contributions to the MISP book. If you want to contribute, see our [contributing guide](#)

Format

MISP book is available in [HTML](#), [PDF](#), [ePub](#) and [Kindle mobi format](#).

License

The MISP user guide is dual-licensed under [GNU Affero General Public License version 3](#) and [CC-BY-SA 4.0 international](#).

- Copyright (C) 2012 Christophe Vandeplas
- Copyright (C) 2012 Belgian Defence
- Copyright (C) 2012 NATO / NCIRC
- Copyright (C) 2013-2020 Andras Iklody
- Copyright (C) 2015-2021 Alexandre Dulaunoy
- Copyright (C) 2014-2021 CIRCL - Computer Incident Response Center Luxembourg
- Copyright (C) 2018 Camille Schneider
- Copyright (C) 2018-2020 Steve Clement
- Copyright (C) 2021 Jeroen Pinoy

Last modified: Sun Feb 28 2021 09:22:59 GMT+0100 (Central European Standard Time)

description: Convention Used in MISP-Book

Convention Used in This Book

`code block or value`

- Used for variable, function or menu names in MISP.

Language

The language in this book is American English. All the screenshots and examples are in English.

CoC

The same code of conduct applies to this book as for the main MISP project. As a book can some times be considered the inadvertent soul of a piece of software, please take good care and consideration of our `Code of Conduct` . The CoC [can be read here](#).

Example install

The examples and screenshots provided in this book have been created with the MISP Autogenerated VM.

To get a copy of the latest VM [click here](#)

MISP Instance

In general when talking about a network of inter-connected MISP servers, each server is a [MISP instance](#). Whilst we have no strong feelings towards anyones naming schemes, as a rule of thumb try to have a scheme that makes everyday use easy when analysts need to talk about remote MISP instances.

The hostname used for the instance in this book is `misp.local` and we will henceforth refer to it either by name or as `local MISP instance` .

Example Organisations

As MISP is a platform to support information sharing, example organisations are often used within this book.

A set of users and organisations are used in the different examples.

The following two organisations are regularly used as example:

- Setec Astronomy with UUID `58d38339-7b24-4386-b4b4-4c0f950d210f`
- Acme Finance with UUID `58d38326-eda8-443a-9fa8-4e12950d210f`

Starting from MISP 2.4.71, the example organisations with the above mentioned UUID are **blocklisted** to avoid

large distribution of sample events while testing a [MISP instance](#). If you want to test your distribution, the

sample organisation blocklisting can be removed in `Administration / Manage Org blocklists`.

Example IOCs

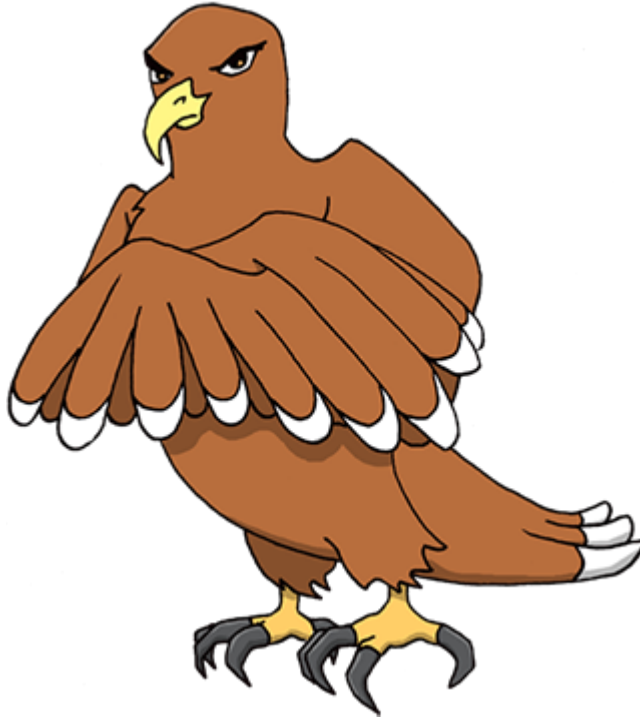
As with the example organisations, we want to make this book as useful as possible by using real life examples.

The following [IOC](#) examples have been used:

- [Sirefef](#) (aka ZeroAccess) Sample Event ID: #31337
- [WannaCry](#) Sample Event ID: #42
- [Dridex](#) Sample Event ID: #23

Last modified: Sun Feb 28 2021 09:22:59 GMT+0100 (Central European Standard Time)

Quick Start



MISP (Open Source Threat Intelligence and Sharing Platform) software facilitates the exchange and sharing of threat intelligence, [Indicators of Compromise \(IoCs\)](#) about targeted malware and attacks, financial fraud or any intelligence within your [community](#) of trusted members. MISP sharing is a distributed model containing technical and non-technical information which can be shared within closed, semi-private or open communities. Exchanging such information should result in faster detection of targeted attacks and improve the detection ratio, whilst also reducing the number of false positives.

With the focus on automation and standards, MISP provides you with a powerful ReST [API](#), extensibility (via misp-modules) or additional libraries such as PyMISP, jump ahead to these chapters to get started.

Login into MISP

MISP default credentials:

Username:	admin@admin.test
Password:	admin

I forgot my admin password :(

You can quickly reset it via the command line. You need to know the Admins E-Mail address. Replace www-data with whoever runs the webserver.

```
sudo -u www-data /var/www/MISP/app/Console/cake Password admin@admin.test Passv
```

Tasks to do after first Start

1. [Change site admin password](#)
2. [Activate Feeds](#)
3. [Setup your User](#) 3.1 Designate a [Site Admin](#) and an [Org Admin](#) 3.2 Add some contributing users and assign the corresponding [Roles](#)
4. [MISP Administration](#) 4.1 Edit your first organisations' name

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.

If you need a password generator use:

- Ubuntu / Debian: [pwgen](#)
- Website: [LastPass PW Generator](#)

- Built-in generator in Keepass* and other password manager
- Built-in generator in various web browsers

All Generator tools are only possibilities without any guarantee!

tl; dr

Create an Event

A. Add Event

1. Click **Add Event** in the left sidebar.

2. Populate Fields: Fill out the **Add Event** form. Fields include Date (e.g., 09-09), Distribution (e.g., This community only), Risk (e.g., Medium), and Info (e.g., Example Event).

3. Click **Add** at the bottom of the form.

4. Click **Add Attachment** in the left sidebar.

C. Add Event Attributes

5. Populate Fields: Fill out the **Add Attribute** form. Fields include Category (e.g., Network activity), Type (e.g., domain), and Value (e.g., example.org).

6. Click **Submit** at the bottom of the form.

B. Add Attachments

7. Click **Add Attachment** in the left sidebar.

8. Populate Fields: Fill out the **Add Attachment** form. Fields include Category (e.g., Payload delivery), Distribution (e.g., This community only), and a file upload (e.g., payload.txt).

9. Click **Upload** at the bottom of the form.

All IOC data entered is made up of an event object and described by its connected attributes.

The following attribute types should be added for each event:

- ip-src: source IP of attacker
- email-src: email used to send malware
- md5/sha1/sha256: checksum
- Hostname: full host/dnsname of attacker
- Domain: domain name used in malware

Browse Past Events

The screenshot illustrates the process of browsing past events in the Malware Information Sharing Platform (MISP). It includes a navigation menu, a table of events, and a detailed view of a selected event.

1. List Events

2. Filter

3. Click any row

4. See events with one or more matching attributes

Valid	Org	Id	#Attr	Date	Risk	Analysis	Info	Distribution	Actions
<input checked="" type="checkbox"/>	CyberSOC	106	1	2013-09-09	Medium	Initial	Example Event	This community only	Not published
<input checked="" type="checkbox"/>	CyberSOC	105	0	2013-09-04	Low	Ongoing	Example Event	This community only	Not published

Event

ID: 104
Uuid: 50fe6590-3ed4-4a09-8351-5492ac1d4fa4
Org: NCIRC
Date: 2013-01-22
Risk: Undefined
Analysis: Completed
Distribution: All communities, this will share the event with all MISP communities, allowing the event to be freely propagated from one server to the next.
Info: FAKEM RAT report from Trend Micro - Expanded iocs based on ISC passive DNS
Published: Yes

Related Events

2013-01-17 (103) 2012-11-27 (81)
2012-07-21 (45) 2012-07-16 (32)
2012-07-12 (25) 2012-07-12 (26)
2012-07-11 (31) 2012-07-02 (7)

Attributes

Category	Type	Value	Related Events	IDS	Distribution	Actions
Network activity	domain	zapto.org	81 25 7	No	All	<input checked="" type="checkbox"/>
	domain	bluematt.me		No	All	<input checked="" type="checkbox"/>

Export Events for logsearches



Create an Event

Home Event Actions Galaxies Input Filters Global Actions Sync Actions Administration

List Events
Add Events
Import from...
List Attributes
Search Attributes
View Proposals
Events with proposals
Export
Automation

The event created will be restricted to the organisations included in the distribution setting on the local instance only until it is published.

Add Event

Date: 2018-05-10 Distribution: This community only
Threat Level: High Analysis: Initial
Event Info: Quick Event Description or Tracking Info
Extends event: Event UUID or ID. Leave blank if not applicable.
GFI sandbox: Choose file No file chosen
Add

1. Add Events

2. Summarized description:

- Distribution
- Threat Level
- Event Info
- GFI sandbox (optional)
- Does it extend? (optional)

3. Add == Save

You only have to add a few pieces of information to register your Event. Further details will be specified after the Event has been added.

Describe Event

The event has been saved

View Event

View Correlation Graph

View Event History

Edit Event

Delete Event

Add Attribute

Add Object

Add Attachment

Populate from...

Enrich Event

Merge attributes from...

Publish Event

Publish (no email)

Publish event to ZMQ






Contact Reporter

Download as...

List Events

Add Event

OSINT - Threat Spotlight: Ratsnif - New Network Vermin from OceanLotus

Event ID	1
UUID	5d2417e3-4448-4d33-bbdd-2a1938a8ac86
Creator org	ORGNNAME
Owner org	ORGNNAME
Email	admin@admin.test
Tags	 
Date	2019-07-09
Threat Level	Undefined
Analysis	Initial
Distribution	This community only 
Info	OSINT - Threat Spotlight: Ratsnif - New Network Vermin from OceanLotus
Published	No
#Attributes	0 (0 Object)
First recorded change	1970-01-01 01:00:00
Last change	2019-07-09 06:28:19
Modification map	
Sightings	0 (0) - restricted to own organisation only 

⌵ Pivots

⌵ Galaxy

⌵ Event graph

⌵ Correlation graph

⌵ ATT&CK matrix

⌵ Attributes

⌵ Discussion

✕ 1 OSINT

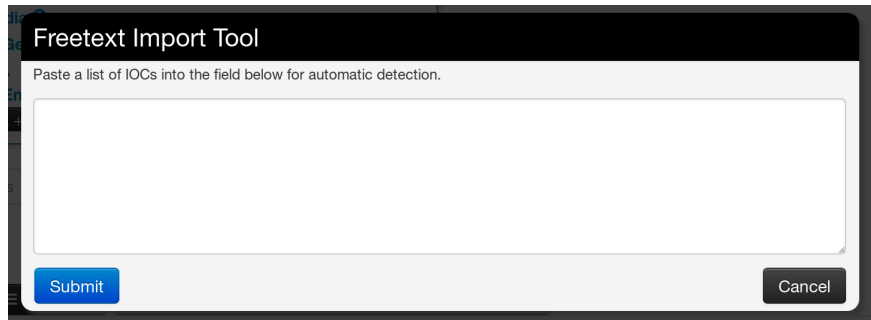
Now you can specify the information for your Event (you will need to scroll the window).

Free-Text Import Tool

The screenshot shows the 'Free-Text Import Tool' interface. At the top, a navigation bar includes tabs for 'Pivots', 'Galaxy', 'Event graph', 'Correlation graph', 'ATT&CK matrix', 'Attributes', and 'Discussion'. Below this, a blue button labeled '1: OSINT ...' is visible. A red text annotation points to the 'Galaxies' section, stating: 'All IoC data entered is made up of an event object and described by its connected attributes'. The 'Galaxies' section itself contains a blue header 'Galaxies' and two icons. Below this, there are navigation buttons: '« previous', 'next »', and 'view all'. A red arrow points to a menu icon in the top navigation bar, with a red text annotation: 'To get straight to the Freetext import tool click here'. Below the navigation bar, there is a row of tabs: 'Date', 'Org', 'Category', 'Type', 'Value', 'Tags', 'Galaxies', 'Comment', 'Correlate', and 'Related Events'. A red text warning is displayed below the tabs: 'Attribute warning: This event doesn't contain any attribute. It's strongly advised to populate the event with attributes (indicators, observables or ...)'. At the bottom, there are more navigation buttons: '« previous', 'next »', and 'view all'.

The following will pop-up.

If you have a list of [indicators](#) from which you would like to quickly generate attributes then the **Free-text import tool** is just what you need. Simply paste your list of [indicators](#) (separated by line-breaks) into this tool.



The screenshot shows a window titled "Freetext Import Tool". Inside the window, there is a text area with the instruction "Paste a list of IOCs into the field below for automatic detection." Below the text area are two buttons: "Submit" on the left and "Cancel" on the right.

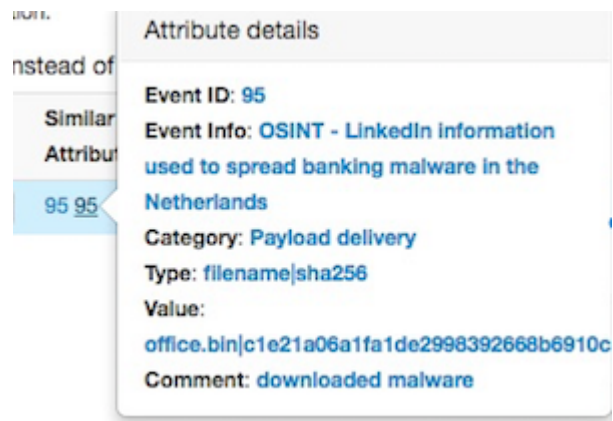
Freertext Import Results

Below you can see the attributes that are to be created. Make sure that the categories and the types are correct, often several options will be offered based on an inconclusive automatic resolution.

☐ Proposals instead of attributes

Value	Similar Attributes	Category	Type	IDS <input type="checkbox"/>	Comment	Actions
c1e21a06a1f8	95 95	Payload delivery	sha256	<input checked="" type="checkbox"/>	Imported via the Freertext Import	
Submit		<div>sha256 → authentichash</div>		Change all		
		<div>Update all comment fields</div>		Change all		

The tool will help you to find similarities between your import and other issues already registered in MISP.



For example, you can see the ID of all related Events and view their information.

Alternative to import

An alternative route to reach the Freetext import tool is shown below.

The event has been saved

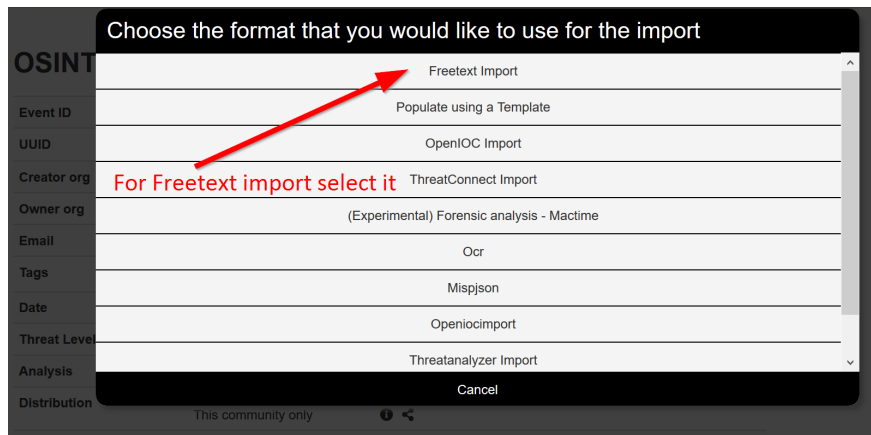
[View Event](#)
[View Correlation Graph](#)
[View Event History](#)

[Edit Event](#)
[Delete Event](#)
[Add Attribute](#)
[Add Object](#)
[Add Attachment](#)
[Populate from...](#)
[Enrich Event](#)
[Merge attributes from...](#)

OSINT - Threat Spotlight: Ratsnif - New Network Vermin...

Event ID	1
UUID	5d2417e3-f448-4d33-bbdd-2a1938a6ac88
Creator org	ORGNAME
Owner org	ORGNAME
Email	admin@admin.test
Tags	
Date	2019-07-09
Threat Level	Undefined
Analysis	Initial

To add attributes select "Populate from..."






Tags and Taglist

Using existing Data

Another easy way to add information is to use Tags. You can see the result of adding existing Tags (circl:incident-classification=XSS and circl:incident-classification="information-leak").

OSINT - Threat Spotlight: Ratsnif - New Network Vermin...

Event ID	1
UUID	5d2417e3-f448-4d33-bbdd-2a1938a6ac88 
Creator org	ORGNAME
Owner org	ORGNAME
Email	admin@
Tags	 
Date	2019-07
Threat Level	Undefined
Analysis	Initial


Add a tag

[Tag Collections](#) [Custom Tags](#) [All Tags](#)

To add tags from a Taxonomy or Custom tags, click here

By clicking the button, you can add more tags from an existing Taglist.

OSINT - Threat Spotlight: Ratsnif - New Network Vermin...

Event ID	1	!! If no tags show up, enable a Taxonomy or create some custom tags
UUID	5d2417e3-f448-4d33-bbdd-2a1938a6ac88	+
Creator org	ORGNAME	Select Tag collections (taxonomies) or self-
Owner org	ORGNAME	created tags
Email	admin@	
Tags		
Date	2019-07	
Threat Level	Undefined	
Analysis	Initial	

Add a tag

Tag Collections

Custom Tags

All Tags

L

malware







Submit

Select the input box to see the tags

In particular the "Taxonomy Library: circl" Taglist is very complete.

Once you added the tag(s) it will show in you main event window and in the list event view.

OSINT - Threat Spotlight: Ratsnif - New Network Vermin...






Event ID	1
UUID	5d2417e3-f448-4d33-bbdd-2a1938a6ac88 
Creator org	ORGNAME
Owner org	ORGNAME
Email	admin@admin.test
Tags	 malware    
Date	2019-07-09
Threat Level	Undefined
Analysis	Initial

Once you have confirmed the tag(s)
they will appear here

Local tags

Local tags can be added in a similar fashion.

OSINT - Threat Spotlight: Ratsnif - New Network Vermin...

Event ID	1
UUID	5d2417e3-f448-4d33-bbdd-2a1938a6ac88 
Creator org	ORGNAME
Owner org	ORGNAME
Email	admin@admin
Tags	   
Date	2019-07-09
Threat Level	Undefined
Analysis	Initial

Add a local tag

[Tag Collections](#) [Custom Tags](#) [All Tags](#)

To add local tags, click here

They will be identified by a corresponding icon.

Tags

type:OSINT x

osint:lifetime="perpetual" x

circl:osint-feed x

ttp:white x

osint:source-type="blog-post" x

osint:certainty="93" x

estimative-language:confidence-in-analytic-judgment="high" x

workflow:todo="review-for-privacy" x


+ +

Date	2019-07-04
Threat Level	Low
Analysis	Ongoing
Distribution	All communities <div><div></div><div>i</div><div></div></div>

No tags in list

In case you get the below. You need to either enable an existing Taxonomy or add some custom tags.

OSINT - Threat Spotlight: Ratsnif - New Network Vermin...

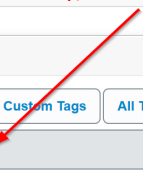
Event ID	1
UUID	5d2417e3-f448-4d33-bbdd-2a1938a6ac88
Creator org	ORNAME
Owner org	ORNAME
Email	admin@
Tags	
Date	2019-07
Threat Level	Undefined
Analysis	Initial

Red text annotation: **!! If no tags show up, enable a Taxonomy or create some custom tags**

Add a tag

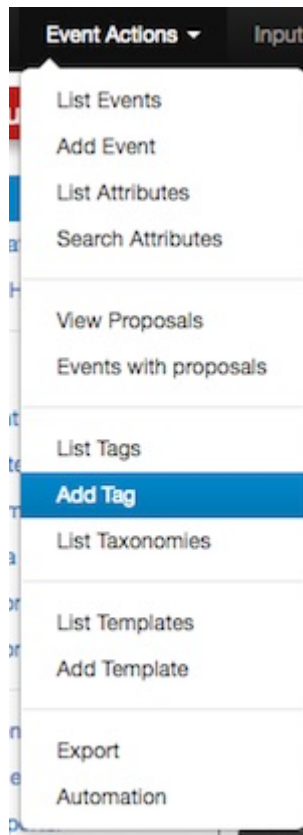
Tag Collections Custom Tags All Tags

Nothing to pick



Make your own Taglist

If you want make your own Taglist, select Add Tag.



You will see the following window:

The screenshot shows a web application interface. At the top is a dark navigation bar with links: Home, Event Actions, Input Filters, Global Actions, Sync Actions, Administration, Audit, and Discussions. On the left is a sidebar with links: List Favourite Tags, List Tags, and Add Tag (which is highlighted in blue). The main content area is titled 'Add Tag' and contains three input fields: 'Name' with the value 'Popom', 'Colour' with the value '#1bb5f7', and 'Restrict tagging to' with a dropdown menu showing 'Unrestricted'. Below these fields is a checked checkbox labeled 'Exportable' and a blue 'Add' button.

Name	Colour	Restrict tagging to
Popom	#1bb5f7	Unrestricted

☒ Exportable

Add

Then, when you add the new tag it will appear in the Custom Taglist.

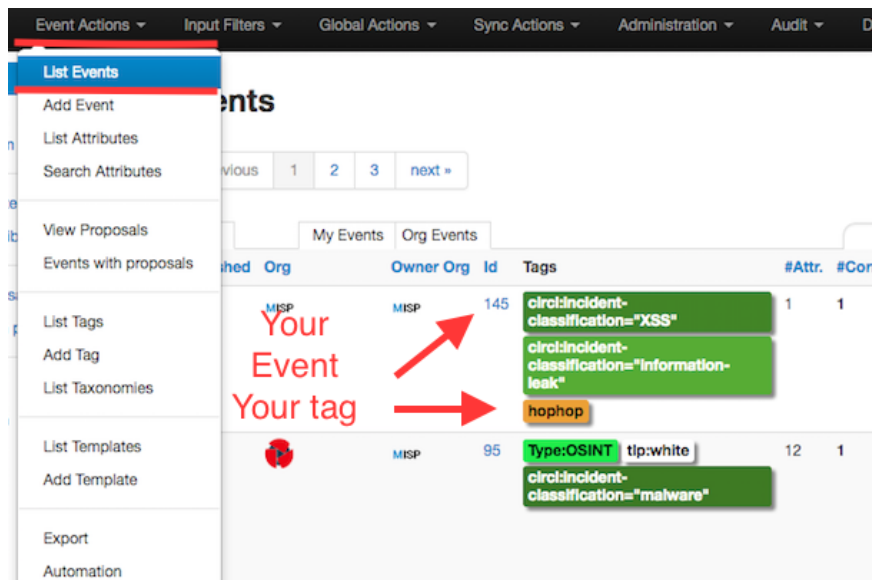
Suggestions

The following attribute types should be added for each Event:

- ip-src: source IP of attacker
- email-src: email used to send malware
- md5/sha1/sha256: checksum
- Hostname: full host/dnsname of attacker
- Domain: domain name used in malware

Browsing Events

To see your Event, select List Events from the menu Events Action. You can click any row and select a filter.



If you click on your Event's number, you can see all the information related to your Event.

OSINT - Threat Spotlight: Ratsnif - New Network Vermin...

ORGNAME

Event ID	1
UUID	5d2417e3-4448-4d33-bbdd-2a1938a6ac88
Creator org	ORGNAME
Owner org	ORGNAME
Email	admin@admin.test
Tags	
Date	2019-07-09
Threat Level	Undefined
Analysis	Initial

Related Events

OR...

Unidentified Malware via SpamMailServer3

2019-07-09

1

This is the Organizations name

Number of matching attributes

Related events, events that share attributes, will be displayed here

Export Events for Log Search

Export functionality is designed to automatically generate signatures for intrusion detection systems. To enable signature generation for a given attribute, the Signature field of this attribute must be set to Yes. Note that not all attribute types are applicable for signature generation, currently we only support [NIDS](#) signature generation for IP, domains, host names, user agents etc., and hash list generation for MD5/SHA1 values of file artifacts. Support for more attribute types is planned.

The screenshot shows the MISP (Malware Incident Response System) interface. The top navigation bar includes links for Home, Event Actions, Input Filters, Global Actions, Sync Actions, and Admin. The left sidebar contains a menu with the following items: List Events (highlighted), Add Event, Import From MISP Export, List Attributes, Search Attributes, View Proposals, Events with proposals, Export (indicated by a red arrow and the text 'Click to go'), and Automation. The main content area is titled 'Events' and features a pagination control (1, 2, 3) and a search bar. Below the search bar are tabs for 'My Events' and 'Org Events'. A table of events is displayed with columns: Published, Org, Owner Org, Id, and Tags. The first event has Id 145 and is published. The second event has Id 95 and is highlighted in blue. The tags for the first event include 'circl:incident-classification="X"', 'circl:incident-classification="In leak"', and 'hophop'. The tags for the second event include 'Type:OSINT' and 'tip:'.

Published	Org	Owner Org	Id	Tags
✓	MISP	MISP	145	circl:incident-classification="X", circl:incident-classification="In leak", hophop
✓	MISP	MISP	95	Type:OSINT, tip:

Simply click on any of the following buttons to download the appropriate data for log correlation.

List Events

Add Event

Import From MISP Export

List Attributes

Search Attributes

View Proposals

Events with proposals

Export

Automation

Export

Export functionality is designed to automatically generate signatures for intrusion detection systems. To enable signature generation for a given attribute, Signature field of this attribut must be set to Yes. Note that not all attribute types are applicable for signature generation, currently we only support NIDS signature generation for IP, domains, host names, user agents etc., and hash list generation for MD5/SHA1 values of file artifacts. Support for more attribute types is planned.

Simply click on any of the following buttons to download the appropriate data.

Type	Last Update	Description	Outdated	Progress	Actions
XML	N/A	Click this to download all events and attributes that you have access to (except file attachments) in a custom XML format.	Yes	N/A	Download Generate
CSV_Sig	N/A	Click this to download all attributes that are indicators and that you have access to (except file attachments) in CSV format.	Yes	N/A	Download Generate
CSV_All	N/A	Click this to download all attributes that you have access to (except file attachments) in CSV	Yes	N/A	Download Generate

Enable a Taxonomy

Enable and fetch a feeds

Last modified: Sun Feb 28 2021 09:22:59 GMT+0100 (Central European Standard Time)

MISP Instance requirements

- [Intro](#)
- [The biggie](#)
 - [Tool assisted sizing](#)

Intro

There are various ways you can run a [MISP instance](#).

- Virtualized with docker/ansible/packer etc
- VMware/Virtualbox/Xen etc
- Dedicated hardware
- Road warrior setups
- Air-gapped setups

Whilst there is never an ultimate answer to what specifications a system needs, we try to give an approximate answer depending on your use case.

The biggie

Having millions of events with millions of attributes ([indicators](#)) will eventually result in sub-par performance. Ideally you have millions of attributes and thousands of events. But this also depends on how you ingest the data. With millions of attributes a bottleneck could be the correlation engine. Especially if you have many duplicates in your events. (Use the feed matrix to see if feeds are massively overlapping)

Tool assisted sizing

During a hackathon [misp-sizer](#) was conceived. ([code](#)) This can give you a very rough estimate and needs some more [improvements](#).

Last modified: Sun Feb 28 2021 09:22:59 GMT+0100 (Central European Standard Time)

Get your own MISP instance

The intention of this chapter is to support you in getting your own [MISP instance](#) up and running.

MISP Virtual Machine

CIRCL maintains the image of a recent MISP virtual machine online. This VM is generated after every commit to the main MISP repository on Github.

This is a very easy out of the box solution, optimized for product evaluation and to support trainings held by CIRCL staff.

MISP VM Download

The best place to get the latest version of the MISP virtual machine, as well as all the available training materials is the [MISP training materials page](#) on the CIRCL website.

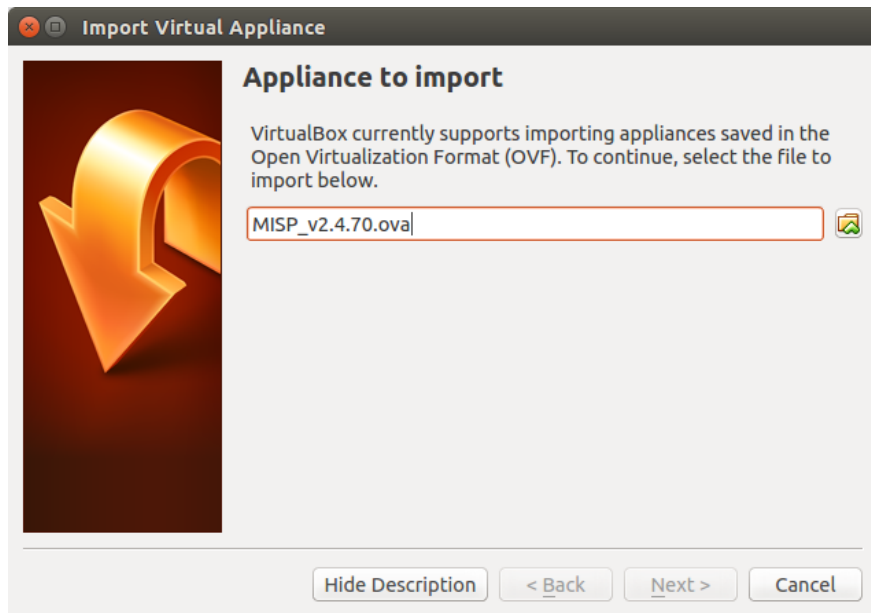
If you do not remember the direct link to the MISP training materials here are the very easy to remember steps you have to follow to reach the right place:

1. Access the [CIRCL homepage](#)
2. Navigate to the [Training area](#)
3. Click [MISP Malware Information Sharing Platform - Threat Sharing](#)
4. Follow the link to the [Training materials freely available](#)

Download the image of the virtual machine and validate the SHA512 fingerprint.

Import Appliance

In VirtualBox use the "Import Appliance..." functionality to import the virtual machine.



The instructions in this manual covers VirtualBox only. If you prefer another virtualization solution like VMWare you can find some quick instruction on the [MISP training materials page](#).

ESXi Servers have been tested too. Should work without problem but some manual changing of the ATA-Bus is needed.

MISP VM Credentials

The MISP image is pre-configured to be reachable on the private IP address **localhost** by SSH on port 2222. The GUI is reachable by <http://localhost:8080/>.

You should have two interfaces on your VirtualBox configuration (NAT and host-only). You can also configure access to the [MISP instance](#) by doing port forwarding on the NAT interface.

Depending on your setup (for example accessing the VM from another host), you might want to change the base URL in MISP server settings. This can be done from the command line:

```
sudo -u www-data /var/www/MISP/app/Console/cake Baseurl [baseurl]
```

You can confirm the baseurl is updated correctly by checking the config.php file:

```
grep baseurl /var/www/MISP/app/Config/config.php
```

You can set the external_baseurl via the GUI or via the command below later. Changing it is never required to access the GUI.

```
sudo -u www-data /var/www/MISP/app/Console/cake Admin setSetting external_baseurl
```

MISP credentials:

- **GUI Admin:** admin@admin.test:admin (it's the [site admin](#) account with full rights, feel free to create other users)
- **Shell/SSH:** misp : Password1234
- **MySQL:** The credentials are generated during the VM generator. The details are located in ~misp/mysql.txt

Networking on the VM

Virtualbox has a neat feature to forward ports from your Host machine to the Guest VM. We forward the following ports:

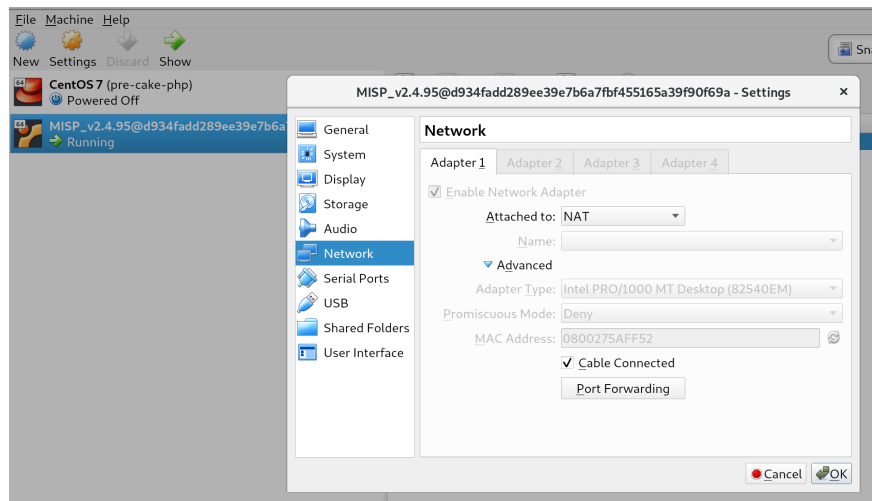
- **ssh** Forward from 2222 on Host -> 22 on guest
- **http** Main WebUI - 8080 on Host -> 80 on guest
- **https** Not in use - 8443 on Host -> 443 on guest
- **8001** MISP Dashboard - 8001 on Host -> 8001 on guest
- **8888** Viper Web UI - 8888 on Host -> 8888 on guest

- **1666** misp-modules used to poll the misp-modules [API](#) - 1666 on Host -> 6666 on guest

If the port is already used on your host, virtualbox will still boot and all the other ports will work.

To change the port forwarding select the running VM in the UI and click on

Settings -> Network -> Advanced -> Port forwarding



Overview of default port forwards

Port Forwarding Rules
✕

Name	Protocol	Host IP	Host Port	Guest IP	Guest Port
dashboard	TCP		8001	0.0.0.0	8001
http	TCP		8080		80
https	TCP		8443		443
misp-modules	TCP		1666	0.0.0.0	6666
ssh	TCP		2222	0.0.0.0	22
viper	TCP		8888	0.0.0.0	8888

Cancel
OK

The reason that some entries have `0.0.0.0` and other are left blank is due to a virtualbox bug where traffic would not be sent to the Guest VM.



VMWare users will need to connect to whatever IP the VM has on your host.
There is NO port forwarding done for VMWare.

Potential issues

You might have a very old VM installed and the ports are not be forwarded. Either configure the port forwards manually or download a new VM.

Last modified: Tue Mar 02 2021 14:01:38 GMT+0100 (Central European Standard Time)

General Layout

The top bar

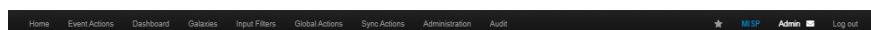
This menu contains all of the main functions of the site as a series of dropdown menus. These menus contain all (from the current user's perspective) accessible functions sorted into several groups.

Simple User



- **Home button:** This button will return you to the start screen of the application, which is the event index page or the page the user set as custom home page using the star in the top bar.
- **Event Actions:** All the malware data entered into MISP is made up of an event object that is described by its connected attributes. The Event actions menu gives access to all the functionality that relates to the creation, modification, deletion, [publishing](#), searching and listing of events and attributes.
- **Dashboard:** Allows you to create a custom dashboard using widgets.
- **Galaxies:** Shortcut to the list of [MISP Galaxies](#) on the [MISP instance](#).
- **Input Filters:** Input filters alter what and how data can be entered into this instance. Apart from the basic validation of attribute entry by type, it is possible for the site administrators to define regular expression replacements and blocklists for certain values in addition to blocking certain values from being exportable. Users can view these replacement and blocklist rules here while an administrator can alter them.
- **Global Actions:** This menu gives you access to information about MISP and this instance. You can view and edit your own profile, view the manual, read the news or the terms of use again, see a list of the active organisations on this instance and a histogram of their contributions by attribute type.
- **MISP:** Simple link to your BASEURL
- **Name:** Name (Auto generated from Mail address) of current logged in user
- **Envelope:** Link to User Dashboard where you can consult some of your notifications and changes since last visit. Like some of the [proposals](#) received for your organisation.
- **Log out:** The Log out button to end your session immediately.

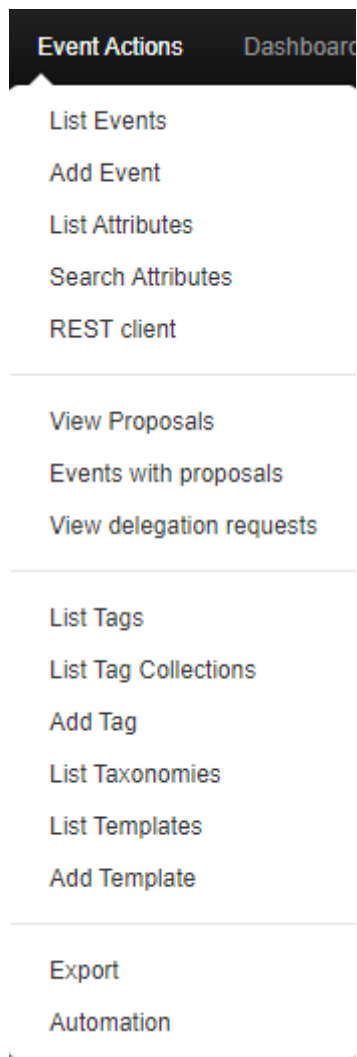
Admin User



- **Home button:** See description given earlier for user.
- **Event Actions:** See description given earlier for user.
- **Dashboard:** See description given earlier for user.
- **Galaxies:** You can additionally update the Galaxies.
- **Input Filters:** See description given earlier for user.
- **Global Actions:** See description given earlier for user.
- **Sync Actions:** With administrator access rights, shows a list of the connected instances and allows the initiation of a [push](#) and a [pull](#). See [sharing and synchronisation](#).
- **Administration:** Administrators can add, edit or remove user accounts and user [roles](#). [Roles](#) define the access rights to certain features such as [publishing](#) of events, usage of the REST interface or synchronization of any user belonging to the given role. Site administrators can also access a contact form, through which it is possible to reset the passwords of users, or to just get in touch with them via encrypted e-mails.
- **Audit:** If you have audit permissions, you can view the logs for your organisation (or for site admins for the entire system) here or even search the logs if you are interested in something specific.
- **MISP:** See description given earlier for user.
- **Admin:** User role.
- **Envelope:** See description given earlier for user.
- **Log out:** See description given earlier for user.

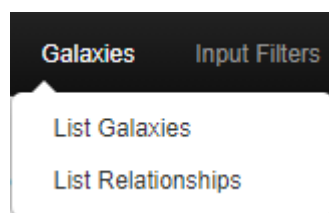
Content of each of the top menu bar drop-down menus

Event actions



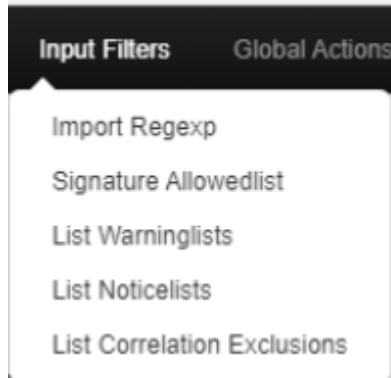
- **List Events:** Lists all the events in the system that are not private or belong to your organisation. You can add, modify, delete, publish or view individual events from this view.
- **Add Event:** Allows you to fill out an event creation form and create the event object, which you can start adding attributes.
- **List Attributes:** Lists all the attributes in the system that are not private or belong to your organisation. You can modify, delete or view each individual attribute from this view.
- **Search Attributes:** You can set search terms for a filtered attribute index view [here](#).
- **REST client** MISP Online REST client where you can make calls directly to the [API](#) via a Web UI.
- **View Proposals:** Shows a list of all [proposals](#) that you are eligible to see.
- **Events with proposals:** Shows all of the events created by your organisation that has pending [proposals](#).
- **List Tags:** List all the tags that have been created by users with tag creation rights on this instance.
- **List Tag Collections:** List all the tag collections that have been created by users with tag creation rights on this instance. Tag collections allow you to assign a collection of tags to an event or attribute in one action.
- **Add Tag:** Create a new tag.
- **List Taxonomies:** List all of the taxonomies installed on the [MISP instance](#). This is also the place to activate the taxonomies as a [Org Admin/Site Admin](#).
- **List Templates:** List all of the event templates created by users with template creation rights on this instance.
- **Add Template:** Create a new template.
- **Export:** Export the data accessible to you in various formats.
- **Automation:** If you have authentication key access, you can view how to use your key to use the REST interface for automation [here](#).

Galaxies



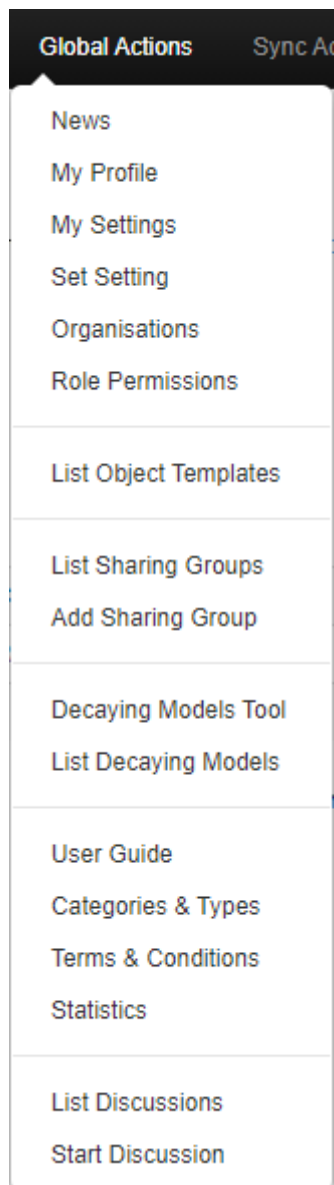
- **List Galaxies:** Index of [MISP Galaxies](#) on the [MISP instance](#).
- **List Relationships:** Shows a list of galaxy cluster relationships.

Input filters



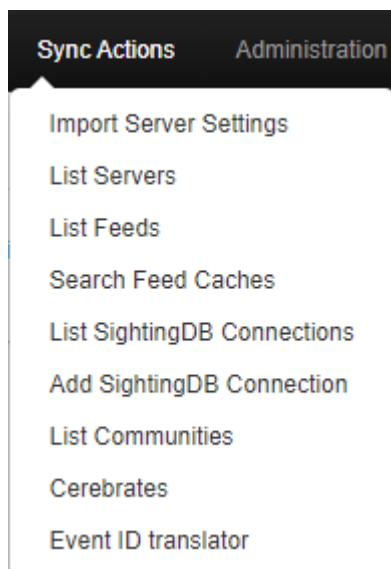
- **Import Regexp:** You can view the Regular Expression rules, which modify the data that can be entered into the system. This can and should be used to help filter out personal information from automatic imports (such as removing the username from windows file paths), having unified representation for certain common values for easier correlation or simply standardizing certain input. It is also possible to block certain values from being inserted. As a site administrator or a user with regex permission, you can also edit these rules.
- **Signature Allowlist:** You can view the allowlist rules, which contains the values that are blocked from being used for exports and automation on this instance. Site administrators have access to editing this list.
- **List Warninglists:** [MISP warninglists](#) are lists of well-known [indicators](#) that can be associated to potential false positives, errors or mistakes. The warning lists are integrated in MISP to display an info/warning box at the event and attribute level.
- **List Noticelists:** MISP noticelists inform MISP users of the legal, privacy, policy or even technical implications of using specific attributes, categories or objects.
- **List Correlation Exclusions:** Allows for the exclusion of certain values from the correlation engine.

Global Actions



- **News:** Read about the latest news regarding the MISP system
- **My Profile:** Manage your user account.
- **My Settings:** View your user specific settings.
- **Set Setting:** Set user specific settings.
- **Organisations:** View the organisations having a presence on this instance.
- **Role Permissions:** You can view the role permissions here.
- **List Sharing Groups:** You can view the list of existing [Sharing Groups](#) to which you or your organisation have access.
- **Add Sharing Group:** Create a sharing group.
- **Decaying Models Tool:** Allows you to create decaying models.
- **List Decaying Models:** Manage existing decaying models.
- **User Guide:** A link to this user guide.
- **Categories & Types:** Quick overview of Attribute Categories and Types. e.g: md5 -> Payload delivery, Artifacts dropped, Payload installation, External analysis
- **Terms & Conditions:** General terms and conditions which can be configured in Administration -> Server Settings -> MISP Settings: MISP.terms_file . From the UI: "The filename of the terms and conditions file. Make sure that the file is located in your MISP/app/files/terms directory"
- **Statistics:** View a series of statistics about the users and the data on this instance.
- **List Discussions:** List threads of discussions created on the [MISP instance](#) by the organisations connected to this local [community](#).
- **Start Discussion:** Create a new discussion thread.

Sync Actions



- **Import Server Settings:** Import sync server configuration.
- **List Servers:** Connect your [MISP instance](#) to other instances, or view and modify the currently established connections.
- **List Feeds:** Follow the RSS feeds of other organisation or CERTs worldwide.
- **Search Feed Caches:** Search for values potentially contained in the cached feeds and servers.
- **List SightingDB Connections:** Allows you to manage existing SightingDB connections. SightingDB is an alternate sighting database that MISP interconnects with.
- **Add SightingDB Connection:** Create a SightingDB connection.
- **List Communities:** A list of communities that chose to advertise their existence to the general MISP user-base.
- **Cerebrates:** Connect your MISP to one or several Cerebrate instances to act as lookup directories for organisation and sharing group information.
- **Event ID translator:** Allows to translate a local ID into the corresponding event ID on sync servers configured.

Administration

Administration	Audit
List Users	
List Auth Keys	
List User Settings	
Set User Setting	
Add User	
Contact Users	
User Registrations	
List Organisations	
Add Organisations	
List Roles	
Add Roles	
Server Settings & Maintenance	
Jobs	
Scheduled Tasks	
Event Block Rules	
Blocklist Event	
Manage Event Blocklists	
Blocklist Organisation	
Manage Org Blocklists	

- **List Users:** View, modify or delete the currently registered users.
- **List Auth Keys:** Shows a list of the auth keys on this instance (auth keys from the advanced auth key system) with their comments.
- **List User Setting:** Lists user setting for the users on this instance.
- **Set User Setting:** Set user specific settings for the users on this instance.
- **Add User:** Create an account for a new user for your organisation. Site administrators can create users for any organisation.
- **Contact Users:** You can use this view to send messages to your current or future users or send them a temporary password.

When adding a new user to the system, or when you want to manually reset the password for a user, just use the "Send credentials automatically" setting.

After selecting the action, choose who the target of the e-mails should be (all users, a single user or a user not yet in the system).

You can then specify (if eligible) what the e-mail address of the target is (for existing users you can choose from a dropdown menu).

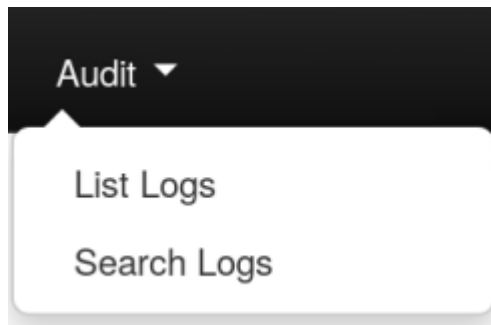
In the case of a new user, you can specify the future user's GnuPG key, to send his/her new key in an encrypted e-mail.

The system will automatically generate a message for you, but it is also possible to write a custom message if you tick the check-box, don't worry about assigning a temporary password manually. The system will do that for you, it will be in the mail after your custom message.

- **User Registrations:** You can find messages sent to this instance in this view.
- **List Organisations:** View the organisations having a presence on this instance, with some useful information.
- **Add Organisations:**
- **List Roles:** List, modify or delete currently existing [roles](#).
- **Add Role:** Create a new role group for the users of this instance, controlling their privileges to create, modify, delete and to publish events and to access certain features such as the logs or automation.
- **Server Settings & Maintenance:** Various tools, upgrade scripts that can help a site-admin run the instance & Set up and diagnose your MISP installation.
- **Jobs:** View the background jobs and their progress
- **Scheduled Tasks:** Schedule the pre-defined tasks for your instance (this currently includes export caching, server [pull](#) and server [push](#)).
- **Event Block Rules:** Set event block rules. Event block rules allow you to add a simple tag filter to block events from being added or synced. See [administration](#).
- **Blocklist Event:** Link to form where you can quickly add an event to a blocklist with it's UUID. For more information, see [administration](#).
- **Manage Event Blocklists:** List of blocklisted events on [MISP instance](#).
- **blocklist Organisation:** Link to for where you can quickly add an organisation to a blocklist with it's UUID. For more information, see [administration](#).

- **Manage Org blocklists:** List of blocklisted Organisations on this instance.

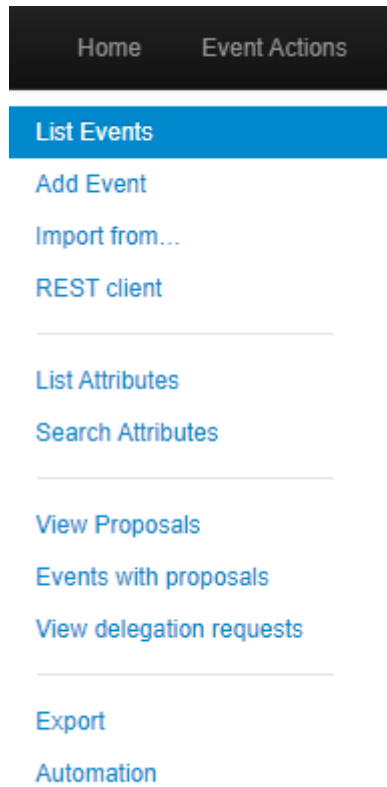
Audit



- **List Logs:** View the logs of the instance.
- **Search Logs:** Search the logs by various attributes.

The left bar

The menu items in this menu bar are different depending on the current page you are on. The blue highlight shows you what page you are on.



Last modified: Sun Feb 28 2021 09:22:59 GMT+0100 (Central European Standard Time)

- [General Concepts](#)
 - [Admins and Site Admins](#)
 - [Background Jobs](#)
 - [MISP Instance](#)
 - [Organisation administrators and Site administrators](#)
 - [Pivot path](#)
 - [Pivoting](#)
 - [Proposals](#)
 - [Publishing](#)
 - [Pull](#)
 - [Push](#)
 - [Scheduled Tasks](#)
 - [Sync User](#)
 - [Synchronisation](#)
 - [Tagging](#)
 - [Templating](#)

General Concepts

Admins and Site Admins

There are two types of admins in MISP: Admins (also referred to as org admins) and Site Admins. Whilst the former can only do some limited administration of users of his/her own organisation, site admins have access to all of the features and data of the system. They are in charge of making sure that the system runs correctly and the maintenance of MISP.

Background Jobs

A lot of the heavier tasks are a burden to users, in that their actions can cause long delays (and in some cases timeouts) while the application logic is executing. To alleviate this, long processes have been (if enabled) moved to background jobs, meaning that their execution happens asynchronously in the background, allowing the user to freely interact with the platform whilst the request is being processed.

MISP Instance

A [MISP instance](#) is an installation of the MISP software and the connected database. All the data visible to the users is stored locally in the database and data that is shareable (based on the distribution settings) can be synchronised with other instances via the Sync actions. The instance that you are reading this manual on will be referred to as "this instance" or "your instance". The instances that your instance synchronises with will be referred to as "remote instances".

Organisation administrators and Site administrators

We have two types of administrators, site and organisation admins. The former has access to every administrator feature for all the data located on the system including global features such as the creation and modification of user [roles](#) and instance links, whilst organisation admins can administer users, events and logs of their own respective organisations.

Pivot path

The (branching) path taken by a user from event to event while following correlation links. This is represented by the branching graph in the event view.

Pivoting

The act of navigating from event to event through correlation links.

Proposals

Each event can only be directly edited by users of the original creator organisation (and site admins). However, if another organisation would like to amend an event with extra information on an event, or if they'd like to correct a mistake in an attribute, they can create a Proposal. These [proposals](#) could then be accepted by the original creator organisation. These [proposals](#) can be pulled to another server, allowing users on connected instances to propose changes which then could be accepted by the original creators on another instance (and subsequently pushed back).

Publishing

When an event is first created by a user, it is visible to everyone on the instance based on the access rights ("Your organisation only" events will not be visible to users of other organisations), but they will not be synchronised and they won't be exportable. For this, a user with [publishing](#) permission of the organisation that created the event has to publish the event. The system will then inform all the users of the instance that are subscribing to e-mail notifications and who have access to view the published event via an e-mail.

Pull

Pulling is the process of using the configured [sync user](#) on a remote instance to REST GET all of the accessible data (based on the distribution rights) to your instance and store it.

Push

Pushing is the process of using a configured instance link to send an event or all accessible events (limited by the distribution rights) through the REST interface to a remote instance.

Scheduled Tasks

Certain common tasks can be scheduled for a later execution or for regular recurring executions. These tasks currently include caching all of the export formats, pulling from all eligible instances and pushing to all eligible instances.

Sync User

A user of a role that grants sync permissions, these users (and their authentication keys) are used to serve as the points of connection between instances. Events pushed to an instance are pushed to a [sync user](#), who then creates the events on the remote instance. Events pulled are added by the [sync user](#) that is used to connect the remote instance to your instance. As an administrator, keep in mind that a [sync user](#) needs auth key and publish permissions, has to have undergone the mandatory password change and has to have accepted the Terms of Use in order for the sync to work. Please make sure that all of these steps are taken before attempting to [push](#) or [pull](#).

Synchronisation

What we call [synchronisation](#) is an exchange of data between two (or more) MISP instances through our [pull](#) and [push](#) mechanisms.

Tagging

Users with [tagging](#) rights can assign various dynamically created tags to events, allowing an arbitrary link between events to be created. It is possible to filter events based on these tags and they can also be used to filter events for the automation.

Templating

Users with [templating](#) rights can create easy to fill forms that help with the event creation process.

Last modified: Sun Feb 28 2021 09:22:59 GMT+0100 (Central European Standard Time)

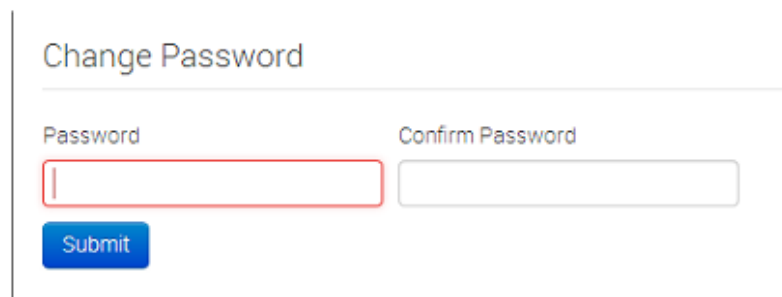
- [User Management and Global Actions](#)
 - [First run of the system](#)

User Management and Global Actions

First run of the system

When first logging into MISP with the username and password provided by your administrator, there are a number of things that need to be done, before you can start using the system.

- **Accepting the Terms of use:** The terms of use are shown immediately after logging in for the first time, make sure to read through this page before clicking "Accept Terms" at the bottom of the page.
- **Changing the password:** After accepting the ToU, you'll be prompted to change your password, but keep in mind that it has to be pass to the [MISP password policy](#). Enter the same password into the confirm password field, before clicking submit to finalise the change.

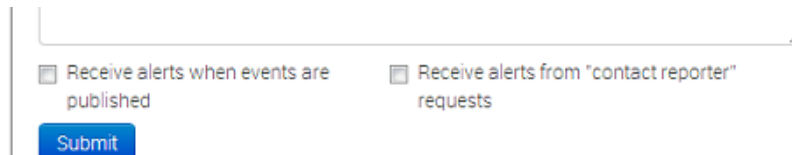


Change Password

Password Confirm Password

Submit

- **Setting up the GnuPG Key:** In order for the system to be able to encrypt the messages that you send through it, it needs to know your GnuPG key. Navigate to the Edit profile view (My Profile on the left -> Edit profile in the top right corner). Paste the key into the GnuPG Key field and click submit.
- **Subscribing to Auto-alerts:** Turning auto-alerts on will allow the system to send you e-mail notifications about any new public events entered into the system by other users and private events added by members of your organisation. To turn this on, navigate to the Edit profile view (My profile on the left navigation menu -> Edit profile in the top right corner). Tick the auto-alert checkbox and click submit to enable this feature.



The screenshot shows a portion of a web form. At the top is a large, empty text input field. Below it are two checkboxes, each with a label: ☐ Receive alerts when events are published and ☐ Receive alerts from "contact reporter" requests. Below these checkboxes is a blue button with the text "Submit".

- **Subscribing to e-mails sent via the "Contact Reporter" functionality:**
This feature is turned on right below the autoalerts and will allow you to receive e-mails addressed to your organisation whenever a user tries to ask about an event that was posted by a user of your organisation. Keep in mind that you can still be addressed by such a request even when this setting is turned off, if someone tries to contact you as the event creator directly or your organisation for an event that you personally have created then you will be notified.
- **Reviewing the Terms & Conditions:** To review the Terms & Conditions or to read the User Guide, use the appropriate button on the left navigation menu.
- **Making sure that compatibility mode is turned off (IE9&IE10):**
Compatibility mode can cause some elements to appear differently than intended or not appear at all. Make sure you have this option turned off.

Last modified: Thu Mar 04 2021 14:48:45 GMT+0100 (Central European Standard Time)

- [Using the system](#)
 - [Creating an event](#)
 - [Add attributes to the event](#)
 - [Add Attribute](#)
 - [Add Object](#)
 - [Create and manage Sharing Groups](#)
 - [Populate from Template](#)
 - [Freetext Import Tool](#)
 - [Attribute Replace Tool](#)
 - [Add attachments to the event](#)
 - [Propose a change to an event that belongs to another organisation](#)
 - [Populate from OpenIOC](#)
 - [Populate from ThreatConnect](#)
 - [Adding IOCs from a PDF report](#)
 - [Publish an event](#)
- [Browsing past events](#)
 - [To list all events](#)
 - [Filters](#)
 - [Event view](#)
 - [Event History](#)
 - [Listing all attributes](#)
 - [Searching for attributes](#)
- [Updating and modifying events and attributes](#)
- [Tagging](#)
- [Templating](#)
- [Contacting the reporter](#)
- [Automation](#)
- [Exporting data](#)
 - [Export page with background jobs disabled](#)
 - [Export page with background jobs enabled](#)
 - [Exporting search results and individual events](#)
- [Connecting to other instances](#)
 - [Setting up a connection to another server](#)
 - [Browsing the currently set up server connections and interacting with them](#)
- [Rest API](#)
 - [Requests](#)
 - [Example - Get single Event](#)
 - [Example - Add new Event](#)

Using the system

Creating an event

The process of entering an event can be split into 3 phases, the creation of the event itself, populating it with attributes and attachments and finally [publishing](#) it.

During this first step, you will create a basic event without any actual attributes, but storing general information such as a description, time and risk level of the incident. To start creating the event, click on the New Event button on the left and fill out the form you are presented with. The following fields need to be filled out:

Add Event

Date	Distribution
<input type="text"/>	<div>All communities ▼</div>
Threat Level	Analysis
<div>High ▼</div>	<div>Initial ▼</div>
Event Description	
<div>Quick Event Description or Tracking Info</div>	
GFI sandbox	
<div>Choose File</div> No file chosen	
<div>Add</div>	

- **Date:** The date when the incident has happened. Just click this field and a date-picker will pop up where you can select the desired date.
- **Distribution:** This setting controls, who will be able to see this event once it becomes published and eventually when it becomes pulled. Apart from being able to set which users on this server are allowed to see the event, this also controls whether the event will be synchronised to other servers or not. The distribution is inherited by attributes: the most restrictive setting wins. The following options are available:
 - **Your organization only:** This setting will only allow members of your organisation to see this. It can be pulled to another instance by one of your organisation members where only your organisation will be able to see it. Events with this setting will not be synchronised. Upon [push](#): do not [push](#). Upon [pull](#) : [pull](#).
 - **This [Community](#)-only:** Users that are part of your MISP [community](#) will be able to see the event. This includes your own organisation, organisations on this MISP server and organisations running MISP servers that synchronise with this server. Any other organisations connected to such linked servers will be restricted from seeing the event. Upon [push](#): do not [push](#). Upon [pull](#): [pull](#) and downgrade to Your organization only.
 - **Connected communities:** Users that are part of your MISP [community](#) will be able to see the event. This includes all organisations on this MISP server, all organisations on MISP servers synchronising with this server and the hosting organisations of servers that connect to those aforementioned servers (so basically any server that is 2 hops away from this one). Any other organisations connected to linked servers that are 2 hops away from this own will be restricted from seeing the event. Upon [push](#): downgrade to This [Community](#) only and [push](#). Upon [pull](#): [pull](#) and downgrade to This [Community](#) only.
 - **All communities:** This will share the event with all MISP communities, allowing the event to be freely propagated from one server to the next. Upon [push](#): [push](#). Upon [pull](#): [pull](#).
 - **Sharing group:** This will share the event to the defined sharing group. This includes only the organisations defined in the sharing group. The distribution can be local and cross-instance depending of the sharing group definition. For more information on [sharing groups](#), refer to the sharing group section.
- **Threat Level:** This field indicates the risk level of the event. Incidents can be categorised into three different threat categories (low, medium, high). This field can alternatively be left as undefined. The 3 options are:
 - **Low:** General mass malware.
 - **Medium:** Advanced Persistent Threats (APT)
 - **High:** Sophisticated APTs and Oday attacks.
- **Analysis:** Indicates the current stage of the analysis for the event, with the following possible options:
 - **Initial:** The analysis is just beginning
 - **Ongoing:** The analysis is in progress
 - **Completed:** The analysis is complete

- **Event Description:** The info field, where the malware/incident can get a brief description starting with the internal reference. This field should be as brief and concise as possible, the more detailed description happens through attributes in the next stage of the event's creation. Keep in mind that the system will automatically replace detected text strings that match a regular expression entry set up by your server's administrator(s).
- **GFI Sandbox:** It is possible to upload the exported .zip file from GFI sandbox with the help of this tool. These will be dissected by the MISP and a list of attributes and attachments will automatically be generated from the .zip file. Whilst this does most of the work needed to be done in the second step of the event's creation, it is important to manually look over all the data that is being entered.

Add attributes to the event

The second step of creating an event is to populate it with attributes and attachments. This can be done by adding them manually or importing the attributes from an external format (OpenIOC, ThreatConnect). To import from an external format or to upload an attachment use the options in the menu on the left.



Using the above shown buttons, you can populate an event using various tools that will be explained in the following section. Let's start with the Add Attribute button.

Add Attribute

Keep in mind that the system searches for regular expressions in the value field of all attributes when entered, replacing detected strings within it as set up by the server's administrator (for example to enforce standardised capitalisation in paths for event correlation or to bring exact paths to a standardised format). The following fields need to be filled out:

Add Attribute

Category	Type	Distribution
Network activity ▼	url ▼	All communities ▼

Value

<http://www.teamliquid.net>

Contextual Comment

☒ for Intrusion Detection System ☐ Batch Import

[Submit](#)

- **Category:** This drop-down menu explains the category of the attribute, meaning what aspect of the malware this attribute is describing. This could mean the persistence mechanisms of the malware or network activity, etc. For a list of valid categories, [click here](#)
- **Type:** Whilst categories determine what aspect of an event they are describing, the Type explains by what means that aspect is being described. As an example, the source IP address of an attack, a source e-mail address or a file sent through an attachment can all describe the payload delivery of a malware. These would be the types of attributes with the category of payload deliver. For an explanation of what each of the types looks like together with the valid combinations of categories and types, [click here](#)
- **Distribution:** This drop-down list allows you to control who will be able to see this attribute. The distribution is inherited by attributes: the most restrictive setting wins. For more info, read the distribution information in the creating an event section - [click here](#)
- **Value:** The actual value of the attribute, enter data about the value based on what is valid for the chosen attribute type. For example, for an attribute of type ip-src (source IP address), 11.11.11.11 would be a valid value. For more information on types and values, [click here](#)
- **Contextual Comment:** You can add some comments to the attribute that will not be used for correlation but instead serves as purely an informational field.
- **For Intrusion Detection System:** This option allows the attribute to be used as an IDS signature when exporting the [NIDS](#) data, unless it is being overruled by the allowedlist. For more information about the allowedlist, head over to the [administration](#) section. If the IDS flag is not set, the attribute is considered as contextual information and not to be used for automatic detection.
- **Batch import:** If there are several attributes of the same type to enter (such as a list of IP addresses, it is possible to enter them all into the same value-field, separated by a line break between each line. This will allow the system to create separate lines for the each attribute.

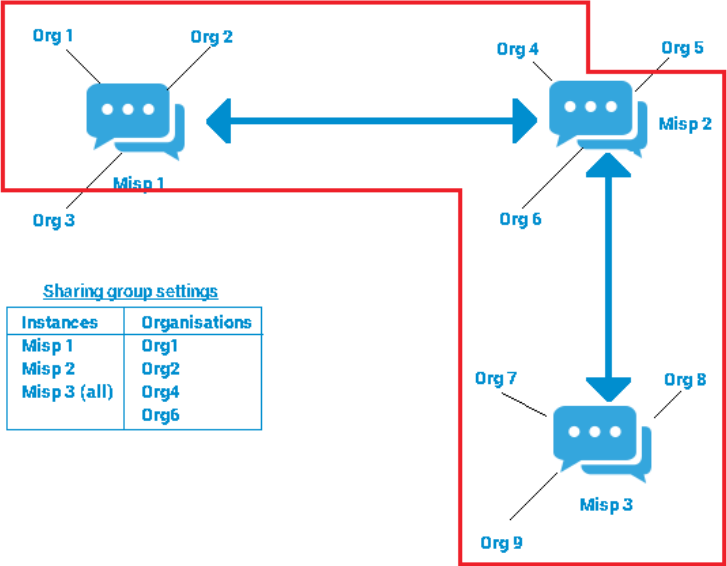
Add Object

Please have a look at the [MISP objects chapter](#)

Create and manage Sharing Groups

[Sharing groups](#) in MISP are a more granular way to create re-usable distribution lists for events/attributes that allow users to include organisations from their own instance (local organisations) as well as organisations from directly, or indirectly connected instances (external organisations). [Sharing groups](#) can be created by any user that has the sharing group editor permission. Additionally, [sharing groups](#) can be edited by any user that has the aforementioned permission in addition to being a member of the sharing group's creating organisation, or any organisation that is marked as an "extender" of the sharing group. The main use for the extend feature is delegating the rights to add users to trusted partners. For example, when sharing with a different industry sector, knowing all actors that should receive the information is often not possible, so delegating the rights to

extend the event to a trusted representative of said sector would allow for someone with more insight to find and add the proper list of partners for the sharing group.



The most general use-cases for [sharing groups](#) are creating re-usable topical subgroups in MISP that share events or for ad-hoc sharing scenarios (such as several organisations involved in a specific incident wanting to work together). Generally [sharing groups](#) add a level of complexity for the users involved as well as a performance overhead on the data marked with it.

As a best-practice recommendation, using traditional distribution methods is preferred unless they cannot cover the given use-case. Also, whilst [sharing groups](#) can be assigned to both events and attributes, it is highly recommended to use the special "inherit" distribution setting on attributes whenever the attribute's sharing group would match the event's.

[Sharing groups](#) consist of the following elements, each of which has its own page in the sharing group creator/editor tool (accessed via the Global actions -> List [Sharing Groups](#) and Add Sharing Group functionalities):

New Sharing Group

General

Organisations

MISP Instances

Summary and Save

Name

Financial Sector

Releasable to

Financial Sector organisations

Description

A general sharing group for the financial sector including financial sector actors like banks, insurance companies or payment processing companies.

☒ Make the sharing group selectable (active)

Next page

- **General:** Metadata describing the intent of the sharing group
 - **Name:** The unique name of the sharing group.
 - **Releasable to:** A human-readable description of who data marked with the sharing group is shareable with. This field is NOT used by MISP for anything besides for being an informational field aimed at extender organisations of the sharing group.
 - **Description:** A natural-text representation of the intent of the sharing group.
 - **Make the sharing group selectable (active):** A sharing group can be made passive by unchecking this setting. All events and attributes will continue to adhere to a passive sharing group's distribution setting, however, the sharing group will not be offered as a selectable option when setting the distribution of events/attributes. The idea behind this is that ad-hoc [sharing groups](#) that have outlived their purpose can be retired in order to reduce the clutter in the UI.

New Sharing Group

General



Organisations

MISP Instances

Summary and Save

Add local organisation

Add remote organisation

Type	Name	UUID	Extend	Actions
local	Org221		<input checked="" type="checkbox"/>	
remote	CIRCL		<input type="checkbox"/>	
remote	CthulhuSPRL.be		<input type="checkbox"/>	

Previous page

Next page


- **Organisations:** The second page of the tool contains the distribution list containing all organisations directly named as a member of the sharing group
 - **Add Local/remote organisations:** The organisations are split into two lists (shown as two tabs in the tool) for local and known remote/external organisations. Local organisations are expected to have at least one local user on the instance whilst remote organisations do not. Synchronising with remote instances will create remote organisations whenever a new event is received of a yet unknown organisation. Remote organisations can always be converted to local organisations - this becomes interesting if a user of an external organisation requests access to your [MISP instance](#).
 - **Extend checkmark:** Checking the extend checkmark makes the selected organisation an extender of the sharing group, meaning they can edit the sharing group. It is expected of these trusted partners that they adhere to the "releasable to" tag set on the general page. The organisation creating the sharing group is always included as an extender.

New Sharing Group

General
Organisations
MISP Instances
Summary and Save

☐ **Enable roaming mode** for this sharing group (pass the event to any connected instance where the sync connection is tied to an organisation contained in the SG organisation list).

Add instance

Name	URL	All orgs	Actions
Local instance	http://192.168.56.101	<input checked="" type="checkbox"/>	
other	http://192.168.56.105	<input type="checkbox"/>	

Previous page
Next page

- **Servers:** The third page of the tool describes the MISP instances the data marked with the given sharing group are allowed to be synchronised with. Keep in mind that any user that can view an event on a given instance will have the right to [pull](#) the event to their home instance, as they are part of the sharing group, however the organisation distribution list will still apply.
 - **Enable roaming mode:** This setting will disable the server list and rely purely on the organisation list to distribute the data. If a sync connection's host organisation is in the organisation distribution list the instance becomes eligible for synchronising the data marked with the sharing group. Generally this carries a slightly higher risk as it relies on administrators correctly setting up the host organisation settings, but it removes the need to know the specific instance urls where the event/attribute should flow.
 - **Add instance:** Add an instance to the distribution list from the sync instances set up under sync actions -> servers
 - **All orgs:** Checking this checkmark will automatically include all organisations on the given instance in the sharing group. This means that in order to exchange with all users of a linked [community](#), one does not need to know every organisation residing on the instance. This also means that the distribution list will not include the organisation names, which can be interesting for certain privacy sensitive communities.

New Sharing Group

General
Organisations
MISP Instances
Summary and Save

General: You are about to create the **Financial Sector** sharing group, which is intended to be releasable to **Financial Sector organisations**.

Local organisations: It will be visible to **all organisations on this instance**, from which **Org221** can extend the sharing group.

External organisations: It will also be visible to **CIRCL, CthulhuSPRL.be**, out of which **nobody** can extend the sharing group.

Synchronisation: Furthermore, events are automatically pushed to: **other**

You can edit this information by going back to one of the previous pages, or if you agree with the above mentioned information, click Submit to create the Sharing group.

Previous page
Submit

- **Summary:** Once everything is set up, MISP will summarise the sharing group in a highlighted text page, which is highly advised to be reviewed before submitting the new sharing group/editing the sharing group. Mistakes in the sharing group settings can lead to organisations that should not be involved in the sharing group getting access or organisations receiving unwanted editing rights to the sharing group. Keep in mind that even if you have submitted a sharing group, it is not propagated until an event/attribute receives the sharing group as the selected distribution.

Populate from Template

Templates allow users to rapidly populate events of a specific type by filling out a series of pre-defined fields. Users with template creation privileges can create new templates for their organisations or for all organisations on their instance. If you are interested in template creation, please refer to the [templating](#) section. For users trying to populate an event, after clicking on the populate from template button, you'll be presented with a list of all currently accessible templates. Pick the one that best describes the event that you are creating.



Once you have chosen a template, you'll be presented with the actual form contained within. Make sure you fill out as many fields as possible with the mandatory fields - marked by a star in a bracket such as this: (*) - are filled out. Templates are divided into sections, with each section having a title and a description in addition to a series of fields. Each field can be an attribute or a file attachment field. An attribute field has the following components:

The screenshot shows a form section titled "Dropped Artifacts" with a blue header. Below the header is a description: "Describe any dropped artifacts that you have encountered during your analysis". The form contains three fields: "Field:" with the value "Artifacts Dropped (File) (*)", "Description:" with the value "Insert any data you have on dropped files here.", and "Types:" with a row of buttons: "filename", "filename/md5", "filename/sha1", "filename/sha256", "md5", "sha1", and "sha256". Below the "Types:" field is a text area with the placeholder text: "Describe the Artifacts Dropped (File) using one or several (separated by a line-break) of the following types: filename".

Field:	Artifacts Dropped (File) (*)
Description:	Insert any data you have on dropped files here.
Types:	<input type="button" value="filename"/> <input type="button" value="filename/md5"/> <input type="button" value="filename/sha1"/> <input type="button" value="filename/sha256"/> <input type="button" value="md5"/> <input type="button" value="sha1"/> <input type="button" value="sha256"/>

Describe the Artifacts Dropped (File) using one or several (separated by a line-break) of the following types: filename

- **Field:** The name of the field along with an indication if the field is mandatory.
- **Description:** A short description of the field.
- **Types:** The value(s) that are valid for the field. In the case of several types being shown here, you can enter value(s) matching any one of the types, or in the case of a batch import field, any mixture of the given types.
- **Text field:** This field can either be a single line textfield or a multi-line text area. For the former, enter a single value of the above indicated type, whilst for the latter you can paste a list of values separated by line-breaks.

Freetext Import Tool



The screenshot shows a web-based interface titled "Freetext Import Tool". Below the title bar, there is a text instruction: "Paste a list of IOCs into the field below for automatic detection." This instruction is positioned above a large, empty text input area. At the bottom of the interface, there are two buttons: a blue "Submit" button on the left and a grey "Cancel" button on the right.

If you have a list of [indicators](#) that you would like to quickly generate attributes out of then the Free-text import tool is just what you need. Simply paste a list of [indicators](#) (separated by line-breaks into this tool).

Freetext Import Results

Below you can see the attributes that are to be created based on the results of the free-text import. Make sure that the categories and the types are correct, often several options will be offered based on an inconclusive automatic resolution.

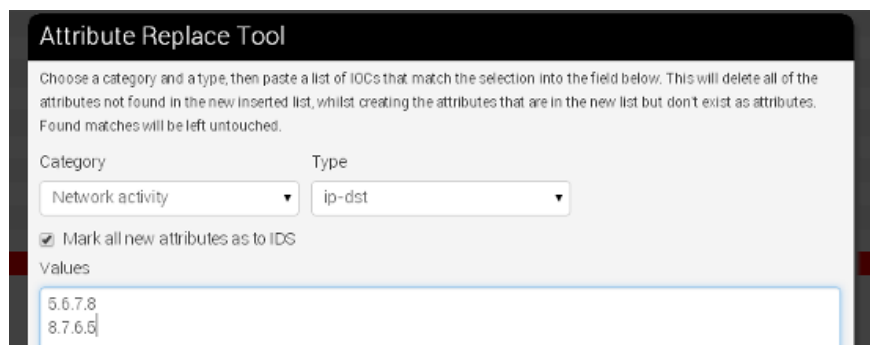
Value	Category	Type	IDS	Actions
192.168.0.1	<input type="text" value="Network activity"/>	<input type="text" value="ip-dst"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
domain.hostname.com	<input type="text" value="Network activity"/>	<input type="text" value="hostname"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
chrome.exe	<input type="text" value="Payload delivery"/>	<input type="text" value="filename"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Since there are several category / type combinations that can be valid for a lot of values, MISP will suggest the most common settings. You can alter the category / type / IDS fields manually if you disagree with the results. The options will be restricted to valid category/type combinations for the value that you have entered.

If any correlation is already found, these correlations will be displayed in the result page.

Attribute Replace Tool

If you would like to create and maintain an event with a set of [indicators](#) that receives removals and additions over time, then the attribute replace tool might make this task easier for you.



The screenshot shows the 'Attribute Replace Tool' interface. It features a title bar, a descriptive text block, two dropdown menus for 'Category' and 'Type', a checkbox for 'Mark all new attributes as to IDS', and a 'Values' text area. The 'Category' dropdown is set to 'Network activity' and the 'Type' dropdown is set to 'ip-dst'. The 'Mark all new attributes as to IDS' checkbox is checked. The 'Values' text area contains the IP addresses '5.6.7.8' and '8.7.6.5'.

Attribute Replace Tool

Choose a category and a type, then paste a list of IOCs that match the selection into the field below. This will delete all of the attributes not found in the new inserted list, whilst creating the attributes that are in the new list but don't exist as attributes. Found matches will be left untouched.

Category: Network activity ▼ Type: ip-dst ▼

☒ Mark all new attributes as to IDS

Values

5.6.7.8
8.7.6.5

Simply select the desired category / type combination, choose whether the attributes should be marked for IDS exports and paste the new list of [indicators](#) into the textarea. Attributes of the same category/type that are present in the event but not the new list will be removed, values in the pasted list that do not yet exist as attributes will be created as attributes and values that already have matching attributes will be left untouched.

Add attachments to the event

You can also upload attachments, such as the malware itself, report files from external analysis or simply artifacts dropped by the malware. Clicking on the add attachment button brings up a form that allows you to quickly attach a file to the event. The following fields need to be filled out:

Add Attachment

Category

Antivirus detection ▼

Distribution

All communities ▼

Contextual Comment

Choose File

No file chosen

☐

Malware

Upload

- **Category:** The category is the same as with the attributes, it answers the question of what the uploaded file is meant to describe.
- **Distribution:** This drop-down list allows you to control who will be able to see this attachment. The distribution is inherited by attributes: the most restrictive setting wins. For more info, refer to the distribution information in the [event section](#).
- **Upload field:** By hitting browse, you can browse your file system and point the uploader to the file that you want to attach to the attribute. This will then be uploaded when the upload button is pushed.
- **Malware:** This check-box marks the file as malware and as such it will be zipped and passworded, to protect the users of the system from accidentally downloading and executing the file. Make sure to tick this if you suspect that the file is infected, before uploading it.
- **Contextual Comment:** You can add some comments to the attribute that will not be used for correlation but instead serves as purely an informational field.

Propose a change to an event that belongs to another organisation

If you would like to propose a modification to an attribute, or to propose some additional attributes to the creating organisation, you can do this with the buttons that replace the add attribute field on the left and the edit icon on the right end of each listed attribute in the event view. The creating organisation of the event will be able to see any [proposals](#) and discard or accept the changes.

Network activity	ip-sec	1.1.1.34	Yes	Connectica communis
		1.1.1.353		

If the organisation that has created the event is on another connected server, they will be able to accept the proposal once they initiate a [pull](#) and receive your proposal. After this they can republish the event, sending the altered attribute back to your instance.

Populate from OpenIOC

It is also possible to attempt to import the data contained in a [.ioc](#) file. The import tool will attempt to gather as many IndicatorItems within nested logical operators as possible without breaking their validity. After the procedure is done, you'll be presented with a list of successfully created attributes and a list of failed IndicatorItems as well as a graph of the [.ioc](#) file.

13 attributes created successfully, 6 indicators could not be mapped and saved.

Successfully added attributes:

Uuid	Category	Type	Value
b9ef2559-cc59-4463-81d9-52800545e16e	Other	other	FileItem/PEInfo/Sections/Section/Name: stub
156bc4b6-a2a1-4735-bfe8-6c8d1f7ee338	Payload installation	filename	mdmcpq3.PNF
e57d9a5b-5e6a-41ec-87c8-ee67f3ed2e20	Payload installation	filename	mdmmerc3.PNF
R2d7baaR-hR7R-4RRR-2d4R-1rRaaR7RRRf	Devined installation	filename	namR/C DME

Visualisation:

```

_OR
  _FileItem/PEInfo/Sections/Section/Name: contains: .stub
  _FileItem/FileName: contains: mdmcpq3.PNF
  _FileItem/FileName: contains: mdmefic3.PNF
  _FileItem/FileName: contains: oem6C.PNF
  _FileItem/FileName: contains: oem7A.PNF
_AND
  _DriverItem/DeviceItem/AttachedToDriverName: contains: fs_rec.sys
  _DriverItem/DeviceItem/AttachedToDriverName: contains: mxiamd.sys
  _DriverItem/DeviceItem/AttachedToDriverName: contains: sr.sys
  _DriverItem/DeviceItem/AttachedToDriverName: contains: fastfat.sys
_AND
  _FileItem/FileName: contains: mxcls.sys
  _FileItem/PEInfo/DigitalSignature/CertificateSubject: contains: Realtek Semiconductor Corp
_AND
  _FileItem/FileName: contains: mxnet.sys
  _FileItem/PEInfo/DigitalSignature/CertificateSubject: contains: Realtek Semiconductor Corp
_AND
  _RegistryItem/Path: contains: HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VMRxCls\ImagePath
  _RegistryItem/Text: contains: mxcls.sys
_AND
  _RegistryItem/Path: contains: HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VMRxNet\ImagePath
  _RegistryItem/Text: contains: mxnet.sys

```

Populate from ThreatConnect

You can also import the data from a ThreatConnect export csv file. The following columns are used by the import tool (and are thus mandatory fields to select during the export):

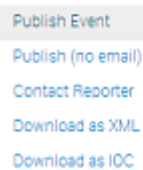
- Type
- Value
- Confidence
- Description
- Source

The result will be a list of attributes that get added to the currently selected event, each of which will be marked with a comment that indicates that its origin being from a ThreatConnect import.

Adding IOCs from a PDF report

You can use a generic script called [IOC parser](#) or use a script published by Palo Alto to convert [IOC parser](#) output to a [MISP event](#): [report_to_misp] (https://github.com/PaloAltoNetworks-BD/report_to_misp/).

Publish an event



Publish Event

- Publish (no email)
- Contact Reporter
- Download as XML
- Download as IOC

Once all the attributes and attachments that you want to include with the event are uploaded / set, it is time to finalise its creation by **publishing** the event (click on publish event in the event view). This will alert the eligible users of it (based on the private-controls of the event and its attributes/attachments and whether they have auto-alert turned on), **push** the event to instances that your instance connects to and propagate it further based on the distribution rules. It also readies the network related attributes for **NIDS** signature creation (through the **NIDS** signature export feature, for more information, go to the export section.). There is an alternate way of **publishing** an event without alerting any other users, by using the "publish (no email)" button. This should only be used for minor edits (such as correcting a typo).

If your instance has background jobs enabled then the event might not get published immediately.

Browsing past events

The MISP interface allows the user to have an overview over or to search for events and attributes of events that are already stored in the system in various ways.

To list all events

On the left menu bar, the option "List events" will generate a list of the last 60 events. While the attributes themselves aren't shown in this view, the following pieces of information can be seen:

Events

« previous		next »	
Datefrom : 2014-03-04 Dateuntil : 2014-03-05 org : ADMIN ✕			
Published Q	Org Q	id	Tags Q #Attr: Q Date Q Threat Q Analysis Q Info Q Distribution Q Actions
ADMIN			
✓		3	4 2014-03-05 High Initial Test Event 3 All 
✓		2	 1 2014-03-05 High Initial Test Event 2 All 
✓		1	1 2014-03-05 Low Completed Test Event 1 All 

- **Published:** Already published events are marked by a checkmark. Unpublished events are marked by a cross.
- **Org:** The organisation that created the event.
- **Owner Org:** The organisation that owns the event on this instance. This field is only visible to administrators.
- **ID:** The event's ID number, assigned by the system when the event was first entered (or in the case of an event that was synchronized, when it was first copied over - more on [synchronisation](#) in chapter xy)
- **Tags:** Tags that are assigned to this event.
- **#Attr.:** The number of attributes that the event has.
- **Email:** The e-mail address of the event's reporter. This is not visible to regular users. Organisation administrators can see the e-mail addresses of their own organisation's users.
- **Date:** The date of the attack.
- **Threat Level:** The risk level of the attack, the following levels are possible:
 - **Low:** General Malware
 - **Medium:** Advanced Persistent Threats (APTs)
 - **High:** Sophisticated APTs and Oday exploits
 - **Undefined:** This field can be left undefined and edited at a later date.
- **Analysis:** Indicates the current stage of the analysis for the event, with the following possible options:
 - **Initial:** The analysis is just beginning
 - **Ongoing:** The analysis is in progress
 - **Completed:** The analysis is complete
- **Info:** A short description of the event, starting with an internal reference number.
- **Distribution:** This field indicates what the sharing privileges of the event. For details, refer to the distribution information in the [event section](#).
- **Actions:** The controls that the user has to view or modify the event. The possible actions that are available (depending on user privileges - [click here](#) to find out more about privileges):
 - **Publish:** [Publishing](#) an event will have several effects: The system will e-mail all eligible users that have auto-alert turned on (and having the needed privileges for the event, depending on its private classification) with a description of your newly published event, it will be flagged as published and it will be pushed to all eligible servers (to read more about [synchronisation](#) between servers, have a look at the [section on connecting servers](#))
 - **Edit:** Clicking on the edit button will bring up the same same screen as the one used for creating new events, with the exception that all fields come filled out with the data of the event that is being edited. The distribution of an event can only be edited if you are a user of the creating organisation of the event. For more information on this view, refer to the section on [creating an event](#).
 - **Delete:** The system will prompt you before erasing the unwanted event.
 - **View:** Will bring up the event view, which besides the basic information contained in the event list, will also include the following:

Filters

It is also possible to filter the events shown by clicking on the small magnifying glass icons next to the field names and entering a filter term.

Event view

Test Event 3

Event ID3

Uuid53174081-1d0c-41be-9bd9-4f1ec0a80e0a

OrgADMIN

Contributorsargh

Tags

test

Date2014-03-05

Threat LevelHigh

AnalysisInitial

DistributionAll communities, this will share the event with all MSP communities, allowing the event to be freely propagated from one server to the next.

DescriptionTest Event 3

PublishedYes

Pivots

Attributes

Discussion

3: Test Ev.

Related Events

[2014-03-05 \(1\)](#) [2014-03-05 \(2\)](#) [2014-02-21 \(4\)](#)

Date

Category

Type

Value

Comment

Related Events

IDS

Distribution

Actions

2014-03-05

Network activity

io-src

1.1.1.1

An IP address

2.1

Yes

All

2014-03-05

io-src

2.2.2.2

An IP address

Yes

All

2.2.2.3

An IP address

2014-03-05

io-src

3.3.3.3

An IP address

4

Yes

All

General Event Information

- **ID:** The ID of the event.
- **Uuid:** In order to avoid collisions between events and attributes (during for example a sync) a Uuid is assigned that uniquely identifies each of them.
- **Org** The organisation that has originally created the event. The logo (if it exists on the server, alternatively a string) representing the organisation is also shown in the right upper corner.
- **Contributors:** Shows a list of the organisations that have contributed to the event via [proposals](#). If you click any of the logos listed here, you'll get redirected to a filtered event history view, including only the changes made by the organisation.
- **Tags:** A list of tags associated with the event. Clicking a tag will show a list of events with the same tag attached. The little cross next to each tag allows you to remove the tag from the event, whilst the '+' button allows you to assign a tag. For the latter two options to be visible, you have to have [tagging](#) permission.
- **Date:** The date of detection, set by the user that creates the event, not to be confused with the creation date of the event.
- **Threat Level:** The assigned threat level of the event.
- **Analysis:** The status of the analysis.
- **Distribution:** This shows the distribution rules applied to this event, controlling whether only the creating organisation can see (Your organisation only) it or everyone on the instance (This [community](#) only). The two remaining settings allow the event to be propagated to organisations on remote connected instances.
- **Info:** A short description of the event itself. Make sure not to put information in here that could be used for correlation purposes and be better suited as an Attribute.
- **Published:** Whether the event has been published or not. [Publishing](#) allows the attributes of the event to be used for all eligible exports and it notifies users that have subscribed to the event alerts. Also, a publish initiates a [push](#) to all eligible instances.

List of Related Events The list of relations is shown on the right hand side of the general event information. Events can be related by having one or more attributes that are exact matches. For example, if two events both contain a source IP attribute of 11.11.11.11 then they are related. The list of events that are related to the currently shown one, are listed under "Related Events", as links (titled the related event's date and ID number) to the events themselves.

Data Element Toggles You can control some of the data that is shown on this page using three toggles. The elements that can be disabled are the pivot threads, the attributes (and [proposals](#)) and the Discussions. You can collapse these elements and then expand them again using the same button.

Pivot Threads While moving from event to event through the relation links (a process that we refer to as [pivoting](#)), you create a path that shows which events you have traversed. This path is reset by leaving the event view and navigating elsewhere in the application or by deleting the root pivot element. Each event

visited is represented by a bubble in the pivot thread graph, connected by lines that show how the user has arrived at the next connected event. It is possible to jump back to an earlier relation and pivot to another event through that, creating branches in the graph. The currently selected event is coloured blue in the graph. If you would like to delete an element from the graph (including all of elements that branch off of it) just click on the small x within a pivot bubble. For a deletion to be possible the following conditions have to be met:

- The pivot element to be deleted cannot be on the path that leads to the currently selected event
- The pivot element residing in the graph's root can always be deleted - this will simply reset the current pivot thread

Attributes and [Proposals](#) A list of all attributes and [proposals](#) attached to the event. The fields for each of them only differ in the available actions and the fact that for [proposals](#) to attributes all fields are blank that would stay unchanged if the proposal was accepted (for example, proposing a change to an attribute to turn the IDS flag on will have all fields apart from the IDS flag blank in the proposal. Here is a list of what each of the fields represents:

- **Date:** The date of the last modification to the attribute. [Proposals](#) don't have a date of last edit.
- **Category:** The category of the attribute or proposal. For a list of possible categories visit the section on [categories and types](#).
- **Type:** The type of the attribute or proposal. For a list of possible categories visit the section on [categories and types](#).
- **Value:** The value or value-pair of the attribute. This is the main payload of the attribute, which is described by the category and type columns. For certain types of attributes that are made up of value-pairs the two parts will be split by a pipe (|), such as for filename|md5. The value field(s) are used by the correlation engine to find relations between events. In value-pair attributes both values are correlated individually.
- **Comment:** Attributes can have a contextual comment to further describe the attribute. These comments are not used for correlation and are purely informative.
- **Related Events:** A list of the event IDs that also contain an attribute with the same value.
- **IDS:** Flags an attribute as an indicator of compromise, allowing it to be included in all of the eligible exports.
- **Distribution:** Defines the distribution of the attribute individually. An attribute can have a different distribution level than the event. In any case, the lowest distribution level of the two is used.
- **Actions:** The user can interact with the events through these buttons, which will be further described in the next portion of the guide as they differ for attributes and [proposals](#).

Depending on the colour coding of the row, you can have an attribute, a proposal to the event or a proposal to an attribute:

- **Attributes:** Each uncoloured line represents an Attribute.

- **Proposals to an Event:** Each gray line at the end of the list represents a Proposal to an event. These are [proposals](#) for a new attribute, mostly unrelated to any of the currently existing attributes. If the creator of the event accepts one of these a new attribute will be created.
- **Proposals to an Attribute:** Each attribute can have several edit [proposals](#). These will be placed right below the attribute that the proposal affects and - as with the event [proposals](#) - is coloured grey. The original attribute's row is coloured blue if a proposal exists for it.

Using the modify button will bring up the attribute creation view, with all data filled out with the attribute's currently stored data.

Event Discussion Thread

Each event has its own assigned discussion where users (that are eligible to see the event) can participate in an open discussion. The users are anonymised in the messages, all that other users will see is their user ID number and their organisation. To post a message on the Event Discussion, either use the reply button on a previous post or use the quickresponse field at the bottom of the page. Each post is made up of the following:

- **Date:** The date when the post was created.
- **Post navigation:** This should be the post's ID as well as a link to jump to the top of the discussion thread on the page itself.
- **Organisation logo:** If such an image exists for the organisation that has posted the message, then the logo is shown.
- **Message:** The body of the post itself. This can also include automatically generated links to other events and threads as well as show quoted text in embedded bubbles. Editing an event will also append a post with a message indicating that it was edited together with the timestamp of the edit.
- **User:** The e-mail address of the poster if he/she is from the organisation as the current user. Alternatively a generated string is shown that includes the user ID of the user, so that his/her e-mail address could remain hidden whilst still being identifiable.
- **Action buttons:** Edit, Delete and Reply. The first two of the three options are only available to the poster of the message or a [site admin](#). Quoting a post will automatically include the original message in [quote] tags.

Here is a list of the various tools you can use while using this feature:

- **Pagination:** There are 5 posts visible on each event page, if there have been more messages posted, use the previous and next button to navigate through the thread. This will not reload the rest of the page.
- **Discussion Tags:** Users can quote something by encapsulating it in [quote] [/quote] tags, they can create a link to another event with the [event] [/event] tags or to another discussion thread with [thread] [/thread].
- **Quick Post:** Adding a post will take the user to a separate add Post page, something that can be a bit of an inconvenience. To avoid this, there is a quick post button, where users can add messages on the fly without having to reload the page. On top of the quick post field, 3 buttons allow users to generate quote, event and thread tags quickly.


Event History

View the logs of the event that show how the event has changed over time, including the contribution from other organisations in the form of [proposals](#). There are two ways to get to this view, either by clicking on View Event History on the side menu of an event view, or by clicking on a contributing organisation's logo on the event view. The latter will show a restricted form of the logs, showing only [Proposals](#) created by the selected organisation. The fields shown in this view are as described as follows:

- **Org:** The logo (or in the lack thereof a string representation) of the organisation.
- **Action:** Each entry in the log happens during an action, such as the creation, modification or deletion of data and some special actions (such as accepting a proposal). This field shows which action caused the entry to be created.
- **Model:** As described above, a log entry is generated on certain actions. This field shows which type of data was affected that caused the log entry to be created (such as a change to the event, the creation of an attribute, the discarding of a proposal, etc).
- **Title:** This is a short description of the change itself and it is not nearly as detailed as the information administrators get in the audit logs. However, for attributes and [proposals](#) the category / type and value of the created or edited attribute is shown.
- **Created:** The date and time of the log entry's creation.

Listing all attributes

Apart from having a list of all the events, it is also possible to get a list of

Event	Org	Category	Type	Value	Comment	IDS	Actions
5		Other	comment	asdasdasd		Yes	
4		Network activity	ip-src	2.2.2.2		Yes	
4		Network activity	ip-src	3.3.3.3		Yes	

- **Event:** This is the ID number of the event that the attribute is tied to. If an event belongs to your organisation, then this field will be coloured red.
- **Org:** The organisation that has created the event.
- **Category:** The category of the attribute, showing what the attribute describes (for example the malware's payload). For more information on categories, go to section xy
- **Type:** The type of the value contained in the attribute (for example a source IP address). For more information on types, go to section xy
- **Value:** The actual value of the attribute, describing an aspect, defined by the category and type fields of the malware (for example 11.11.11.11).
- **Comment:** An optional contextual comment attached to the attribute.
- **IDS:** Shows whether the attribute has been flagged for [NIDS](#) signature generation or not.
- **Actions:** A set of buttons that allow you to view the event that the attribute is tied to, to edit the attribute (using the same view as what is used to set up attributes, but filled out with the attribute's current data) and a delete button.

Searching for attributes

Apart from being able to list all events, it is also possible to search for data contained in the value field of an attribute, by clicking on the "Search Attributes" button.

Search Attribute

You can search for attributes based on contained expression within the value, event ID, submitting organisation, category and type.
For the value, event ID and organisation, you can enter several search terms by entering each term as a new line. To exclude things from a result, use the NOT operator (!) in front of the term.

Containing the following expressions

Being attributes of the following event IDs

From the following organisation(s)

Type

ALL

Category

ALL

☐ Only find valid IOCs





Search

This will bring up a form that lets you enter one or several search strings (separate search strings with line breaks) that will be compared to the values of all attributes, along with options to narrow down the search based on category and type. The entered search string has to be an exact match with (the sub-string of) a value. A second text field makes it possible to enter event IDs for events that should be excluded from the search (again, each line represents an event ID to be excluded). The third text field allows the user to restrict the results to attributes from certain organisations or to attributes not created by certain other organisations, using the above described syntax. The list generated by the search will look exactly the same as listing all attributes, except that only the attributes that matched the search criteria will be listed (to find out more about the list attributes view, [click here](#)). The search parameters will be shown above the produced list and the search terms will be highlighted. The last option is a checkbox that restricts all of the results to attributes that are marked as IDS signatures.

Attributes

Results for all attributes with the value containing "1.1.1.1".

« PREVIOUS
NEXT »

Event #	Org	Category	Type	Value	Comment	IDS	Actions
3		Network activity	ip-src	1.1.1.1	An IP address	Yes	
5		Network activity	ip-src	1.1.1.1	The same IP address	Yes	

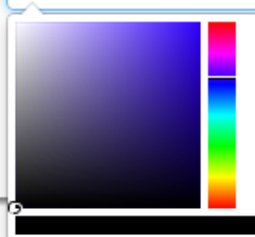
Updating and modifying events and attributes

Every event and attribute can easily be edited. First of all it is important to find the event or attribute that is to be edited, using any of the methods mentioned in the section on [browsing past events](#). Once it is found, the edit button (whether it be under actions when events/attributes get listed or simply on the event view) will bring up the same screen as what is used to create the entry of the same type (for an event it would be the event screen as [seen here](#), for an attribute the attribute screen as [described here](#)). You can also simply double-click on the event you wish to edit and enter the edit mode. Keep in mind that editing any event (either directly or indirectly through an attribute) will unpublish it, meaning that you'll have to publish it (through the event view) again once you are done.

Tagging

As described earlier, users with [tagging](#) rights can arbitrarily tag events using tags chosen from a pool of available options. If you have [tagging](#) privileges and would like to create a new tag, navigate to Event Actions - Add Tag. You'll be presented with the following form:

Add Tag

Name	Colour
<input type="text" value="OSINT"/>	<input type="text" value="#000000"/>
<input type="button" value="Add"/>	

Fill out the following fields:

- **Name:** Pick a name for the tag. Try to use consistent naming conventions across your instance, to avoid confusion.
- **Colour:** You can choose a colour for the tag by clicking on the colour field and using the colour picker tool. Try to avoid having duplicate or similar looking colours to help avoid confusion.

Templating

Newer users can easily be overwhelmed by having to manually populate events with attributes without any guidance. What sort of information should go into the event? What should be the category and type of a C2 IP? Templates allow users to use simple forms to populate events. Even though MISP ships with a few default templates, it is possible for users (with the appropriate [templating](#) privilege) to create new templates for their users or for all users of the instance. Let's look at how you can create a template. First go to Event Actions - Add Template to go to the event creation view.

Create Template

Name

Tags

OSINT x +

Event Description

Use this template to create OSINT events.

☒ Share this template with others

Create

The following fields have to be filled out:

- **Name:** The name of the template should describe what type of an event it should be used to generate attributes.
- **Tags:** You can attach tags to the template - an event populated using the template would automatically receive the tag(s). Add new tags using the + button. If you change your mind about a tag you can remove it with the cross next to the tag name.
- **Event Description:** A short description about the events that this template should be used for.
- **Share this template with others:** The template can be set to be usable by any organisation on the instance or only by the one that has created it.

Once the skeleton template is created, you can start populating the template with data. There are 3 types of elements that can be used during the creation of a template: attribute, file and text elements. Text elements divide the template into sections with an information field, followed by all of the attribute/file fields until a new text field is read. Don't worry about the order of the elements during creation, they can be re-arranged using drag & drop. Let's look at the 3 element types:

Attribute Element

Add Attribute Element To Template

Name

Description

Category: Payload installation Type: File

☒ Use complex types

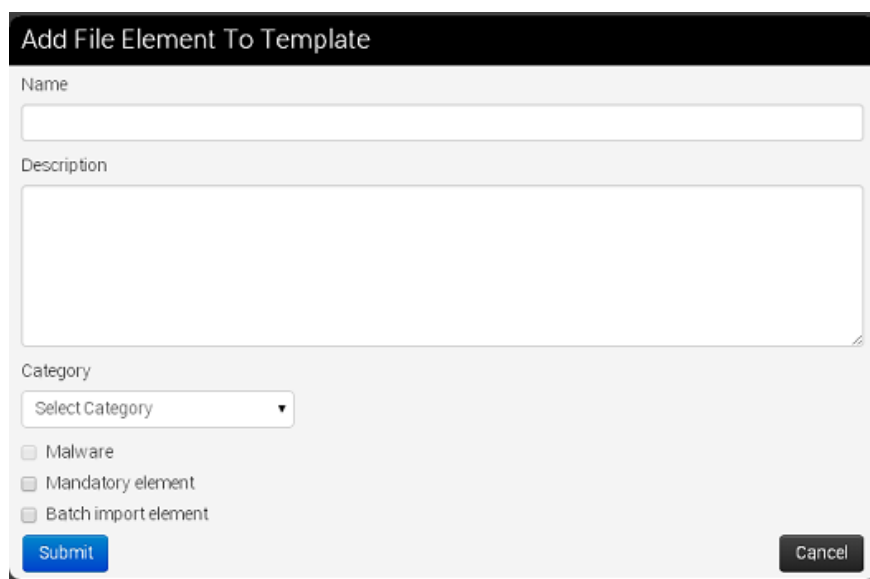
Types allowed based on the above setting:
 filename filename/md5 filename/sha1 filename/sha256 md5 sha1 sha256

☐ Automatically mark for IDS
☐ Mandatory element
☐ Batch import element

The following fields have to be filled out:

- **Name:** The field name that will be presented to the user.
- **Description:** A brief description of the element. Make sure that you provide sufficient information to the user to make it obvious what is expected.
- **Category:** The category used for any attributes created using this template element.
- **Type:** The type or complex type used for any attributes created using this template element. Complex types allow for several related types to be used on data entry. For example, a "file" complex type element allows for filenames and hashes.
- **Use Complex types:** If the category permits it, switch to a complex type using this checkbox.
- **Automatically mark for IDS:** If checked, any attributes generated using this element will be marked for IDS exporting.
- **Mandatory element:** If the element is marked as mandatory, then the template form can only be submitted by users if this field is filled out.
- **Batch import element:** Allow for multiple values to be entered (separated by line breaks).

File Element



The screenshot shows a web form titled "Add File Element To Template". The form has a light gray background and a dark gray header bar with the title. It contains the following fields and controls:

- Name:** A text input field.
- Description:** A large text area for a detailed description.
- Category:** A dropdown menu with the placeholder text "Select Category".
- Malware:** A checkbox.
- Mandatory element:** A checkbox.
- Batch import element:** A checkbox.
- Submit:** A blue button.
- Cancel:** A gray button.

The following fields have to be filled out:

- **Name:** The field name that will be presented to the user.
- **Description:** A brief description of the element. Make sure that you provide sufficient information to the user to make it obvious what is expected.
- **Category:** The category to be used by all attachments uploaded through this element.
- **Malware:** If the uploaded files are malicious and should be encrypted and password protected, mark this checkbox.
- **Mandatory element:** If it should be required to upload an attachment, check this checkbox.
- **Batch import element:** Ticking this checkbox allows users to upload several files using this element.

Text Element

Add Text Element To Template

Name

Text

Submit

Cancel

The following fields have to be filled out:

- **Name:** The name of the section that will be presented to the user.
- **Text:** The description of the section. Explain briefly to the user what the following attribute/file elements will be dealing with. There are several ways to split a template into sections, try to have ease of use in mind while creating it.

Contacting the reporter

To get in touch with the reporter of a previously registered event, just find the event for which you would like to contact the reporter by either finding it on the list of events, by finding it through one of its attributes or by finding it through a related event. Once the event is found and the event view opened, click the button titled "Contact Reporter". This will bring up a view where you can enter your message that is to be e-mailed to all members of the reporting organisation that subscribe to receiving such reports or the reporting user himself. Along with your message, the detailed information about the event in question will be included in the e-mail.

Contact organization reporting event 12

You are about to contact the organization that reported event 12.
Feel free to add a custom message that will be sent to the reporting organization.
Your email address and details about the event will be added automatically to the message.

Message

☐ Submit only to person

By selecting this box you will contact the creator of the event only.

Submit

By default, the message will be sent to every member of the organisation that posted the event in the first place, but if you tick the check-box below the message field before sending the mail, only the person that reported the event will get e-mailed.

Automation

It is possible to quickly and conveniently export the data contained within the system using the automation features located in the main menu on the left (available to users with authentication key access only). There are various sets of data that can be exported, by using the authentication key provided by the system (also shown on the export page). If for whatever reason you would need to invalidate your current key and get a new one instead (for example due to the old one becoming compromised) just hit the reset link next to the authentication key in the export view or in your "my profile" view. To find out about the various export formats and the usage within the automation functions, please read the page on the [API's usage](#).

Exporting data

For users that do not have authentication key access, an alternate export feature is available that relies on your interactive login to the site. To access these, just use the export menu button to the left and you'll be presented with a list of export options. Depending on your server's configuration, you will be presented with one of two possible pages, depending on whether you have background processing enabled or not.

Export page with background jobs disabled

The page will list a set of export formats that you can immediately download as a file. Just click on the desired export format and MISP will start collecting all the data that you will receive in a file. Keep in mind that this can be a lengthy process. To avoid having to wait, consult with your instance's site administrator about enabling the background processing.

Export

Export functionality is designed to automatically generate signatures for intrusion detection systems. To enable signature generation for a given attribute, Signature field of this attribute must be set to Yes. Note that not all attribute types are applicable for signature generation, currently we only support NIDS signature generation for IP, domains, host names, user agents etc. and hash list generation for MD5/SHA1 values of file artifacts. Support for more attribute types is planned.

Simply click on any of the following buttons to download the appropriate data.

- Click this to download all events and attributes that you have access to (except file attachments) in a custom XML format.
- Click this to download all attributes that are indicators and that you have access to (except file attachments) in CSV format.
- Click this to download all attributes that you have access to (except file attachments) in CSV format.
- Click this to download all network-related attributes that you have access to under the Snort rule format. Only published events and attributes marked as IDS Signature are exported. Administration is able to maintain a whitelist containing host, domain name and IP numbers to exclude from the NIDS export.
- Click on one of these two buttons to download all MD5 or SHA1 checksums contained in file-related attributes. This list can be used to feed forensic software when searching for suspicious files. Only published events and attributes marked as IDS Signature are exported.
-

Click on one of these buttons to download all the attributes with the matching type. This list can be used to feed forensic software when searching for suspicious files. Only published events and attributes marked as IDS Signature are exported.

- | | | | | | | | | | | | | | |
|---|---|--|---|--|---|---|---------------------------------------|--|---|--|---|--|--|
| <input type="button" value="md5"/> | <input type="button" value="sha1"/> | <input type="button" value="sha256"/> | <input type="button" value="filename"/> | <input type="button" value="filenamemd5"/> | <input type="button" value="filenamesha1"/> | <input type="button" value="filenamesha256"/> | <input type="button" value="ip-src"/> | <input type="button" value="ip-dst"/> | <input type="button" value="hostname"/> | <input type="button" value="domain"/> | <input type="button" value="email-src"/> | <input type="button" value="email-dst"/> | <input type="button" value="email-subject"/> |
| <input type="button" value="email-attachment"/> | <input type="button" value="url"/> | <input type="button" value="http-method"/> | <input type="button" value="user-agent"/> | <input type="button" value="regkey"/> | <input type="button" value="regkeyvalue"/> | <input type="button" value="AS"/> | <input type="button" value="snort"/> | <input type="button" value="pattern-in-file"/> | <input type="button" value="pattern-in-traffic"/> | <input type="button" value="pattern-in-memory"/> | <input type="button" value="yara"/> | <input type="button" value="vulnerability"/> | |
| <input type="button" value="attachment"/> | <input type="button" value="malware-sample"/> | <input type="button" value="link"/> | <input type="button" value="comment"/> | <input type="button" value="text"/> | <input type="button" value="other"/> | <input type="button" value="named pipe"/> | <input type="button" value="mutex"/> | <input type="button" value="target-user"/> | <input type="button" value="target-email"/> | <input type="button" value="target-machine"/> | <input type="button" value="target-org"/> | <input type="button" value="target-location"/> | |
| <input type="button" value="target-external"/> | | | | | | | | | | | | | |

Export page with background jobs enabled

If the background jobs are enabled, you'll be redirected to a different version of the export page. Here you will see a table with all of the major export formats and the current status of the cached export files. Keep in mind that these are generated on an organisation by organisation basis, so even though others have generated newer export caches your organisation may have an outdated cache. You can simply issue a generate command (by clicking the "Generate" button) on the desired export type and the background workers will start fetching and assembling your cache. A progress bar will show the progress of the export process. Once done, you can click "Download" to download the freshly generated cache file. If the cache is already up to date from before, then you don't have to regenerate the cache, just click on the "download" button. You may have noticed that the TEXT export only has a generate button - this is because TEXT exports are made up of a lot of types of exports, all of which get generated together. To download any of these files, just click on any of the attribute types at the bottom of the table. A quick description of each of the fields in the table:

- **Type:** The type of the export (such as XML, Suricata, MD5, etc.).
- **Last Update:** The generation date of the current cache for the given export type.
- **Description:** A description of the export format.
- **Outdated:** This compares the cache generation date to the last timestamp when an event was updated and lets you know whether the cache is outdated or not.
- **Progress:** Shows the progress of the last initiated generation process.
- **Actions:** Download or Generate the given cache with these buttons.

Export

Export functionality is designed to automatically generate signatures for intrusion detection systems. To enable signature generation for a given attribute, Signature field of this attribute must be set to Yes. Note that not all attribute types are applicable for signature generation, currently we only support NIDS signature generation for IP, domains, host names, user agents etc., and hash list generation for MD5/SHA1 values of file artifacts. Support for more attribute types is planned.

Simply click on any of the following buttons to download the appropriate data.

Type	Last Update	Description	Outdated	Progress	Actions
XML	N/A	Click this to download all events and attributes that you have access to (except file attachments) in a custom XML format.	Yes	Completed.	Download Generate
CSV_Sig	N/A	Click this to download all attributes that are indicators and that you have access to (except file attachments) in CSV format.	Yes	Completed.	Download Generate
CSV_All	N/A	Click this to download all attributes that you have access to (except file attachments) in CSV format.	Yes	Completed.	Download Generate
Suricata	N/A	Click this to download all network related attributes that you have access to under the Suricata rule format. Only published events and attributes marked as IDS Signature are exported. Administration is able to maintain a whitelist containing host, domain name and IP numbers to exclude from the NIDS export.	Yes	Completed.	Download Generate
Snort	N/A	Click this to download all network related attributes that you have access to under the Snort rule format. Only published events and attributes marked as IDS Signature are exported. Administration is able to maintain a whitelist containing host, domain name and IP numbers to exclude from the NIDS export.	Yes	Completed.	Download Generate
MD5	2 weeks ago	Click on one of these two buttons to download all MD5 checksums contained in file-related attributes. This list can be used to feed forensic software when searching for suspicious files. Only published events and attributes marked as IDS Signature are exported.	Yes	Completed.	Download Generate
SHA1	N/A	Click on one of these two buttons to download all SHA1 checksums contained in file-related attributes. This list can be used to feed forensic software when searching for suspicious files. Only published events and attributes marked as IDS Signature are exported.	Yes	Completed.	Download Generate
TEXT	N/A	Click on one of the buttons below to download all the attributes with the matching type. This list can be used to feed forensic software when searching for suspicious files. Only published events and attributes marked as IDS Signature are exported.	Yes	Completed.	Generate

[md5](#) [sha1](#) [sha256](#) [filename](#) [filenamemd5](#) [filenamesha1](#) [filenamesha256](#) [ip-src](#) [ip-dst](#) [hostname](#) [domain](#) [email-src](#) [email-dst](#) [email-subject](#) [email-attachment](#) [url](#) [http-method](#) [user-agent](#) [regkey](#)
[regkeyvalue](#) [ad](#) [snort](#) [pattern-in-file](#) [pattern-in-traffic](#) [pattern-in-memory](#) [vba](#) [vulnerability](#) [attachment](#) [malware-sample](#) [link](#) [comment](#) [text](#) [other](#) [named pipe](#) [mutex](#) [target-user](#) [target-email](#)

Exporting search results and individual events

Apart from the options offered by the export pages, it's also possible to export all events involved in a search attribute result table, by using the "Download results as XML" button on the left menu bar.

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

[List Attributes](#)
[Search Attributes](#)

[Download results as XML](#)

[Export](#)
[Automation](#)

Attributes

Results for all attributes with the value containing "1.1.1":

« previous next »

Event	Category	Type	Value
7	Network activity	ip-src	1.1.1.34

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

« previous next »

Each event's view has its own export feature, both as an XML export and as a [.ioc](#) file. To reach these features, just navigate to an event and use the appropriate buttons on the right side.

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

[List Attributes](#)
[Search Attributes](#)

[Download results as XML](#)

[Export](#)
[Automation](#)

Attributes

Results for all attributes with the value containing "1.1.1*":

« previous next »

Event	Category	Type	Value
7	Network activity	ip-src	1.1.1.34

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

« previous next »

Connecting to other instances

Apart from being a self contained repository of attacks/malware, one of the main features of MISP is its ability to connect to other instances and share (parts of) its information. The following options allow you to set up and maintain such connections.

Setting up a connection to another server

In order to share data with a remote server via pushes and pulls, you need to request a valid authentication key from the hosting organisation of the remote instance. When clicking on List Servers and then on New Server, a form comes up that needs to be filled out in order for your instance to connect to it. The following fields need to be filled out:

Add Server

Base URL	Organization	Authkey
<input type="text" value="https://www.friendlymisp.com"/>	<input type="text" value="Org_name"/>	<input type="text"/>
<input checked="" type="checkbox"/> Push	<input checked="" type="checkbox"/> Pull	
<input type="checkbox"/> Self Signed		
Certificate file		
<input type="button" value="Choose File"/>	No file chosen	
<input type="button" value="Add"/>		

- **Base URL:** The URL of the remote server.
- **Organization:** The organisation that runs the remote server. It is very important that this setting is filled out exactly as the organisation name set up in the bootstrap file of the remote instance.
- **Authkey:** The authentication key that you have received from the hosting organisation of the remote instance.
- **Push:** This check-box controls whether your server is allowed to [push](#) to the remote instance.
- **Pull:** This check-box controls whether your server can request to [pull](#) all data from the remote instance.
- **Self Signed:** Ticking this checkbox will allow syncing with instances using self-signed certificates.
- **Certificate File:** If the instance that you want to connect to has their entire own certificate chain, you can use this to import a .pem file with it and override CakePHP's standard root CA file.

If you are an administrator, trying to allow another instance to connect to your own, it is vital that two rules are followed when setting up a [synchronisation](#) account:


- The [synchronisation](#) user has to have the sync permission and full read/write/publish privileges turned on
- Both the [sync user](#) and the organisation setting in your instance's Config/bootstrap.php file have to match the organisation identifier of the hosting organisation.

Browsing the currently set up server connections and interacting with them

If you ever need to change the data about the linked servers or remove any connections, you have the following options to view and manipulate the server connections, when clicking on List Servers: (you will be able to see a list of all servers that your server connects to, including the base address, the organisation running the server the last pushed and pulled event IDs and the control buttons.).

Servers

« previous next »

Push	Pull	Url	From	Cert File	Self Signed	Org	Last Pulled ID	Last Pushed ID	Actions
No	Yes	http://192.168.14.11	11	5.pem	Yes	ADMIN			 

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

- **Editing the connection to the:** By clicking edit a view, [that is identical to the new instance view](#), is loaded, with all the current information of the instance pre-entered.
- **Deleting the connection to the instance:** Clicking the delete button will delete the link to the instance.
- **Push all:** By clicking this button, all events that are eligible to be pushed on the instance you are on will start to be pushed to the remote instance. Events and attributes that exist on the far end will be updated.
- **Pull all:** By clicking this button, all events that are set to be [pull](#)-able or full access on the remote server will be copied to this instance. Existing events will not be updated.

Rest API

The platform is also [RESTfull](#), so this means that you can use structured format (XML or JSON) to access Events data.

Requests

Use any HTTP compliant library to perform requests. You can choose which format you would like to use as input/output for the REST calls by specifying the Accept and Content-Type headers.

The following headers are required if you wish to receive / [push](#) XML data:

Authorization: *your authorisation key* **Accept:** *application/xml* **Content-Type:** *application/xml*

The following headers are required if you wish to receive / [push](#) JSON data:

Authorization: *your authorisation key* **Accept:** *application/json* **Content-Type:** *application/json* The following table shows the relation of the request type and the resulting action:

HTTP format	URL	Controller action invoked
GET	/events	EventsController::index()
GET	/events/123	EventsController::view(123)
POST	/events	EventsController::add()
PUT	/events/123	EventsController::edit(123)
DELETE	/events/123	EventsController::delete(123)
POST	/events/123	EventsController::edit(123)

*Attachments are included using base64 encoding below the `data` tag.

Example - Get single Event

In this example we fetch the details of a single Event (and thus also his Attributes). The request should be:

```
GET https://your_misp_url/events/123
```


And with the HTTP Headers: `Accept: application/xml` `Authorization: your_api_key`

The response you're going to get is the following data:

```
<pre><?xml version="1.0" encoding="UTF-8" standalone="no"?>
<response>
  <Event>
    <id>57</id>
    <org>NCIRC</org>
    <date>2014-03-04</date>
    <threat_level_id>1</threat_level_id>
    <info>Code monkey doing code monkey stuff</info>
    <published>1</published>
    <uuid>50aa54aa-f7a0-4d74-910d-10f0ff32448e</uuid>
    <attribute_count>1</attribute_count>
    <analysis>1</analysis>
    <timestamp>1393327600</timestamp>
    <distribution>1</distribution>
    <proposal_email_lock>0</proposal_email_lock>
    <orgc>Iglocska</orgc>
    <locked>0</locked>
    <publish_timestamp>1393327600</publish_timestamp>
    <Attribute>
      <id>9577</id>
      <type>other</type>
      <category>Artifacts dropped</category>
      <to_ids>1</to_ids>
      <uuid>50aa54bd-adeb-4544-b494-10f0ff32448e</uuid>
      <event_id>57</event_id>
      <distribution>1</distribution>
      <timestamp>1393327600</timestamp>
      <comment>This is an Attribute</comment>
      <value>Some_attribute</value>
      <ShadowAttribute />
    </Attribute>
    <ShadowAttribute />
    <RelatedEvent />
  </Event>
  <xml_version>2.2.0</xml_version>
</response>
```

Example - Add new Event

In this example we want to add a single Event. The request should be:

```
POST https://your_misp_url/events
Accept: application/xml
Authorization: your_api_key
```

And the request body:

```
<Event>
  <date>2014-03-04</date>
  <threat_level_id>1</threat_level_id>
  <info>Something concise</info>
  <published>1</published>
  <analysis>1</analysis>
  <distribution>1</distribution>
  <Attribute>
    <type>other</type>
    <category>Artifacts dropped</category>
    <to_ids>1</to_ids>
    <distribution>1</distribution>
    <comment>This is an Attribute</comment>
    <value>Some_attribute</value>
  </Attribute>
</Event>
```

The response you're going to get is the following data:

```
HTTP/1.1 100 Continue
HTTP/1.1 200 Continue
Date: Tue, 04-Mar-2014 15:00:00
Server: Apache/2.2.22 (Ubuntu) PHP/5.4.9-4ubuntu2.3
X-Powered-By: PHP/5.4.9-4ubuntu2.3
Set-Cookie: CAKEPHP=deleted; expires=Wed, 05-Mar-2014 15:00:00 GMT; path=/
Set-Cookie: CAKEPHP=a4ok3lr5p9n5drqj27025i4le3; expires Tue, 04-Mar-2014 15:00
Content-Length: 1 kB
Content-Type: application/xml
```

```

<?xml version = "1.0" encoding = "UTF-8"?>
<response>
  <Event>
    <id>76</id>
    <org>NCIRC</org>
    <date>2014-03-04</date>
    <threat_level_id>1</threat_level_id>
    <info>Something concise</info>
    <published>1</published>
    <uuid>50aa54aa-f7a0-4d74-920d-10f0ff32448e</uuid>
    <attribute_count>1</attribute_count>
    <analysis>1</analysis>
    <timestamp>1393328991</timestamp>
    <distribution>1</distribution>
    <proposal_email_lock>0</proposal_email_lock>
    <orgc>Iglocska</orgc>
    <locked>0</locked>
    <publish_timestamp>1393947960</publish_timestamp>
    <Attribute>
      <id>10462</id>
      <type>other</type>
      <category>Artifacts dropped</category>
      <to_ids>1</to_ids>
      <uuid>50aa54bd-adec-4544-b412-10f0ff32448e</uuid>
      <event_id>76</event_id>
      <distribution>1</distribution>
      <timestamp>1393328991</timestamp>
      <comment/>
      <value>Some_attribute</value>
      <ShadowAttribute/>
    </Attribute>
    <ShadowAttribute/>
    <RelatedEvent>
      <id>75</id>
      <org>NCIRC</org>
      <date>2012-11-19</date>
      <info>Code monkey doing code monkey stuff</info>
      <uuid>50aa54aa-f7a0-4d74-910d-10f0ff32448e</uuid>
      <published>1</published>
      <analysis>1</analysis>
      <attribute_count>1</attribute_count>
      <orgc>Iglocska</orgc>
      <timestamp>1393327600</timestamp>
      <distribution>1</distribution>
      <proposal_email_lock>0</proposal_email_lock>
      <locked>0</locked>
      <threat_level_id>1</threat_level_id>
      <publish_timestamp>1393947655</publish_timestamp>
    </RelatedEvent>
  </Event>
  <xml_version>2.2.0</xml_version>
</response>

```

The response from requesting an invalid page

```

<?xml version = "1.0" encoding = "UTF-8"?>
<response>
  <name>Not Found</name>
  <url>/The_meaning_of_life</url>
</response>

```

Last modified: Sun Feb 28 2021 09:22:59 GMT+0100 (Central European Standard Time)

Delegation

In information sharing, privacy of the reporting organisation can be important in such case as:

- an incident doesn't want to be linked to a potential victim.
- to avoid the relation of an organisation with the information shared.

MISP has a functionality to delegate the publication and completely remove the binding between the information shared and its organisation. If you want to publish an event without you or your organisation being tied to it, you can delegate the publication to an other organisation. That also means they will take the ownership of the event. You can only delegate to local target organisations, not any remote organisations.

[warning] You need to have a role with "Delegation access" to delegate an event.

[warning] Also activate MISP.delegation parameter in your instance.

Send a delegation request

To do so, you first need to put the distribution of the event as "your organisation only".

Publish Event	Distribution	Your organisation only
Publish (no email)	Info	Delegate me
Delegate Publishing	Published	No
Contact Reporter	Sightings	0 (0) ↗
Download as...	Activity	
	Correlation	Enabled (disable)

Otherwise the delegation option will not be available.

Publish Event	Distribution	All communities
Publish (no email)	Info	Delegate me
Contact Reporter	Published	No
Download as...	Sightings	0 (0) 
	Activity	
	Correlation	Enabled (disable)

When the "Delegate [Publishing](#)" option is clicked, a pop-up will show up:

Delegate the publishing of the Event to another organisation

Warning: You are about to request another organisation to take ownership of this event.

Target Organisation

Select organisation

Desired Distribution

Recipient decides

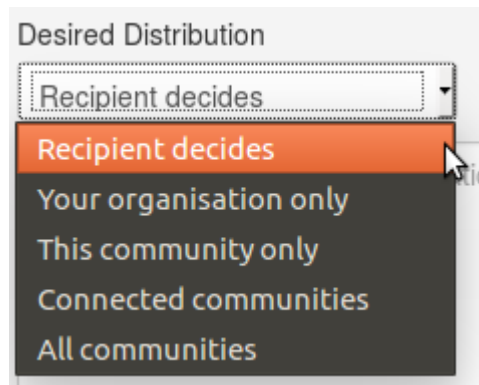
Message to the recipient organisation

Yes

No

Here you can choose

- to which organisation you wish to delegate the event among all those registered on the server. For this example we are going to ask Setec Astronomy to publish the event for us.
- The distribution option you would like to put on the event. You can let the other organisation (called "recipient") choose if you don't mind it. For this example, we will request the recipient to share it to all communities, but it is only a suggestion, and the recipient will be able to modify the diffusion setting if wanted.



- Finally you can leave a free message to the recipient organisation.

Delegate the publishing of the Event to another organisation

Warning: You are about to request another organisation to take ownership of this event.

Target Organisation

Setec Astronomy ▼

Desired Distribution

Recipient decides ▼

Message to the recipient organisation

Yes

No

You can also see more details by clicking on "View request details"

Event Delegation

Request details
Your organisation is requesting **Setec Astronomy** to take over this event.

Message from requester

Discard

Cancel

And you can also discard the request your self, by using this pop-up or the link in the left menu.

Answer a delegation request

As the recipient organisation, you will then receive the request of delegation. You will be notified by a red circle around the envelope on the top right of the screen.



When you click it, you will be redirected as usual on the dashboard, where we can see one delegation request on the left frame.

Dashboard

Notifications

Proposals: **0** ([View](#))

Events with proposals: **0** ([View](#))

Delegation requests: **1** ([View](#))

Changes since last visit

Events updated: **571** ([View](#))

Events published: **571** ([View](#))

[Reset](#)

Clicking on the "view" link then redirect to an event list view showing all the events other organisations wish to delegate to your organisation. Here we only see one event, from Acme Factory.

Events

« previous

next »

Published	Org	Id	Clusters	Tags	#Attr.	#Corr.	#Sightings	#Posts	Date	Threat Level	Analysis	Info	Distribution	Actions
✖	Acme Finance	1096			0				2017-03-23	High	Initial	Delegate me	Organisation	Not published

And here are the metadata of the so called event.

View Event

View Correlation Graph

View Event History

Propose Attribute

Propose Attachment

Accept Delegation Request

Discard Delegation Request

Contact Reporter

Download as...

List Events

Add Event

Delegate me

Event ID	1096
Uuid	58d38964-6be8-4c5b-a338-4920950d210f
Org	Acme Finance
Contributors	
Tags	
Date	2017-03-23
Threat Level	High
Analysis	Initial
Distribution	Your organisation only
Info	Delegate me
Published	No
Sightings	0 (0) ↗
Activity	
Delegation request	Acme Finance has requested that you take over this event. (View request details)
Correlation	Enabled

You will be able to view the details by clicking the so called link.

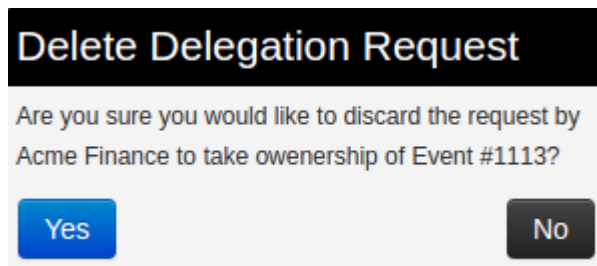
Event Delegation

Request details
Acme Finance is requesting **your organisation** to take over this event.
The desired distribution level is **All communities**

Message from requester
This is a delegation test

If your role have [publishing](#) rights, you will be able to manage the delegation request by using one of the two links in the left menu.

You can either discard it:



Or accept the delegation:

Accept Delegation Request

Are you sure you would like to accept the request by Acme Finance to take ownership of Event #1113?

Please notice that the distribution desired by the requester will not automatically be set on the event, which will stay as distributed to your own organisation only if the parameter is not modified.

Last modified: Sun Feb 28 2021 09:22:59 GMT+0100 (Central European Standard Time)

MISP Extended Events

MISP can now extend an event (starting from version 2.4.90). This allows users to build full blown events that extend an existing event, giving way to a combined event view that includes a sum total of the event along with all extending events.

[More](#)

Last modified: Wed Mar 24 2021 22:22:36 GMT+0100 (Central European Standard Time)

- [Administration](#)
 - [Users](#)
 - [Adding a new user](#)
 - [Listing all users](#)
 - [Contacting a user](#)
 - [Organisations](#)
 - [Adding a new organisation](#)
 - [Listing all organisations](#)
 - [Merge organisations](#)
 - [Roles](#)
 - [Adding a new role](#)
 - [Listing roles](#)
 - [Tools](#)
 - [Server settings and maintenance](#)
 - [Worker types](#)
 - [Workers dead](#)
 - [Blocklists and block rules](#)
 - [Event blocklist](#)
 - [Blocklisting an event](#)
 - [Viewing event blocklist entries](#)
 - [Event block rules](#)
 - [Organisation blocklist](#)
 - [Blocklisting an organisation](#)
 - [Viewing organisation blocklist entries](#)
 - [Import Regexp](#)
 - [The purpose of Import Regexp entries](#)
 - [Adding and modifying entries](#)
 - [Managing the Signature allowedlist](#)
 - [Allowlisting an address](#)
 - [Managing the list](#)
 - [Managing correlation exclusions](#)
 - [Using MISP logs](#)
 - [Browsing logs](#)
 - [Searching Logs](#)
 - [Background Processing](#)
 - [Command Line Tools for the Background Workers](#)
 - [Monitoring the Background Processes](#)
 - [Scheduling Jobs and Recurring Jobs](#)
 - [Various administration tips & tricks](#)
 - [Setting a Publish Alert Filter](#)
 - [Default sharing level](#)
 - [Adding organisation logos](#)
 - [The _schedlr_ worker is not starting](#)
 - [How to redirect HTTP to HTTPS](#)
 - [Increase max size of Samples / other files](#)
 - [Support & feature requests](#)

- More information in the notification emails about new events
- Get top API users
- MISP Logs
- Logging of failed authentication attempts
- Clearing expired sessions
- Troubleshooting MISP not connecting to redis but redis-cli working
- Errors about fields or tables
- Jobs
 - TODO: Explain differences Default, Email, Cache
 - Scheduled Tasks
- MISP Backup
- MISP Restore
- Command line interface (CLI) commands
 - Administering MISP via the CLI
 - Get Setting
 - Set Setting
 - Get Authkey
 - Reset Authkey
 - Set Baseurl
 - Change Password
 - Clear Bruteforce Entries
 - Run Database Update
 - Update All JSON Structures
 - Update Galaxy Definitions
 - Update Taxonomy Definitions
 - Enable all tags of a taxonomy
 - Update Object Templates
 - Update Warninglists
 - Update Noticelists
 - Update MISP
 - Set Default Role
 - Get IPs For User ID
 - Get User ID For User IP
 - Automating certain console tasks
 - PullAll
 - Pull
 - Push
 - Cache Feeds For Quick Lookups
 - Fetch Feeds As Local Data
 - Run Enrichment
 - Test Server
 - List Servers
 - Managing the background workers
 - Get List Of Workers
 - Start A Worker
 - Restart A Worker
 - Restart All Workers
 - Kill A Worker

Administration

- [Users](#)
- [Organisations](#)
- [Roles](#)
- [Tools](#)
- [Server Settings](#)
- [Jobs](#)
- [Scheduled Tasks](#)

[warning] This page is under modification for updating the content. Current status:

- [x] [Users](#) - Reviewed/Updated on: ?
 - [x] [Organisations](#) - Reviewed/Updated on: ?
 - [x] [Roles](#) - Reviewed/Updated on: ?
 - [x] [Tools](#) - Reviewed/Updated on: ?
 - [] [Server Settings](#) - Reviewed/Updated on: ?
 - [] [Jobs](#) aka. Background processing - Reviewed/Updated on: ?
 - [] [Scheduled Tasks](#) aka. Background processing - Reviewed/Updated on: ?
-

Users

As an admin (not to be confused with [Org Admin](#)), you can set up new accounts for users, edit user profiles, delete them, or just have a look at all the viewers' profiles. Organisation admins ([Org Admin](#)) are restricted to executing these actions exclusively within their own organisation's users only.

Adding a new user

To add a new user, click on the Add User button in the administration menu to the left and populate the fields available the loaded view:

Admin Add User

Email

☒ Set password

Password

Confirm Password

Organisation

Role

Authkey

Nids Sid

Sync user for

GPG key

Fetch GPG key

☐ Receive alerts when events are published

☐ Receive alerts from "contact reporter" requests

☐ Disable this user account

Submit

- **Email:** The user's e-mail address, this will be used as his/her login name and as an address to send all automated e-mails as well as e-mails sent by contacting the user as the reporter of an event.
- **Set password:** Tick the box if you want to define a temporary user-password for the user. If you don't, you should use the action button 'reset password' in the 'List Users' view to generate one and send it by email to the user.
- **Password:** *This textbox is displayed only when 'Set password' is ticked.* A Temporary password for the user that he/she should change after the first login. Ensure that password pass the [MISP password policy](#).
- **Confirm Password:** *This textbox is displayed only when 'Set password' is ticked.* This should be an exact copy of the Password field.
- **Organisation:** A drop-down list enables you to choose an organisation for the user. To learn more about organisation, [click here](#).
- **Roles:** A drop-down list allows you to select a role-group that the user should belong to. [Roles](#) define user privileges attributed to the user. To learn more about [roles](#), [click here](#).
- **Authkey:** This is assigned automatically and is the unique authentication key of said user (he/she will be able to reset this and receive a new key). It is used for exports and for connecting one server to another, but it requires the user to be assigned to a role that has auth permission enabled.
- **NIDS SID:** Network Intrusion Detection System ([NIDS](#)) Signature ID (SID). Snort rules exported by the created user will have the offset defined in the user profile and each rule generated during the export will receive an incrementing SID starting with the user's offset. If no SID offset is specified a default, randomized value will be set.
- **Sync user for:** Use this option for granting the user the right to synchronize the event between MISP server. This option is available for admin, [Org Admin](#) and [Sync user](#) role.
- **Gpgkey:** The key used to encrypt e-mails sent through the system.
- **Fetch GnuPG key:** Fetch GnuPG public key.
- **Receive alerts when events are published:** This option will subscribe the new user to automatically generated e-mails whenever an event is published.
- **Receive alerts from "contact reporter" requests:** This option will subscribe the new user to e-mails that are generated when another user tries to get in touch with an event's reporting organisation that matches that of the new user.
- **Disable this user account:** Tick it if you want to disable this user account. (preferred to removing an account)

Listing all users

To list all current users of the system, just click on List Users under the administration menu to the left. A view will load containing a list of all users and the following columns of information:

Users

- previous

next ->

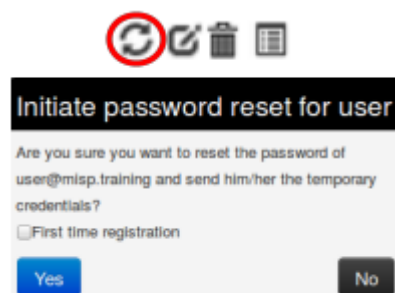
												Filter
id	Org	Role	Email	Authkey	Autoalert	Contactalert	Gpgkey	Nids Sid	Termsaccepted	Last login	Disabled	Actions
3	CIRCL	Publisher	operator@circl.lu	1e8MCDoskGdLX0qTIPsBCYWS6j40xmP9rTj	No	No	No	123456	Yes	N/A	No	  
1	MISP	admin	admin@misp.training	JNqWBxtPjlywz7hUe58MyJf6sD5PYTVaCm7hTn6c	No	No	No	4000000	Yes	2016-08-04	No	  
2	MISP	Publisher	user@misp.training	h6SWqj0N3B5SMPjy0NWEk27XTRMzEVTz1P0c0N	No	No	No	1000001	Yes	2016-08-04	No	  

Page 1 of 1, showing 3 records out of 3 total, starting on record 1, ending on 3

- previous

next ->

- **Id:** The user's automatically assigned ID number.
- **Org:** The organisation that the user belongs to.
- **Email:** The e-mail address (and login name) of the user.
- **Authkey:** Unique authentication key of the user.
- **Autoalert:** Shows whether the user has subscribed to auto-alerts and is continuing to receive mass-emails regarding newly published events that he/she is eligible for.
- **Contactalert:** Shows whether the user has the subscription to contact reporter e-mails directed at his/her organisation is turned on or off.
- **Gpgkey:** Shows whether the user has entered a GnuPG key yet.
- **Nids Sid:** Displays the currently assigned **NIDS** ID.
- **Termsaccepted:** This flag indicates whether the user has accepted the terms of use or not.
- **Last login:** Date of last login.
- **Disabled:** Displays the user status. Enabled or disabled.
- **Action Buttons:** There are 4 options available: reset the password, edit the user, delete the user or display a user's information. These options are also available on the left menu.
 - **Reset Password:** Use this action to reset a password. If you've created a new user without A password, tick the 'First time registration' checkbox to send a welcome message. Otherwise a reset password message will be sent.



- **Edit the user:** Same options of create user's view. Only a few options are available here:
 - **Terms accepted:** Indicates whether the user has accepted the terms of use already or not.
 - **Change Password:** Setting this flag will require the user to change password after the next login.
 - **Reset Auth Key:** Use this link for generate a new AuthKey.



Admin Edit User

Email

user@mlip.training

☐ Set password

Organisation

MISP

Role

Publisher

Authentication key

lek5WqbKN3i655MPgXNWEk27>

Nids Sid

1000001

GPG key

Fetch GPG key

☒ Terms accepted

☐ Change Password

☐ Receive alerts when events are published

☐ Receive alerts from "contact reporter" [Reset Auth Key](#)

☐ Disable this user account

Submit

- **Delete the user:** If you want to delete a user. (Note: disabling is the preferred method)



Are you sure you want to delete # 5? It is highly recommended to never delete users but to disable them instead.

Cancel

OK

- **Display the user:** Display all user's information.



User

Id	2
Org	MISP
Role	Publisher
Email	user@misp.training
Autoalert	No
Contactalert	No
Authkey	EwdHQwWtljGbL4GdjmY2NkQhe2FszjZM1QDX51 (reset)
Invited By	admin@misp.training
PGP key	N/A
Nids Sid	1000001
Termsaccepted	Yes
Password change	No
Newsread	2016/08/04 10:18:39
Disabled	No

Related Events

Contacting a user

Site admins can use the "Contact users" feature to send all or individual user an e-mail. Users that have a GnuPG key set will receive their e-mails encrypted. When clicking this button on the left, you'll be presented with a form that allows you to specify the type of the e-mail, who it should reach and what the content is using the following options:

Contact User(s)

Messaging - here's a quick guide on how this feature works

You can use this view to send messages to your current or future users or send them a temporary password.

- When adding a new user to the system, or when you want to manually reset the password for a user, just use the "Send temporary password" setting.
- After selecting the action, choose who the target of the e-mails should be (all users, a single user or a user not yet in the system).
- You can then specify (if eligible) what the e-mail address of the target is (for existing users you can choose from a dropdown menu).
- In the case of a new user, you can specify the future user's gpg key, to send his/her new key in an encrypted e-mail.
- The system will automatically generate a message for you, but it is also possible to write a custom message if you tick the check-box, but don't worry about assigning a temporary password manually, the system will do that for you, right after your custom message.

Action	Subject
Custom message ▾	<input type="text"/>
Recipient	Recipient Email
A single user ▾	admin@misp.training ▾
<input type="checkbox"/> Enter a custom message	
Message	
<div></div>	
<input type="button" value="Submit"/>	

- **Action:** This defines the e-mail type, which can be a custom message or a password reset. Password resets automatically include a new temporary password at the bottom of the message and will automatically change the user's password accordingly.
- **Subject:** In the case of a custom e-mail, you can enter a subject line here.
- **Recipient:** The recipient toggle lets you contact all your users, a single user (which creates a second drop-down list with all the e-mail addresses of the users) and potential future users (which opens up a text field for the e-mail address and a text area field for a GnuPG public key).
- **Custom message checkbox:** This is available for password resets and for welcome messages. You can either write your own message (which will be appended with a temporary key and the signature), or let the system generate one automatically.

Keep in mind that all e-mails sent through this system, in addition to your own message, will be signed in the name of the instance's host organisation's support team, the e-mail will also include the e-mail address of the instance's support (if the contact field is set in the bootstrap file), and will include the instance's GnuPG signature for users that have a GnuPG key set (and thus are eligible for an encrypted e-mail).



GnuPG instance key is the GnuPG key used by the [MISP instance](#) and which is only used to sign notification. The GnuPG key used in the [MISP instance](#) must not be used anywhere else and should not be valuable.

Organisations

Each users belongs to an organisation. As admin, you can manage these organisations.

Adding a new organisation

To add a new organisation, click on the "Add Organisation" button in the administration menu to the left and fill out the following fields in the view that is loaded:

New 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.

☒ Local organisation

Mandatory fields.

Organisation Identifier

Brief organisation identifier

No image uploaded for this identifier

Uuid

Paste UUID or click generate

Generate UUID

A brief description of the organisation

A description of the organisation that is purely informational.

The following fields are all optional.

Nationality

Not specified

Sector

For example "financial".

Type of organisation

Freetext description of the org.

Contacts

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

Submit

- **Local organisation:** If the organisation should have access to this instance, tick the checkbox. If you would only like to add a known external organisation for inclusion in [sharing groups](#), uncheck it.
- **Organisation Identifier:** Name your organisation. If you want to add a picture, you should add a file on the webserver using the 'Server Settings menu'. Picture should have the same name. To learn more about server settings menu, [click here](#).
- **Uuid:** Unique identifier. If you want to share organisation between MISP multi-instance, use the same Uuid.
- **A brief description of the organisation:** A word for describing the organisation.
- **Nationality:** A drop-down list for selecting the country of organisation.
- **Sector:** Define the sector of organisation (financial, transport, telecom...)
- **Type of organisation:** Define the type of the organisation.
- **Contacts:** You can add some contact details for the organisation.

Listing all organisations

To list all current organisations of the system, just click on List Organisations under the administration menu to the left. There are 3 tabs in this view to filter local organisations, remote organisations or both. The default view displays local organisations. For all views the following columns of information are available:

Local organisations having a presence on this instance

« previous next »

Local organisations										
Known remote organisations										
All organisations										
Filter										
Id	Logo	Name	Uuid	Description	Nationality	Sector	Type	Contacts	Added by	Local
1		MISP	56e13277-1ad4-42f5-b90b-04e5c0a33832	Host organisation for the training instance	International				Unknown	Yes
2		CRCL	55f6e5e-2cb0-40e5-964f-47a8950d210f		Not specified				admin@misp.training	Yes

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

« previous next »

- **Id:** The organisation's automatically assigned ID number.
- **Logo:** Picture of the organisation.
- **Name:** Name of the organisation.
- **Uuid:** Unique identifier of organisation. Share this Uuid when using it between MISP's multi-instance.
- **Description:** Description of the organisation.
- **Nationality:** Country of the organisation.
- **Sector:** Sector defined for the organisation.
- **Type:** Type of organisation.
- **Contacts:** Contacts of organisation.
- **Added by:** Login of the user who added the organisation
- **Local:** Flag defined if the organisation is local or remote.
- **Users:** The amount of users on this instance belonging to the organisation.
- **Actions:** There are 3 options available: edit, delete or display an organisation's information. These options are also available on the left menu when you are on the display view.
 - **Edit Organisation:** Same options of create organisation's view.

Edit 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.

☒ Local organisation

Mandatory fields. Leave the UUID field empty if the organisation doesn't have a UUID from another instance.

Organisation Identifier

CIRCL



Uuid

55f8ea5e-2c60-40e5-964f-47a8950d210f

Generate UUID

A brief description of the organisation

A description of the organisation that is purely informational.

The following fields are all optional.

Nationality

Not specified



Sector

For example "financial".

Type of organisation

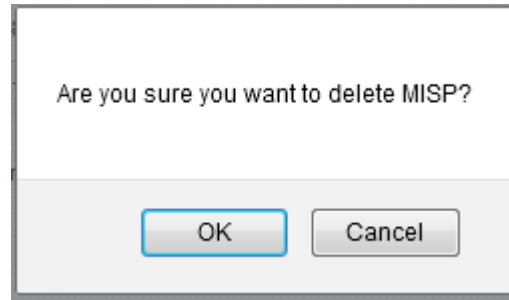
Freetext description of the org.

Contacts

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

Submit

- **Delete Organisation:** Use this option for deleting organisation.



- **View Organisation:** Use this option to display information about the selected organisation. In this view, you can display the user belongs to this organisation and events published by organisation.

Organisation CIRCL

Id	2
Organisation name	CIRCL
Local or remote	Local
Description	
Uuid	55f8ea5e-2c00-40a5-964f-47a8950d210f
Created by	admin@map.training
Nationality	Not specified

Description Members Events

→ → →

Landing page for CIRCL

No landing page has been created for this organisation.

Members of CIRCL

< previous next >

Id	Email	Role	GPGKey
3	operator@circl.lu	Publisher	No

Page 1 of 1, showing 1 records out of 1 total, starting on record 1, 0

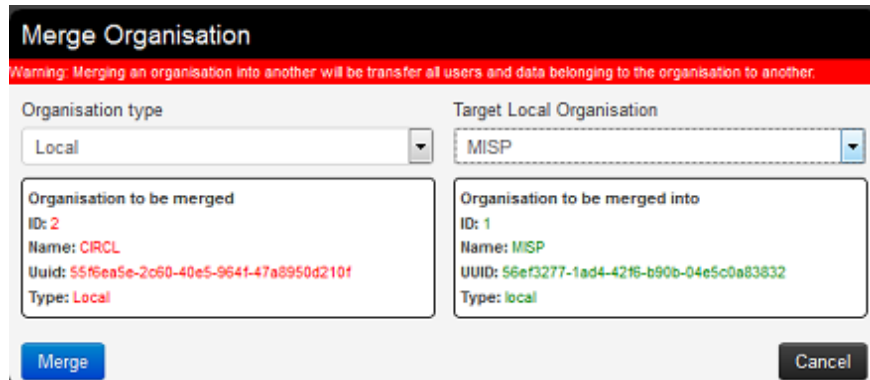
Events

< previous 1 2 3 next >

Published	Org	Owner Org	Id	Tags
✓	✖	WSP	95	Type:OSINT Ip:white CircleanContent: classification:"malware"
✓	✖	WSP	56	Type:OSINT Ip:white

Merge organisations

Merge Organisation menu is available only in the organisation view, under the left menu. Merging one organisation into another will transfer all users and data from one organisation to a different one. The organisation of which the users and data will be transferred is displayed on the left, the target organisation is displayed on the right.



The screenshot shows a 'Merge Organisation' dialog box. At the top, a red warning banner reads: 'Warning: Merging an organisation into another will be transfer all users and data belonging to the organisation to another.' Below the banner, there are two main sections. The left section is titled 'Organisation type' with a dropdown menu set to 'Local'. Below this is a box labeled 'Organisation to be merged' containing the following details: ID: 2, Name: CIRCL, Uuid: 55f6ea5e-2c60-40e5-964f-47a8950d210f, and Type: Local. The right section is titled 'Target Local Organisation' with a dropdown menu set to 'MISP'. Below this is a box labeled 'Organisation to be merged into' containing the following details: ID: 1, Name: MISP, UUID: 56ef3277-1ad4-42f6-b90b-04e5c0a83832, and Type: local. At the bottom of the dialog, there are two buttons: 'Merge' and 'Cancel'.

Organisation to be merged	Organisation to be merged into
ID: 2	ID: 1
Name: CIRCL	Name: MISP
Uuid: 55f6ea5e-2c60-40e5-964f-47a8950d210f	UUID: 56ef3277-1ad4-42f6-b90b-04e5c0a83832
Type: Local	Type: local

Roles

Privileges are assigned to users by assigning them to rule groups. Rule groups use one of four options determining what they can do with events as well as four additional privilege elevation settings. These are the four options to edit the full options available in the [Roles](#) section: Read Only, Manage My Own Events, Manage Organisation Events, Manage & Publish Organisation Events. A short description is provided below:

- **Read Only:** Allows a user to browse events that his organisation has access to, but doesn't allow any changes to be made to the database.
- **Manage My Own Events:** Allows users to create, modify or delete their own events, but they cannot publish them.
- **Manage Organization Events:** Allows users to create events or modify and delete events created by a member of their organisation.
- **Manage & Publish Organisation Events:** Gives users the right to do all of the above and to publish the events of their organisation.

The extra permissions are defined below:

- **Perm Admin:** Gives the user limited administrator privileges, this setting is used for an organisation's admins.
- **Perm Audit:** Grants access to the logs. With the exception of site admins, only logs generated by the user's own org are visible.
- **Perm Tagger:** Allows a user to assign tags to events.
- **Perm Sharing Group:** Grant access to edit or create [sharing groups](#).
- **Perm Site Admin:** Gives the user full administrator privileges, this setting is used for site admins.
- **Perm Auth:** This setting enables the authentication key of the role's users to be used for rest requests.
- **Perm Tag Editor:** Grants access to edit or create tags.
- **Perm Delegate:** Grant access to delegate the publication of an event to a third-party organization.
- **Perm Sync:** This setting enables the users of the role to be used as a [synchronisation](#) user. The authentication key of this user can be handed out to the administrator of a remote [MISP instance](#) to allow the [synchronisation](#) features to work.
- **Perm Regexp Access:** Allows users who have this permission enabled to edit the regular expression table. Be careful when giving out this permission, incorrect regular expressions can be very harmful (infinite loops, loss of data, etc.).
- **Perm Template:** Grant access to create or modify templates.

Adding a new role

When creating a new role, you will have to enter a name for the role to be created and set up permissions (as described above) using the drop-down menu and related check-boxes.

Add Role

Name	Permission	
<input type="text"/>	<input type="text" value="Read Only"/> ▼	
<input type="checkbox"/> Perm Admin	<input type="checkbox"/> Perm Site Admin	<input type="checkbox"/> Perm Sync
<input type="checkbox"/> Perm Audit	<input type="checkbox"/> Perm Auth	<input type="checkbox"/> Perm Regexp Access
<input type="checkbox"/> Perm Tagger	<input type="checkbox"/> Perm Tag Editor	<input type="checkbox"/> Perm Template
<input type="checkbox"/> Perm Sharing Group	<input type="checkbox"/> Perm Delegate	
<input type="button" value="Add"/>		















Listing roles

By clicking on the List [Roles](#) button, you can view a list of all currently registered [roles](#) and their enabled permissions. In addition, you can find buttons that allow you to edit and delete said [roles](#). Keep in mind that you will need to first remove every member from a role before you can delete it.

Roles

< previous

next >

Id	Name	Permission	Admin	Site Admin	Sync Actions	Audit Actions	Auth key access	Regex Actions	Tagger	Tag Editor	Template Editor	Sharing Group Editor	Delegations access	Actions
6	Automation user	Manage & Publish Organization Events					✓						✓	 
2	Org Admin	Manage & Publish Organization Events	✓		✓	✓	✓		✓	✓	✓	✓	✓	 
4	Publisher	Manage & Publish Organization Events											✓	 
7	Read Only	Read Only												 
5	Sync user	Manage & Publish Organization Events			✓		✓					✓	✓	 
3	User	Manage Organization Events												 
1	admin	Manage & Publish Organization Events	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	 

Page 1 of 1, showing 7 records out of 7 total, starting on record 1, ending on 7

< previous

next >

- **Id:** The role's automatically assigned ID number.
- **Name:** The name of role.
- **Permission:** One of the 4 permissions: Read Only, Manage My Own Events, Manage Organization Events, Manage & Publish Organisation Events.
- **Extra Permissions flag:** Flag for each extra permissions: Admin, [Site Admin](#), Sync Actions, Audit Actions, Auth key access, Regex Actions, Tagger, Tag Editor, Template Editor, Sharing Group Editor, Delegations Access.
- **Action Buttons:** There are 2 options available: Edit Role or Delete it.
 - **Edit Role:** Same options of create role's view.

Edit Role

Name
Automation user

Permissions
Manage & Publish Organizal

☐ Perm Admin
☐ Perm Audit
☐ Perm Tagger
☐ Perm Sharing Group

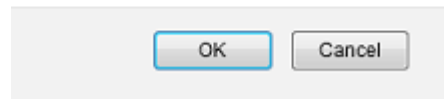
☐ Perm Site Admin
☒ Perm Auth
☐ Perm Tag Editor
☒ Perm Delegate

☐ Perm Sync
☐ Perm Regexp Access
☐ Perm Template

Edit

- o **Delete Role:** Use this option to delete a role.

Are you sure you want to delete Read Only?



Tools

MISP has a couple of administrative tools that help administrators keep their instance up to date and healthy. The list of these small tools can change rapidly with each new version, but they should be self-explanatory. Be sure to check this section after each upgrade to a new version, just in case there's a new upgrade script in there - though if this is the case it will be mentioned in the upgrade instructions.

Administrative actions

- [reportValidationIssuesEvents](#)
- [reportValidationIssuesAttributes](#)
- [Reset the attribute counts](#) (Events need to have no validation issues)
- [Reconcile attributes](#)
- [Reconcile proposals](#)
- [Verify GPG keys](#) (Check whether every user's GPG key is usable)
- [Verify Certificates](#) (Check whether every user's certificate is usable)
- [Extend Organization length](#) (Hotfix 2.3.57: Increase the max length of the organization field when adding a new server connection.)
- [Convert log fields to text](#) (Hotfix 2.3.78: Some of the log fields that were varchar(255) ended up truncating the data. This function will change them to "text")
- [Fix duplicate UUIDs](#) (Hotfix 2.3.107: It was previously possible to get duplicate attribute UUIDs in the database, this script will remove all duplicates and ensure that duplicates will not be entered into the database in the future.)
- [Remove duplicate events \(with the same UUID\)](#) (Hotfix 2.3.115: In some rare situations it could occur that a duplicate of an event was created on an instance, with the exact same uuid. This action will remove any such duplicates and make sure that this cannot happen again.)
- [Prune orphaned attributes](#) (In some rare occasions it can happen that you end up with some attributes in your database that do not belong to an event - for example during a race condition between an event insert and a delete. This tool will collect and delete any such orphaned attributes. If you ever run into an issue where you cannot add an attribute with a specific valid value, this is probably the reason.)
- [Clean regex table of potentially malicious entries](#) (Hotfix 2.3.160: Prior to this version it was possible for a user/admin with Regex permission to create a malicious regular expression that could be used to execute arbitrary code. Since this version it is no longer possible to input such expressions, but already existing malicious entries still have to be cleaned using this tool.)
- [Remove url type attribute sanitisation](#) (Hotfix 2.3.173: Sanitised URLs can cause issues with the NIDS exports and as of this version attributes will be modified on entry to correct this. To correct existing entries, run this script.)
- [Index tables](#) (This script will create indexes for all of the tables in MISP (other than primary keys))
- [Fix non-empty sharing group IDs](#) (This script will change the sharing_group_id to 0 in all non sharing group setting events and attributes)

Upgrading a 2.3 instance to 2.4

Warning: Running the scripts below can result in the loss of data. Make sure that you back your database up before running them

The order for the 2.4 upgrade procedure is:

1. Upgrade to 2.4 - run this to migrate the 2.3 data to the 2.4 format
2. If it completes successfully, run the 2.3->2.4 [cleanup](#) script to remove the fields that are specific to 2.3. Make sure that the migration of the data to the 2.4 format was successful (you can check the result in the audit logs). If you have run the 2.4 upgrade script previously but are running into SQL errors on the column 'org', run this script.

Server settings and maintenance

Since version 2.3, MISP has a settings and diagnostics tool that allows site-admins to manage and diagnose their MISP installation. You can access this by navigating to Administration - Server settings & Maintenance.

Server settings

OverviewMISP settings (6)OnuPO settingsSecurity settingsMisc settings (1)

Settings tabs

Non-critical issues

Critical errors

Diagnostics tab

Workers tab

Download report


DiagnosticsWorkers (4)

Test	Value	Description
Overall health	Critical, your MISP instance requires immediate attention.	The overall health of your instance depends on the most severe unresolved issues.
Critical settings incorrectly or not set	1 incorrect settings.	MISP will not operate correctly or will be unsecure until these issues are resolved.
Recommended settings incorrectly or not set	0 incorrect settings.	Some of the features of MISP cannot be utilised until these issues are resolved.
Optional settings incorrectly or not set	6 incorrect settings.	There are some optional tweaks that could be done to improve the looks of your MISP instance.
Critical issues revealed by the diagnostics	0 issues detected.	Issues revealed here can be due to incorrect directory permissions or not correctly installed dependencies.

The settings and diagnostics tool is split up into several aspects, all accessible via the tabs on top of the tool. For any unset or incorrectly set setting, or failed diagnostic a number next to the tab name will indicate the number and severity of the issues. If the number is written with a red font, it means that the issue is critical. First, let's look at the various tabs:

- **Overview:** General overview of the current state of your MISP installation
- **MISP settings:** Basic MISP settings. This includes the way MISP handles the default settings for distribution settings, whether background jobs are enabled, etc
- **GnuPG settings:** GnuPG related settings.
- **Proxy settings:** HTTP proxy related settings.
- **Security settings:** Settings controlling brute-force protection and the application's salt key.
- **Misc settings:** Settings controlling debug options, please ensure that debug is always disabled on a production system.
- **Diagnostics:** The diagnostics tool checks if all directories that MISP uses to store data are writeable by the apache user. Also, the tool checks whether the STIX libraries and GnuPG are working as intended.
- **Workers:** Shows the background workers (if enabled) and shows a warning if they are not running. Admins can also restart the workers here.
- **Download report:** Download a report of all the settings visible in the tool, in JSON format.

Server settings

Overview		MISP settings (7)		GnuPG settings		Security settings		Misc settings (1)		Diagnostics		Workers (4)			
Priority	Setting	Value		Description		Error Message									
Critical	MISP baseurl	http://192.168.56.12		The base url of the application (in the format https://www.mymispinstance.com). Several features depend on this setting being correctly set to function.		The currently set baseurl does not match the URL through which you have accessed the page. Changed this if you are accessing the page via an alternate URL (for example via IP address).									
Critical	MISP showorg	true		Setting this setting to 'false' will hide all organisation names / logos.											
Critical	MISP email	andreas.blody@gmail.com		The e-mail address that MISP should use for all notifications											
Critical	MISP default_event_distribution	Connected communities		The default distribution setting for events (0-3).											

Each of the setting pages is a table with each row representing a setting. Coloured rows indicate that the setting is incorrect / not set and the colour determines the severity (red = critical, yellow = recommended, green = optional). The columns are as follows:

- **Priority:** The severity of the setting.
- **Setting:** The setting name.
- **Value:** The current value of the setting.
- **Description:** A description of what the setting does.
- **Error Message:** If the setting is incorrect / not set, this field will let the user know what is wrong.

Server settings

Overview			MISP settings (7)	OnuPG settings	Security settings	Misc settings (1)	Diagnostics	Workers (1)	⚙
Worker Type	Worker Id	Status							
cache	iglooska-VirtualBox:9340:cache	OK							
default	iglooska-VirtualBox:9311:default	OK							
email	iglooska-VirtualBox:9380:email	OK							
schedlr	N/A	Worker not running!							

[Restart all workers](#)
 This will start / restart all of the workers and refresh the page. Keep in mind, this process can take a few seconds to complete, so refresh the page again in 5-10 seconds to see the correct results.

The workers tab shows a list of the workers that MISP can use. You can restart workers using the "restart all workers" button. If the button doesn't work, make sure that the workers were started using the apache user. This can however only be done using the command line, refer to the INSTALL.txt documentation on how to let the workers automatically start on each boot.

- **Worker Type:** The worker type is determined by the queue it monitors. MISP currently has 6 queues (cache, default, prio, email, update and a special *schdlr* queue).
- **Worker Id:** The ID is made up of the machine name, the PID of the worker and the queue it monitors.
- **Status:** Displays OK if the worker is running. If the *schdlr* worker is the only one not running, make sure that you copy the config file into the cakeresque directory as described in the INSTALL.txt documentation.

Worker types

cache

Role: Interdependence:

default

Role: Interdependence:

email

Role: Interdependence:

update

Role: Interdependence:

prio

Role: Interdependence:

scheduler

Role: Interdependence:

Workers dead

Even if the workers are dead, any actions related to them are on-hold. Nothing is lost. Simply restarting the worker will resume any operations.

You can either relaunch them via the UI or manually by running **sudo -u www-data bash /var/www/MISP/app/Console/worker/start.sh** on the CLI. For reference, below is the script in question.

```
#!/usr/bin/env bash

# Check if run as root
if [ "$EUID" -eq 0 ]; then
    echo "Please DO NOT run the worker script as root"
    exit 1
fi

# Extract base directory where this script is and cd into it
cd "${0%/*}"

../cake CakeResque.CakeResque stop --all
../cake CakeResque.CakeResque start --interval 5 --queue default
../cake CakeResque.CakeResque start --interval 5 --queue prio
../cake CakeResque.CakeResque start --interval 5 --queue cache
../cake CakeResque.CakeResque start --interval 5 --queue email
../cake CakeResque.CakeResque startscheduler --interval 5

exit 0
```

Blocklists and block rules

It is possible to block certain events or organisations from ever being added to the system. Administrators can add, edit or delete blocklisted items. The appropriate pages are linked in the Administration menu.

Event blocklist

Blocklisting an event prevents the event from being added on the instance. Blocklisting an existing event will not result in the event being removed. The event will still be editable as well. Blocklisting events functionality is enabled by default. If blocklisting events is enabled, deleted events will automatically be added to the event blocklist. Enabling/disabling event blocklisting can be done using the MISP settings view.

Server Settings & Maintenance

Overview MISP settings (11) Encryption settings (4) Proxy settings (5) Security settings Plugin settings (57) ⚠ Diagnostics Manage files Workers			
Priority	Setting	Value	Description
Recommended	MISP.enableEventBlocklisting	true	Since version 2.3.107 you can start blocklisting event UUIDs to prevent them from being pushed to your instance. This functionality is available in the MISP interface.
Recommended	MISP.enableOrgBlocklisting	true	Blocklisting organisation UUIDs to prevent the creation of any event created by the blocklisted organisation.

Blocklisting an event

The blocklist event screen can be accessed through the main administration menu. You can enter the UUID of one event or a list of event UUIDs (one per line). If the optional fields creating organisation, event info or comment are filled in, their values will be added for all added UUIDs.

Add Event Blocklist Entries

Simply paste a list of all the event UUIDs that you wish to block from being entered.

UUIDs

Enter a single or a list of UUIDs

Creating organisation

(Optional) The organisation that the event is associated with

Event info

(Optional) the event info of the event that you would like to block. It's best to leave this empty if you are adding a list of UUIDs.

Comment

(Optional) Any comments you would like to add regarding this (or these) entries.

Add





Viewing event blocklist entries

The list of blocklisted events can be accessed through the main administration menu. You can delete a blocklist entry or access the edit screens for specific blocklisted events from here.

Event Blocklists

« previous

next »

<div>Enter value to search</div> <div>Filter</div>						
<input type="checkbox"/>	Id	Org	Event UUID	Created ↑	Event Info	Actions
<input type="checkbox"/>	15		b20260b0-40a2-47e5-8683-e9648869171d	2021-02-26 00:46:54		 
<input type="checkbox"/>	14	Setec Astronomy	7e95dc98-7ce7-4b01-8d42-4e9169456c17	2021-02-25 23:55:09	Org blocklist test sync	Automatically blocked by deleting event  

Event block rules

Event block rules allow you to add a simple tag filter to block events from being added or synced.

An example of a rule can be found below:

```
{
  "tags": ["tag1", "tag2"]
}
```

The rule will block:

- Syncing of events with "tag1" or "tag2"
- Direct adding of events with "tag1" or "tag2" in one go, for example using `/events/add`

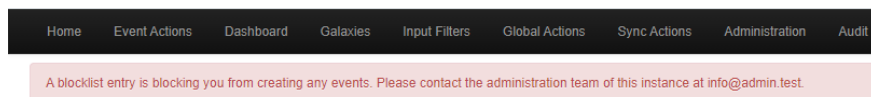
The rule will not block:

- The adding of "tag1" or "tag2" to an existing event through non syncing actions, for example by adding it via the graphical user interface.

It is not possible to add more complex rules with boolean logic (NOT, AND).

Organisation blocklist

Blocklisting an organisation prevents the creation of any event by the blocklisted organisation. It does not prevent a local user from the blocklisted organisation from logging in or viewing data.



When syncing, events created by blocklisted organisations will not be added to the instance. Updates will also not propagate. A user from a blocklisted organisation can still edit an event from the blocklisted organisation locally though. Blocklisting organisations functionality is enabled by default. Enabling/disabling organisation blocklisting can be done using the MISP settings view.

Server Settings & Maintenance

Overview MISP settings (11) Encryption settings (4) Proxy settings (5) Security settings Plugin settings (57) Diagnostics Manage files Workers			
Priority	Setting	Value	Description
Recommended	MISP.enableEventBlocklisting	true	Since version 2.3.107 you can start blocklisting event UUIDs to prevent them from being pushed to your instance. This functionality is available in another instance.
Recommended	MISP.enableOrgBlocklisting	true	Blocklisting organisation UUIDs to prevent the creation of any event created by the blocklisted organisation.

Blocklisting an organisation

The blocklist organisation screen can be accessed through the main administration menu. You can enter the UUID of one organisation or a list of organisations UUIDs (one per line). If the optional fields organisation name or comment are filled in, their values will be added for all added UUIDs.

Add Organisation Blocklist Entries

Simply paste a list of all the organisation UUIDs that you wish to block from being entered.

UUIDs

58d38339-7b24-4386-b4b4-4c0f950d210f

Organisation name

Setec Astronomy

Comment

(Optional) Any comments you would like to add regarding this (or these) entries.

Add



Viewing organisation blocklist entries

The list of blocklisted organisations can be accessed through the main administration menu. You can delete a blocklist entry or access the edit screens for specific blocklisted organisations from here.

Organisation Blocklists

« previous

next »

Id				Organisation name	UUID	Created ↑	Comment	Actions
1				Setec Astronomy	58d38339-7b24-4386-b4b4-4c0f950d210f	2021-02-25 23:12:16		 

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

« previous

next »

Import Regexp

The system allows administrators to set up rules for regular expressions that will automatically alter newly entered or imported events (from GFI Sandbox).

The purpose of Import Regexp entries

They can be used for several things, such as unifying the capitalisation of file paths for more accurate event correlation or to automatically censor the usernames and use system path variable names (changing C:\Users\UserName\AppData\Roaming\file.exe to %APPDATA%\file.exe). The second use is blocking, if a regular expression is entered with a blank replacement, any event info or attribute value containing the expression will not be added. Please make sure the entered regexp expression follows the preg_replace pattern rules as described [here](#)

Adding and modifying entries

Administrators can add, edit or delete regular expression rules, these "expressions" are made up of a regex pattern that the system searches for and a replacement for the detected pattern.

Id	Regexp	Replacement	Type
1	/..ProgramData./i	%ALLUSERSPROFILE%\	ALL
2	/..Documents and Settings.All Users./i	%ALLUSERSPROFILE%\	ALL
3	/..Program Files.Common Files./i	%COMMONPROGRAMFILES%\	ALL
4	/..Program Files (x86).Common Files./i	%COMMONPROGRAMFILES(x86)%\	ALL
5	/..Users.(\\w+).AppData.Local.Temp./i	%TEMP%\	ALL
6	/..ProgramData./i	%PROGRAMDATA%\	ALL
7	/..Program Files./i	%PROGRAMFILES%\	ALL

Managing the Signature allowedlist

The signature allowedlist view, accessible through the administration menu on the left, allows administrators to create and maintain a list of addresses that are allowlisted from ever being added to the [NIDS](#) signatures. Addresses listed here will be commented out when exporting the [NIDS](#) list.

Allowlisting an address

While in the allowedlist view, click on New Allowedlist on the left to bring up the "add allowedlist" view to add a new address.

Managing the list

When viewing the list of allowlisted addresses, the following data is shown: The ID of the allowlist entry (assigned automatically when a new address is added), the address itself that is being allowlisted and a set of controls allowing you to delete the entry or edit the address.

Signature Allowedlist

Regex entries (in the standard php regex /(regex)/(modifier) format) entered below will restrict matching attributes from being included in the IDS flag sensitive exports (such as NIDS exports).

< previous

next >

id	Name ↓	Actions
1	/www.futuremark.com/	<div><div></div><div></div></div>

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

< previous

next >

Managing correlation exclusions

Correlation exclusions allow you to exclude certain values from the correlation engine. Values can be 1:1 matches or substring searches denoted with a leading or ending '%', or both.

Examples:

- <https://www.google.com/> will match anything starting with <https://www.google.com/>
- %google.com% will match anything that contains google.com

After adding an exclusion, new values coming in will not correlate if they match any of the correlation exclusions. To remove existing correlations run the cleaner tool (see 'Clean up correlations' button in screenshot below).

Correlation Exclusions Index

A list of values to exclude from the correlation engine.

« previous

next »

Add correlation exclusion only

Clean up correlations

Enter value to search

Filter

#	Value	JSON source	Actions
1	%google.com%	x	
2	%exclude test	x	
3	https://correlationexclude test	x	

Page 1 of 1, showing 3 records out of 3 total, starting on record 1, ending on 3

« previous

next »

Note: the JSON source field is not used yet

Using MISP logs

Users with audit permissions are able to browse or search logs that MISP automatically appends each time certain actions are taken (actions that modify data or if a user logs in and out). Generally, the following actions are logged:

- **User:** Creation, deletion, modification, Login / Logout
- **Event:** Creation, deletion, modification, [publishing](#)
- **Attribute:** Creation, deletion, modification
- **ShadowAttribute:** Creation, deletion, Accept, Discard
- **Roles:** Creation, deletion, modification
- **Blocklist:** Creation, deletion, modification
- **Allowlist:** Creation, deletion, modification
- **Regexp:** Creation, deletion, modification

Browsing logs

Listing all the log entries will display the following columns generated by the users of your organisation (or all organisations in the case of site admins):

Logs

« previous		32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	next »
Id #	Email	Org	Created	Action	Title	Change																	
1936	admin@admin.test	ADMIN	2013-05-28 10:34:57	add	Attribute (44) from Event (1): Payload installation/md5 7388cd7561cd9a7989202ad4d37eff24f	event_id () => (1), uuid () => (d525d2c9-																	
1935	admin@admin.test	ADMIN	2013-05-28 10:34:57	add	Attribute (43) from Event (1): Payload installation/md5 6f0ec8623951e8b128cd7a07b2031ee6	event_id () => (1), uuid () => (f044476b-c																	
1934	admin@admin.test	ADMIN	2013-05-28 10:34:57	add	Attribute (42) from Event (1): Payload installation/md5 6d2320af561b2315c1241e3ef08067f	event_id () => (1), uuid () => (5023d0c6-																	
1933	admin@admin.test	ADMIN	2013-05-28 10:34:57	add	Attribute (41) from Event (1): Payload installation/md5 68c67a6e26855ebc2599d57699c69a6e	event_id () => (1), uuid () => (aef94cef-d																	
1932	admin@admin.test	ADMIN	2013-05-28 10:34:57	add	Attribute (40) from Event (1): Payload installation/md5 6570163cc34454b3e1476c134d44b9d9	event_id () => (1), uuid () => (8d300eb0-																	

- **Id:** The automatically assigned ID number of the entry.
- **Email:** The e-mail address of the user whose actions triggered the entry.
- **Org:** The organisation of the above mentioned user.
- **Created:** The date and time when the entry originated.
- **Action:** The action's type. This can include: login/logout for users, add, edit, delete for events, attributes, users and servers.
- **Title:** The title of an event always includes the target type (Event, User, Attribute, Server), the target's ID and the target's name (for example: e-mail address for users, event description for events).
- **Change:** This field is only populated for entries with "add" or "edit" actions. The changes are detailed in the following format: *_variable (initial_value) => (new_value),...* When the entry is about the creation of a new item (such as adding a new event) then the change will look like this for example: *org() => (ADMIN), date() => (20012-10-19),...*

Search Logs

Email	Organisation
<input type="text"/>	<input type="text"/>
Action	
<input type="text" value="ALL"/>	<input type="button" value="v"/>
Title	Change
<input type="text"/>	<input type="text"/>
<input type="button" value="Search"/>	

Searching Logs

Another way to browse the logs is to search it by filtering the results according to the following fields (the search is a sub-string search, the sub-string has to be an exact match for the entry in the field that is being searched for):

- **Email:** By searching by Email, it is possible to view the log entries of a single user.
- **Org:** Searching for an organisation allows you to see all actions taken by any member of the organisation.
- **Action:** With the help of this drop down menu, you can search for various types of actions taken (such as logins, deletions, etc).
- **Title:** There are several ways in which to use this field, since the title fields contain several bits of information and the search searches for any substrings contained within the field, it is possible to just search for the ID number of a logged event, the username / server's name / event's name / attributes name of the event target.
- **Change:** With the help of this field, you can search for various specific changes or changes to certain variables (Ex.: using "Published" as the search term for and find all log entries where an event has been "Published", ip-src will find all attributes where a source IP address has been entered / edited, etc).

Background Processing

If enabled, MISP can delegate a lot of the time intensive tasks to the background workers. These will then be executed in sequence, allowing the users of the instance to keep using the system without a hiccup and without having to wait for the process to finish. It also allows for certain tasks to be scheduled and automated.

Command Line Tools for the Background Workers

The background workers are powered by [CakeResque](#), so all of the CakeResque commands work. To start all of the workers needed by MISP go to your

```
/var/www/MISP/app/Console/worker (assuming a standard installation path) and execute start.sh. To interact with the workers, here is a list of useful commands. Go to your /var/www/MISP/app/Console (assuming a standard installation path) and execute one of the following commands as a parameter to ./cake CakeResque (for example: ./cake CakeResque tail):
```

- **start:** Start a new worker.
- **startscheduler:** Start a new scheduler worker.
- **stop:** Stop a worker.
- **pause:** Pause a worker.
- **resume:** Resume a paused worker.
- **cleanup:** Terminate the job that a worker is working on with immediate effect. You will be presented with a choice of workers to choose from when executing this command.

- **restart**: Stop all Resque workers, and start a new one.
- **clear**: Clear all jobs inside a queue
- **reset**: Reset CakeResque internal worker's saved status
- **stats**: Display some statistics about your workers including the count of successful and failed jobs.
- **tail**: Tail the various (workers) log files that CakeResque creates, just choose the one from the list that you are interested in.
- **track**: Track a job status.
- **load**: Load a set of predefined workers.

The other commands should not be required, instead of starting / stopping or restarting workers use the supplied start.sh (it stops all workers and starts them all up again). For further instructions on how to use the console commands for the workers, visit the [CakeResque list of commands](#).

Monitoring the Background Processes

The "Jobs" menu item within the Administration menu allows site admins to get an overview of all of the current and past scheduled jobs. Admins can see the status of each job, and what the queued job is trying to do. If a job fails, it will try to set an error message here too. The following columns are shown in the jobs table:

- **Id:** The job's ID (this is the ID of the job's metadata stored in the default datastore, not to be confused with the process ID stored in the redis database and used by the workers)
- **Process:** The process's ID.
- **Worker:** The name of the worker queue. There are 3+1 workers running if background jobs are enabled: default, cache, email, and a special Scheduler (this should never show up in the jobs table).
- **Job Type:** The name of the queued job.
- **Input:** Shows a basic input handled by the job - such as "Event:50" for a publish email alert job for event 50.
- **Message:** This will show what the job is currently doing or alternatively an error message describing why a job failed.
- **Org:** The string identifier of the organisation that has scheduled the job.
- **Status:** The status reported by the worker.
- **Retries:** Currently unused, it is planned to introduced automatic delayed retries for the background processing and thus add resilience.
- **Progress:** A progress bar showing how the job is coming along.

Jobs

Purge job entries:

Completed 0%

[> previous](#) [1](#) [2](#) [next >](#)

	JS	Default	Email	Cache								
Id		Date created	Date modified	Process ID	Worker	Job type	Input	Message	Organisation name	Status	Retries	Progress
38		2021-02-19 13:08:56	2021-02-19 13:08:58	44a2d93c0ca9fa65893842c750a02b8	email	posts_start	Post: 1	Emails sent.	JERON_4EYES	Completed	0	Completed
37		2021-02-17 15:03:44	2021-02-17 15:03:45	92f2ed9c0ca9fa65893842c750a02b8	update	num_updates	command:	Update done in another worker. Graciously stopping.	SYSTEM	Unknown	0	Completed
36		2021-02-17 15:03:44	2021-02-17 15:03:45	456a03727210a04439f0c33178053	update	num_updates	command:	Update done in another worker. Graciously stopping.	SYSTEM	Unknown	0	Completed
35		2021-02-17 15:03:44	2021-02-17 15:03:45	356a03727210a04439f0c33178053	update	num_updates	command:	Update done in another worker. Graciously stopping.	SYSTEM	Unknown	0	Completed

Scheduling Jobs and Recurring Jobs

Apart from off-loading long-lasting jobs to the background workers, there is a second major benefit of enabling the background workers: Site-administrators can schedule recurring tasks for the jobs that generally take the longest to execute. At the moment this includes pushing / pulling other instances and generating a full export cache for every organisation and export type. MISP comes with these 3 tasks pre-defined, but further tasks are planned. The following fields make up the [scheduled tasks](#) table:

- **Id:** The ID of the task.
- **Type:** The type of the task.
- **Frequency (h):** This number sets how often the job should be executed in hours. Setting this to 168 and picking the next execution on Sunday at 01:00 would execute the task every Sunday at 1 AM. Setting this value to 0 will make the task only run once on the scheduled date / time without rescheduling it afterwards.
- **Scheduled Time:** The time (in 24h format) when the task should be executed the next time it runs (and all consecutive times if a multiple of 24 is chosen for frequency).
- **Next Run:** The date on which the task should be executed.
- **Description:** A brief description of the task.
- **Message:** This field shows when the job was queued by the scheduler for execution.

Scheduled Tasks

Here you can schedule pre-defined tasks that will be executed every x hours. You can alter the date and time of the next scheduled execution and the frequency at which it will be repeated (expressed in hours). If you set the frequency to 0 then the task will not be repeated. To change any of the above mentioned settings just click on the appropriate field and hit update all when you are done editing the scheduled tasks.

[< previous](#)
[next >](#)

Id	Type	Frequency (h)	Scheduled Time	Next Run	Description	Message
3	push_all	0	12:00	2014-02-05	Initiates a full push for all eligible instances.	Not scheduled yet.
2	pull_all	0	12:00	2014-02-05	Initiates a full pull for all eligible instances.	Not scheduled yet.
1	cache_exports	36	18:00	2014-02-20	Generates export caches for every export type and for every organisation. This process is heavy, schedule so it might be a good idea to schedule this outside of working hours and before your daily automatic imports on connected services are scheduled.	32 jobs started at 20/02/2014 - 17:01:27.

Update all

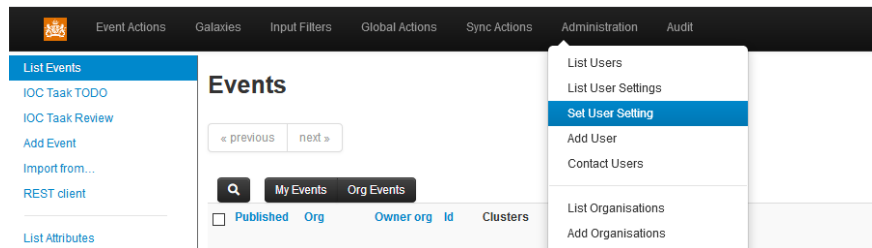
Various administration tips & tricks

Setting a Publish Alert Filter

To regulate the reception of e-mail from MISP it is possible to create filters. Each individual user account can apply such filter.

The filter can be configured by the user but also by the organization administrator.

After login goto Administration -> Set User Setting:



A new screen appears. Make sure the “Setting” drop down box shows “publish_alert_filter”:

Set User Setting

User

Setting

publish_alert_filter

Value

Example:

```
{
  "AND": {
    "NOT": {
      "EventTag.name": [
        "%osint%"
      ]
    }
  }
}
```

Submit

The text field “Value” contains the filter, which needs to be provided in JSON format. Important JSON-objects which can be used here go by the name AND”, “OR” and “NOT”. These should be structured in a logical tree.

The filtering can be applied to tags, the [publishing](#) organization and the threat level. Valid filters:

- AttributeTag.name
- EventTag.name
- Tag.name (checks against both event and attribute tags)
- Orgc.uuid (creator org uuid)
- Orgc.name (creator org name)
- ThreatLevel.name

In the following example, all notifications will be filtered which carry ‘t1p.white’ and ‘t1p.green’ in the name of the tag:

```
{
  "NOT": {
    "Tag.name" : [ "t1p.white", "t1p.green" ]
  }
}
```

The publish_alert_filter setting allows one filter definition to be active.

After applying the configuration, the filter will show up in the “My Settings” menu:

The screenshot shows the 'User settings management' page. The left sidebar contains a menu with 'My Settings' highlighted. The main content area shows a table of user settings. The table has columns for 'Id', 'User', 'Setting', and 'Value'. There is one record with Id 1, User '...', Setting 'publish_alert_filter', and Value containing a JSON filter definition. The value is:

```
{
  "NOT": {
    "Tag.name": [
      "t1p.white",
      "t1p.green"
    ]
  }
}
```

. The page footer indicates 'Page 1 of 1, showing 1 records out of 1 total, starting on record 1, ending on 1'.

Default sharing level

Choose your default sharing level to match your usage scenario for MISP. The setting is named *default_event_distribution* and the values can be:

- Your organisation only (default)
- This [community](#) only
- Connected communities
- All communities

You can also set a default distribution level for attributes contained in an event with *default_attribute_distribution*, and it has the same values as the default sharing level for events plus an additional one that allows attributes to inherit the sharing level of the event.

Adding organisation logos

You can add a logo for your organisations in MISP by uploading them via the tab **Manage files** under the **Administration** menu & **Server Settings** sub-menu. The filename must be exactly the same as the organisation name that you will use in MISP. It is recommended to use PNG files of 48x48 pixels.

The `_scheduler_` worker is not starting

If you already made sure that you copied the config file under the `cakereque` directory, it might be due to the FQDN of the server hosting the instance has changed. A way to fix this is to flush temporary data stored in redis. This can be done by logging in redis, for example when logging in with `redis-cli`, and issuing a `flushall` command.

How to redirect HTTP to HTTPS

Here is a sample configuration for Apache webserver.

```

<VirtualHost *:80>
    ServerAdmin misp@misp.misp
    ServerName misp.misp.misp
    ServerAlias misp-int.misp.misp

    Redirect permanent / https://misp.misp.misp

    LogLevel warn
    ErrorLog /var/log/apache2/misp.local_error.log
    CustomLog /var/log/apache2/misp.local_access.log combined
    ServerSignature Off
</VirtualHost>

<VirtualHost *:443>
    ServerAdmin misp@misp.misp
    ServerName misp.misp.misp
    ServerAlias misp-int.misp.misp

    DocumentRoot /var/www/MISP/app/webroot
    <Directory /var/www/MISP/app/webroot>
        Options -Indexes
        AllowOverride all
        Order allow,deny
        allow from all
    </Directory>

    SSLEngine On
    SSLCertificateFile /etc/ssl/misp.misp.misp/misp.crt
    SSLCertificateKeyFile /etc/ssl/misp.misp.misp/misp.key
    SSLCertificateChainFile /etc/ssl/misp.misp.misp/mispCA.crt

    LogLevel warn
    ErrorLog /var/log/apache2/misp.local_error.log
    CustomLog /var/log/apache2/misp.local_access.log combined
    ServerSignature Off
</VirtualHost>

```

Taken from [Koen Van Impe's blog](#)

Increase max size of Samples / other files

Trying to upload a large samples (>50M) might cause the following error: [!] 500

Server Error: Internal Server Error

Or will give you an error page in browser.

The error logs on the system will display the following:

```
PHP Warning: POST Content-Length of 57526024 bytes exceeds the limit of 8388608 bytes in /var/www/MISP/app/webroot/index.php on line 10
```

And / Or

```
PHP Fatal error: Allowed memory size of 134217728 bytes exhausted (tried to allocate 2097152 bytes) in /var/www/MISP/app/webroot/index.php on line 10
```

To fix that you need to adjust the php settings:

```
vi /etc/php5/apache2/php.ini
```

Increase to the following values (or more if you want to)

```
; Maximum size of POST data that PHP will accept.
; Its value may be 0 to disable the limit. It is ignored if POST data reading
; is disabled through enable_post_data_reading.
; http://php.net/post-max-size
post_max_size = 256M
[...]
; Maximum amount of memory a script may consume (128MB)
; http://php.net/memory-limit
memory_limit = 1024M
```

And then restart apache2

```
service apache2 restart
```

Support & feature requests

The preferred method for support & feature requests is to use the [GitHub ticketing system](#).

If you want to discuss something related to MISP, want some help from the [community](#), etc... You have the [MISP Users mailing list](#) and the [MISP developers mailing list](#).

A number of companies offer custom development, consulting, and support around MISP, please check [the support page of the MISP Project website](#).

More information in the notification emails about new events

The setting `MISP.extended_alert_subject` allows you to have an extended subject. One word of warning though. If you're using encryption : the subject will not be encrypted. Be aware that you might leak some sensitive information this way. Below is an example how the two subject types look like. First with the option disabled, then with the option enabled.

```
Event 7 - Low - TLP Amber
Event 8 - OSINT - Dissecting XXX... - Low - TLP Amber
```

Taken from [Koen Van Impe's blog](#)

Get top API users

Enable the `log_auth` setting in the server settings. Optionally enable `log_client_ip` if you want to get stats per client ip. Log into your mysql server and run the following query:

```
select ip,email,count(id) as c from logs WHERE ip IS NOT NULL group by ip,email
```

This will give you a top 10 table per ip and username:

ip	email	c
1.2.3.4	bob@nsa.gov	4124
5.6.7.8	vladimir@kremlin.ru	1932
9.10.11.12	fred@somewhere.eu	1317
13.14.15.16	SYSTEM	16

MISP Logs

By default, MISP has several layers of logs that can be used to trouble-shoot and monitor the system. Let's walk through each of the available logs:

- **Apache access logs:** Rotating logs generated by apache, logging each request, by default (on Ubuntu) they are found in `/var/log/apache2/misp.local_access.log`. The location can be changed via the apache conf file
- **Apache error logs:** Rotating logs generated by apache, logging error messages, by default (on Ubuntu) they are found in `/var/log/apache2/misp.local_error.log`. This error log file will generally not be used by MISP, however, if there is a PHP level error that prevents MISP from functioning you might have relevant entries here.
- **MISP error log:** Generated by MISP, logging any exceptions that occur during usage. These can be found in `/var/www/MISP/app/tmp/logs/error.log` (assuming default installation path). If you see errors in here and are stuck with an issue [let us know via GitHub!](#)
- **MISP debug log:** Generated by MISP, any debug messages and Notice level messages will be sent to this file. Generally less interesting, but can be helpful during debugging sessions. It should not be necessary to monitor this under normal usage. The file can be found in `/var/www/MISP/app/tmp/logs/debug.log` (assuming default installation path).
- **MISP worker error log:** Generated by MISP background workers, logging any exceptions generated during a background job. It is the equivalent of the MISP error log for background jobs, so if [scheduled tasks](#), [synchronisation](#) or e-mailing with the workers enabled are causing issues, this is the place to check. It can normally be found at `/var/www/MISP/app/tmp/logs/resque-worker-error.log`
- **MISP worker logs:** Rotating logs generated by MISP background workers, logging any jobs executed by workers. This is part of the normal operation of background workers and doesn't have to be monitored, though it can help when debugging issues. Normally found at `/var/www/MISP/app/tmp/logs/resque-[current date].log`
- **MISP scheduler error log:** Generated by MISP scheduler worker, logging any exceptions generated during the scheduling of a background job. It is the

equivalent of the MISP error log for scheduled jobs. It can normally be found at `/var/www/MISP/app/tmp/logs/resque-scheduler-error.log`

- **MISP scheduler logs:** Rotating logs generated by MISP scheduler worker, logging any schedulings of jobs to be executed by workers. This is part of the normal operation of the scheduler worker and doesn't have to be monitored, though it can help when debugging issues. Normally found at `/var/www/MISP/app/tmp/logs/resque-scheduler-[current date].log`

Logging of failed authentication attempts

By default, MISP logs all failed login and authentication attempts in the built in Audit logs. To view any such failed attempts, simply log in as a [site admin](#) and navigate to Audit - List logs.

There are two types of entries that will be interesting if you are looking for failed authentication attempts, entries of action "auth_fail" (for failed attempts to authenticate via the [API](#) key or the external authentication system) and login_fail (for failed login attempts via the login page).

You can also search for any such entries using the Search Logs feature, simply choose the desired action from the two listed above and hit search.

What is logged:

Auth method	Action	Failed credentials logged	IP
Webform	login_fail	None	Optional
API	auth_fail	API key	Optional
Webform	auth_fail	External auth key	Optional

In order to enable IP logging for any logged request in MISP, navigate to Administration - Server settings - MISP settings and enable the `MISP.log_client_ip` setting.

It is also possible to enable full logging of [API](#) and external authentication requests using the `MISP.log_auth` setting in the same location, but keep in mind that this is highly verbose and will log every request made. In addition to the information above, all accessed resource URLs are also logged.

Clearing expired sessions

By default the garbage collection of sessions is disabled in PHP. It is possible to enable it, but it's not recommended and as such MISP provides a manual way of clearing the sessions.

Navigate to the diagnostics screen of MISP (Administration - Server settings - Diagnostics) and near the bottom of the page there will be a counter showing the count of currently stored expired sessions. Simply purge them by clicking the applicable button when the number grows too large.

Troubleshooting MISP not connecting to redis but redis-cli working

If you have an IPv6 enabled OS, but an older redis version that does not support IPv6 (<v2.8), MISP might fail to connect to the redis server while redis-cli is working. The reason is that redis-cli is connecting to 127.0.0.1 directly, while the calls inside the CakeResque library used by MISP are done using "localhost" which resolves both to the IPv4 and IPv6 loopback addresses. For some reasons, the use of the IPv6 address is attempted first which fails.

You can confirm this by trying to connect to redis using **telnet localhost 6379**. If it fails, the error message should mention the IPv6 loopback address (:::1).

Two ways to fix it:

- 1) Upgrade your redis to a server that supports IPv6 (v2.8+). This is the preferred recommendation.
- 2) Comment the localhost mapping to IPv6 address in /etc/hosts

Errors about fields or tables

If you have errors with fields or tables that you can see in the error.log or in the page (if you enabled *debug* or *site_admin_debug* settings), an easy fix to make most of them go away is to use the **clean cache** feature on the *server settings* menu, *diagnostics* tab. An example of error message:

Error: [PDOException] SQLSTATE[42S22]: Column not found: 1054 Unknown column 't

Jobs

The Jobs tab gives you an overview on any currently running jobs or jobs that were previously completed and their status.

Jobs

Purge job entries:

Completed All

< previous 1 2 next >

Id	Date created	Date modified	Process ID	Worker	Job type	Input	Message	Organization name	Status	Retries	Progress
38	2021-02-19 13:08:58	2021-02-19 13:08:58	44ad090a0adff8030427c5da6c268	email	posts_alert	Post: 1	Emails sent.	JERGEN_KEYES	Completed	0	Completed
37	2021-02-17 15:03:44	2021-02-17 15:03:45	93265f6b6dc0d6e269ec17d68f6a6f	update	run_updates	command	Update done in another worker. Gracefully stopping	SYSTEM	Unknown	0	Completed
36	2021-02-17 15:03:41	2021-02-17 15:03:45	544ae033720844e1390cd033178053	update	run_updates	command	Update done in another worker. Gracefully stopping	SYSTEM	Unknown	0	Completed
35	2021-02-17 15:03:41	2021-02-17 15:03:45	256ae075771980b08fae5f18a60b116	update	run_updates	command	Update done	SYSTEM	Unknown	0	Completed

Typically this is one of the places you would turn to even some background process might not complete as expected to get an indication on any issues related to user initiated Jobs.

For ease of use, you can filter the Jobs by 'All', 'Default', 'Email', 'Cache'

TODO: Explain differences Default, Email, Cache

You can also purge the entries, either only by completed status or purge all. This is not automated and needs to be done manually.

Scheduled Tasks

Straight from the UI:

"" Here you can schedule pre-defined tasks that will be executed every x hours. You can alter the date and time of the next scheduled execution and the frequency at which it will be repeated (expressed in hours). If you set the frequency to 0 then the task will not be repeated. To change any of the above mentioned settings just click on the appropriate field and hit update all when you are done editing the [scheduled tasks](#).

Warning: [Scheduled tasks](#) come with a lot of caveats and little in regards of customisations / granularity. You can instead simply create cron jobs out of the console commands as described here: Automating certain console tasks ""

The task scheduler is a sub-par component to enable minimal functionality in terms of automating certain MISP tasks. If you have a dedicated and conscious MISP [Site Admin](#) she can keep an eye on the Scheduler to make sure everything runs smoothly.

For better performance please use a real scheduler like your systems' crontab. As a rule of thumb: If you can click on it, MISP can automate it.

MISP Backup

Currently there exists this backup script simply called [misp-backup.sh](#)

All you need is to copy the the sample config and make sure it is correct. Then launch the script.

```
cd /var/www/MISP/tools/misp-backup
sudo -u www-data cp misp-backup.conf.sample misp-backup.conf
sudo ./misp-backup.sh
```

Script output:


```

/var/www/MISP/tools/misp-backup 2.4 • $ sudo ./misp-backup.sh
File ./misp-backup.conf exists.
copy of org images and other custom images
MySQL Dump
/var/www/MISP/tools/misp-backup
MISP Backup Completed, OutputDir: /opt/backup
FileName: MISP-Backup-20181128_163215.tar.gz
FullName: /opt/backup/MISP-Backup-20181128_163215.tar.gz

```

MISP Restore

In a similar fashion you can restore your [MISP instance](#) with the `misp-restore.sh` script. Read the script for details.

Command line interface (CLI) commands

The below info is also available in the MISP GUI. Go to event actions -> automation -> bottom of the page

Administering MISP via the CLI

Get Setting

```
MISP/app/Console/cake Admin getSetting [setting]
```

Set Setting

```
MISP/app/Console/cake Admin setSetting [setting] [value]
```

Get Authkey

```
MISP/app/Console/cake Admin getAuthkey [email]
```

Reset Authkey

```
MISP/app/Console/cake Authkey [email] [api_key | optional]
```

Set Baseurl

```
MISP/app/Console/cake Baseurl [baseurl]
```

Change Password

```
MISP/app/Console/cake Password [email] [new_password] [--override_password_char
```

Clear Bruteforce Entries

```
MISP/app/Console/cake Admin clearBruteforce [user_email]
```

Run Database Update

```
MISP/app/Console/cake Admin updateDatabase
```

Update All JSON Structures

```
MISP/app/Console/cake Admin updateJSON
```

Update Galaxy Definitions

```
MISP/app/Console/cake Admin updateGalaxies
```

Update Taxonomy Definitions

```
MISP/app/Console/cake Admin updateTaxonomies
```

Enable all tags of a taxonomy

```
MISP/app/Console/cake Admin enableTaxonomyTags [taxonomy_id]
```

Update Object Templates

```
MISP/app/Console/cake Admin updateObjectTemplates
```

Update Warninglists

```
MISP/app/Console/cake Admin updateWarningLists
```

Update Noticelists

```
MISP/app/Console/cake Admin updateNoticeLists
```

Update MISP

```
MISP/app/Console/cake Admin updateMISP
```

Set Default Role

```
MISP/app/Console/cake Admin setDefaultRole [role_id]
```

Get IPs For User ID

```
MISP/app/Console/cake Admin UserIP [user_id]
```

Get User ID For User IP

```
MISP/app/Console/cake Admin IPUser [ip]
```

Automating certain console tasks

If you would like to automate tasks such as caching feeds or pulling from server instances, you can do it using the following command line tools. Simply execute the given commands via the command line / create cron jobs easily out of them.

PullAll

```
MISP/app/Console/cake Server pullAll [user_id] [full|update]
```

Pull

```
MISP/app/Console/cake Server pull [user_id] [server_id] [full|update]
```

Push

```
MISP/app/Console/cake Server push [user_id] [server_id]
```

Cache Feeds For Quick Lookups

```
MISP/app/Console/cake Server cacheFeed [user_id] [feed_id|all|csv|text|misp]
```

Fetch Feeds As Local Data

```
MISP/app/Console/cake Server fetchFeed [user_id] [feed_id|all|csv|text|misp]
```

Run Enrichment

```
MISP/app/Console/cake Event enrichment [user_id] [event_id] [json_encoded_modu
```

Test Server

```
MISP/app/Console/cake Server test [server_id]
```

List Servers

```
MISP/app/Console/cake Server listServers
```

Managing the background workers

The background workers can be managed via the CLI in addition to the UI / [API](#) management tools.

Get List Of Workers

```
MISP/app/Console/cake Admin getWorkers [all|dead]
```

Start A Worker

```
MISP/app/Console/cake Admin startWorker [queue_name]
```

Restart A Worker

```
MISP/app/Console/cake Admin restartWorker [worker_pid]
```

Restart All Workers

```
MISP/app/Console/cake Admin restartWorkers
```

Kill A Worker

```
MISP/app/Console/cake Admin killWorker [worker_pid]
```

Last modified: Tue Mar 09 2021 13:54:37 GMT+0100 (Central European Standard Time)

- [Feeds](#)
 - [Managing feeds](#)
 - [Default feeds](#)
 - [Caching feeds](#)
 - [Fetching feeds](#)
 - [Search feed caches](#)
 - [Adding feeds](#)
 - [Importing feeds](#)
 - [Analyze feed overlap](#)
 - [Exporting feeds](#)
 - [Feed correlation](#)

Feeds

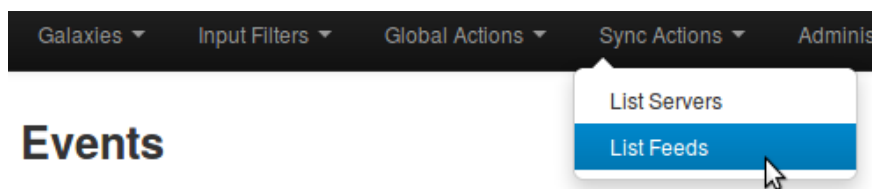
Feeds are remote or local resources containing [indicators](#) that can be automatically imported into MISP at regular intervals. Feeds can be structured in [MISP format](#), CSV format or even free-text format. You can easily import any remote or local URL to store the data in your [MISP instance](#). It's a simple way to gather many external sources of information into MISP without any programming skills.

Feed descriptions can be also easily shared among different MISP instances as you can export a feed description as JSON and import it back in another [MISP instance](#).

Managing feeds

[warning] A [site admin](#) role is required to perform these actions.

To manage feeds you first need to access the Feeds page using the List Feeds item on the top menu:



Then you will see the Feeds page with a table of configured feeds.

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](#)[1](#)[2](#)[next »](#)[last »](#)

Default feedsCustom feedsAll feedsEnabled feeds

<input type="checkbox"/>	Id	Enabled	Caching	Name	Format	Provider	Org	Source	URL
<input type="checkbox"/>	1	✓	✓	CIRCL	misp	CIRCL		network	https://www.circl.lu/doc/misp/feed-osint/
<input type="checkbox"/>	2	✓	✓	Botvrij.eu	misp	Botvrij.eu		network	https://www.botvrij.eu/data/feed-osint
<input type="checkbox"/>	9	✓	✓	Tor exit nodes	csv	TOR Node List from dan.me.uk		network	https://www.dan.me.uk/torlist/?exit

Default feeds

The MISP project supplies a list of open-source feeds. You can load these feed definitions by using the 'Load default feed metadata' button on the Feeds page. This feature creates new feeds by importing the entries in file `app/files/feed-metadata/defaults.json` to the database. Existing feeds are not changed. The feature checks for duplicates using the feed URL. If a feed with the same URL already exists in the database, that entry is not imported. This ensures that local modifications such as name, distribution or enabled status are never overwritten.

Caching feeds

Caching downloads the feed content to the Redis server in your instance, and allows you to correlate attributes and see matching "Feed hits" (similar to correlated "Related Events") in the event view on each attribute row. Caching does not create any events in the database server in your instance.

Use the buttons at the top of the Feeds screen to retrieve data from feeds and store the data in the Redis cache. The buttons let you cache data from all feeds, cache data from freetext/CSV-format feeds only, or cache data from MISP-format feeds only.

Fetching feeds

Use the button at the top right of the Feeds screen to fetch data from all feeds and ingest the data to the MISP database.

Search feed caches

To search the feed caches, select the Search Feed Caches option on the side menu. This displays a table where you can search for values potentially contained in the cached feeds and servers.

Feed Cache Search

Search for values potentially contained in the cached feeds and servers.

« previous 1 2 next » last »

Id	Type	Name	Feed URL
1	MISP Feed	CIRCL	https://www.circl.lu/doc/misp/feed-osint/
2	MISP Feed	Botvrij.eu	https://www.botvrij.eu/data/feed-osint
9	Feed	Tor exit nodes	https://www.dan.me.uk/torlist/?exit

Adding feeds

To add a new feed, select the Add Feed option on the side menu. Here you will have access to a dynamic form. Let's check each field by order. The form shows or hides fields based on the selections in the drop-down fields.

Add MISP Feed

Add a new MISP feed source.

- ☐ Enabled ☐ Caching enabled
☐ Lookup visible

Name

Provider

Input Source

URL

Source Format

Any headers to be passed with requests (for example: Authorization)

Line break separated list of headers in the "headername: value" format

Add Basic Auth

Distribution

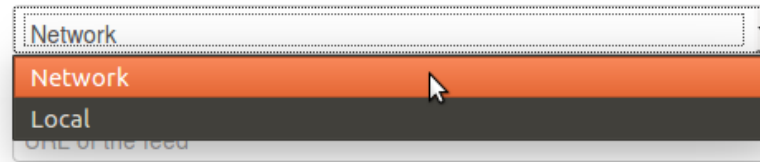
Default Tag

Filter rules:

Modify

- Enabled: Is the feed active or not
- Caching enabled: Should the feed data be cached
- Lookup visible: If this is not checked, correlations will only show up for you; if checked, correlations are visible for other users as well
- Name: Name to identify the feed; not required to be unique
- Provider: Name of the content provider
- Input Source: Where does the input come from

Input Source



- Network: hosted somewhere outside the platform
- Local: Hosted on the local server. In this case, a new checkbox "Remove input after ingestion" will appear. If checked, the source is deleted after usage.

Input Source

☐ Remove input after ingestion

- URL: URL of the feed, where it is located (for Local hosted files, point to the manifest.json; e.g., /home/user/feed-generator/output/manifest.json)
- The Source Format can be:

Source Format



- MISP Feed: The source points to a list of JSON formatted files like MISP events.

Example: <https://www.circl.lu/doc/misp/feed-osint>

- Freetext Parsed Feed: The options for a freetext-parsed feed are shown below.

Source Format

Freetext Parsed Feed

Creator organisation

CIRCL

Target Event

Fixed Event

Target Event ID

Leave blank unless you want to reuse an existing event.

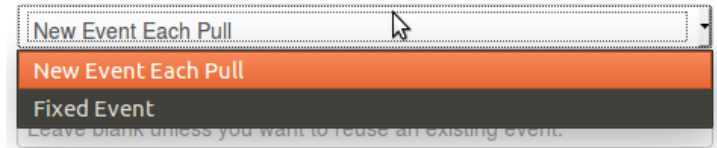
Exclusion Regex

Regex pattern, for example: "/^https://myfeedurl/i

- ☐ Auto Publish
- ☐ Override IDS Flag
- ☐ Delta Merge

- Creator organisation: The creator organisation (orgc_id) for the event created from this feed. Appears in the Org column on the List Feeds screen.
- Target Event: The event to hold data from the feed. Can be either "New Event Each **Pull**" (a new event will be created each time the feed is pulled) or "Fixed Event" (a unique event will be updated with the new data, as determined by the next field).

Target Event



New Event Each Pull

New Event Each Pull

Fixed Event

Leave blank unless you want to reuse an existing event.

- Target Event ID: The ID of the event where the data will be added; if not set, the field will be set the first time the feed is fetched.
 - Exclusion Regex: Add a regex pattern for detecting IoCs that should be skipped. This can be useful to exclude any references to the actual report / feed for example.
 - Auto Publish: If checked, the event created from the feed will be automatically published
 - Override IDS Flag: If checked, the IDS flag will be set to false
 - Delta Merge: If checked, only attributes from the most recent fetch are kept, the old ones are (soft-) deleted.
- o Simple CSV Parsed Feed: The options for a character-separated feed are shown below.

Source Format

Simple CSV Parsed Feed

Creator organisation

CIRCL

Target Event

Fixed Event

Target Event ID

Leave blank unless you want to reuse an existing event.

Value field(s) in the CSV

2,3,4 (column position separated by commas)

Delimiter

,

Exclusion Regex

Regex pattern, for example: "/^https://myfeedurl/i

- ☐ Auto Publish
- ☐ Override IDS Flag
- ☐ Delta Merge

- Creator organisation: The creator organisation (orgc_id) for the event created from this feed. Appears in the Org column on the List Feeds screen.
- Target Event: The event to hold data from the feed. Can be either "New Event Each [Pull](#)" (a new event will be created each time the feed is pulled) or "Fixed Event" (a unique event will be updated with the new data, as determined by the next field).
- Target Event ID: The ID of the event where the data will be added; if not set, the field will be set the first time the feed is fetched.
- Value field(s) in the CSV: Select one or several fields that should be parsed by the CSV parser and converted into MISP attributes; specify column position separated by commas
- Delimiter: Set the field separator; default is comma ","
- Exclusion Regex: Add a regex pattern for detecting IoCs that should be skipped. This can be useful to exclude any references to the actual report / feed for example.
- Auto Publish: If checked, the event created from the feed will be automatically published
- Override IDS Flag: If checked, the IDS flag will be set to false
- Delta Merge: If checked, only attributes from the most recent fetch are kept, the old ones are (soft-) deleted.
- Distribution: The distribution option that will be set on the event created from the feed. The choices are:
 - Your organisation only
 - This [community](#) only
 - Connected communities
 - All communities
 - Sharing Group. In this case, a new field Sharing Group appears where you must select a group.
- Default Tag: A default tag can be added to the created event(s)
- Filter rules: Here you can define which tags or organisations are allowed or blocked.

Set pull rules

Allowed Tags

<<

>>

Blocked Tags

Allowed Organisations

<<

>>

Blocked Organisations

Update

Cancel

To add a tag (or organisation respectively), first type it into the top middle (bottom middle for organisation) text field. Then use the arrows that point to the outside to add it to the allowed or blocked tags (or organisations respectively) list.

Set pull rules

Allowed Tags

Blocked Tags

<<>>

tlp:green

<<>>

Allowed Organisations

Blocked Organisations

<<>>

<<>>

Update

Cancel

Set pull rules

Allowed Tags

tlp:white

<< >>

Blocked Tags

tlp:green

<< >>

Allowed Organisations

<< >>

Blocked Organisations

<< >>

Update

Cancel

To remove a tag (or organisation respectively), select it in the list and click on the arrow pointing to the inside.

Set pull rules

Allowed Tags

tip:white

<< >>

<< >>

Blocked Tags

tip:green

Allowed Organisations

<< >>

<< >>

Blocked Organisations

Update

Cancel

Set pull rules

Allowed Tags

<< >>

<< >>

tlp:green

Allowed Organisations

<< >>

<< >>

Update

Cancel

Importing feeds

To import a new feed, select the Import Feeds from JSON option on the side menu. Paste MISP feed metadata JSON into the text box and click the Add button. Double check values in ID fields that are specific to an instance including the feed ID (field id), event ID (field event_id), organisation ID (field orgc_id), sharing group ID (field sharing_group_id) and tag ID (field tag_id).

Analyze feed overlap

To analyze feed data overlap, select the Feed overlap analysis matrix option on the side menu. This presents overlap matrix obtained by analyzing cached feed data.

Feed overlap analysis matrix

	F1	F2	F9	F10	F20	F25	F26	F31
Feed #1 CIRCL	-	1%	0%	0%	0%	0%	0%	0%
Feed #2 Botvrij.eu	30%	-	0%	0%	0%	0%	0%	0%
Feed #9 Tor exit nodes	0%	0%	-	95%	4%	0%	0%	6%
Feed #10 Tor ALL nodes	0%	0%	22%	-	1%	0%	0%	1%
Feed #20 pop3gropers	0%	0%	0%	0%	-	0%	0%	0%
Feed #25 OpenPhish url list	0%	0%	0%	0%	0%	-	0%	0%
Feed #26 firehol_level1	1%	0%	0%	0%	0%	0%	-	0%
Feed #31 blocklist.de	0%	0%	0%	0%	1%	0%	0%	-

Exporting feeds

To export all feed metadata, select the Export Feeds settings option on the side menu. The server will [push](#) a JSON file for download.

Feed correlation

If an indicator from a feed matches an indicator within a [MISP event](#), it will show up as "Feed hits" in the event overview. The correlation will not show up in the correlation graph of the event.

Last modified: Tue Mar 09 2021 13:54:37 GMT+0100 (Central European Standard Time)

Updating Python Dependencies

MISP requires a couple of python libraries to be installed for the entire set of functionalities to work properly.

These functionalities include for instance the different import and export tools, the binaries extraction from attachments or PyMISP.

Installation

We started using virtual environments in MISP to make the installation and maintenance of the python versions easier.

Either using the [installation script](#) to setup a running MISP on your machine, or starting using the automatically generated [virtual machine](#) will give you access to the latest version of the required python libraries installed within a virtual environment called `virtualenv`.

But if you are using an older MISP version, you may want to install the virtual environment

Set the virtual environment up

```
# Create a python3 virtualenv
sudo -H -u www-data virtualenv -p python3 /var/www/MISP/venv

# Make pip happy
sudo mkdir /var/www/.cache
sudo chown www-data:www-data /var/www/.cache
```

If you already have a `venv` directory, you can skip this step

Updating MISP and its dependencies

Keeping MISP up-to-date as much as possible is the safest way to avoid most of the potential issues.

It can be done either by using the Update button in the diagnostic tool available with the MISP UI, or by using the command line.

Updating MISP core

In order to update MISP dependencies, we first want to [pull](#) the latest MISP version, so we have the latest submodule references as well.

MISP version

Every version of MISP includes a json file with the current version. This is checked against the latest tag on github, if there is a version mismatch the tool will warn you about it. Make sure that you update MISP regularly.

Currently installed version... v2.4.117 (b825e44a3988db8430089b0ebf787af272e06f88)

Latest available version... v2.4.117 (b825e44a3988db8430089b0ebf787af272e06f88)

Status... OK

Current branch... 2.4

Update MISP

Update Progress

OR

```
sudo -H -u www-data git pull origin 2.4
```

Once we have the latest MISP update, we can start updating the python libraries.

Updating the python dependencies

MISP is provided with a lot of submodules used to ensure all the additional functionalities work as expected. Thus it is important to keep those dependencies up-to-date.

```
sudo -H -u www-data git submodule update --init --recursive
```

Updating python dependencies

It is possible to check the status of all the python libraries required by MISP, using again the diagnostic tool.

Advanced attachment handler

The advanced attachment tools are used by the add attachment functionality to extract additional data about the uploaded sample.

```
pydeep:... OK
llef:... OK
magic:... OK
pymisp:... OK
```

STIX and Cybox libraries

Mitre's STIX and Cybox python libraries have to be installed in order for MISP's STIX export to work. Make sure that you install them (as described in the MISP installation instructions) if you receive an error below.

If you run into any issues here, make sure that both STIX and CyBox are installed as described in the INSTALL.txt file. The required versions are:

```
STIX: > 1.2.0.6
CyBox: > 2.1.0.18.dev0
mixbox: 1.0.3
maec: > 4.1.0.14
STIX2: > 1.2.0
PyMISP: > 2.4.93
```

Other versions might work but are not tested / recommended.

```
Current libraries status...OK
STIX library version...OK
CYBOX library version...OK
MIXBOX library version...OK
MAEC library version...OK
STIX2 library version...OK
PYMISP library version...OK
```

Yara

This tool tests whether plyara, the library used by the yara export tool is installed or not.

```
plyara library installed...OK
```


If something is going wrong, updating the corresponding library will make the diagnostic happy.

```
# Update PyMISP
cd /var/www/MISP/PyMISP
sudo -H -u www-data /var/www/MISP/venv/bin/pip install -U .

# Update the advanced attachment handler libraries (PICK THE ONE.S YOU NEED TO
# lief
sudo -H -u www-data /var/www/MISP/venv/bin/pip install -U lief
# python-magic
sudo -H -u www-data /var/www/MISP/venv/bin/pip install -U python-magic
# pydeep - WARNING: It requires libfuzzy-dev
sudo -H -u www-data /var/www/MISP/venv/bin/pip install -U pydeep

# Update the STIX dependencies (PICK THE ONE.S YOU NEED TO UPDATE)
# STIX
cd /var/www/MISP/app/files/scripts/python-stix
sudo -H -u www-data /var/www/MISP/venv/bin/pip install -U .
# mixbox
cd /var/www/MISP/app/files/scripts/mixbox
sudo -H -u www-data /var/www/MISP/venv/bin/pip install -U .
# Cybox
cd /var/www/MISP/app/files/scripts/python-cybox
sudo -H -u www-data /var/www/MISP/venv/bin/pip install -U .
# MAEC
cd /var/www/MISP/app/files/scripts/python-maec
sudo -H -u www-data /var/www/MISP/venv/bin/pip install -U .
# STIX 2
cd /var/www/MISP/cti-python-stix2
sudo -H -u www-data /var/www/MISP/venv/bin/pip install -U .

# Update Yara python library
sudo -H -u www-data /var/www/MISP/venv/bin/pip install -U plyara
```

Note that if any of the STIX, Cybox, mixbox or MAEC update fails because of a `No such file or directory` error, you just have to `git clone` them and start again the `pip` command above.

```
cd /var/www/MISP/app/files/scripts
sudo -H -u www-data git clone https://github.com/CybOXProject/python-cybox.git
sudo -H -u www-data git clone https://github.com/STIXProject/python-stix.git
sudo -H -u www-data git clone https://github.com/MAECProject/python-maec.git
sudo -H -u www-data git clone https://github.com/CybOXProject/mixbox.git
```

If you want to use / update the ZeroMQ functionality, you can also install / update the `zmq` python library.

```
# Install zmq library
sudo -H -u www-data /var/www/MISP/venv/bin/pip install zmq
# Update zmq library
sudo -H -u www-data /var/www/MISP/venv/bin/pip install -U zmq
```

Updating MISP modules

Another set of dependencies you may want to update are [MISP modules](#).

[MISP modules](#) have their own dependencies that need to be up-to-date as well as the modules scripts themselves.

Note that the following instructions consider your [MISP modules](#) are installed in the default path where we install them on our virtual machine or following the install script. Please change the path accordingly if needed.

```
# Change here the path if needed
cd /usr/local/src/misp-modules
# Update misp-modules requirements
sudo -H -u www-data /var/www/MISP/venv/bin/pip install -U -r REQUIREMENTS
# Update misp-modules scripts
sudo -H -u www-data /var/www/MISP/venv/bin/pip install -U .
```

You will then need to restart the modules, please refer to the [documentation](#).

Last modified: Sat Apr 24 2021 16:29:31 GMT+0200 (Central European Summer Time)

- Automation API
 - General
 - Automation URL
 - Automation key
 - Accept and Content-Type headers
 - Automation using PyMISP
 - Status Codes
 - Error Handling
 - Wrong endpoint chosen
 - Example
 - Search
 - Events management
 - /events
 - Accepted Methods
 - Description
 - GET /events
 - Description
 - URL Arguments
 - Output
 - Example
 - POST /events
 - Example
 - DELETE /events
 - Description
 - URL Arguments
 - Output
 - Example
 - GET /events/index
 - Description
 - Output
 - Example
 - POST /events/AddTag
 - URL Arguments
 - POST /events/removeTag
 - URL Arguments
 - GET /events/pushEventToZMQ/
 - Description
 - URL Arguments
 - Example
 - GET /events/nids NIDS rules export
 - GET /events/hids Hash - HIDS database export
 - GET /events/stix STIX export
 - Various ways to narrow down the search results of the STIX export
 - Tag management
 - POST /tags/add

- Description
- URL Arguments
 - Mandatory
 - Optional
- Example
- POST /tags/attachTagToObject
 - Description
 - URL Arguments
 - Response
 - Example
- POST /tags/removeTagFromObject
 - Description
 - URL Arguments
 - Response
 - Example
- GET /tags/tagStatistics/
 - Description
 - Output
 - Example
- Attribute management
 - POST /attributes/add/
 - URL Arguments
 - Output
 - Example
 - GET /attributes
 - URL Arguments
 - URL Attributes
 - Output
 - Example
 - POST /attributes/delete/
 - Description
 - URL Arguments
 - Output
 - Example
 - POST /attributes/addTag
 - URL Arguments
 - POST /attributes/removeTag
 - URL Arguments
 - GET /attributes/attributeStatistics
 - Description
 - Output
 - Example
 - GET /attributes/describeTypes Describe types API
 - Example
 - POST /attributes/restSearch
 - Parameters
 - Example
- Objects management

- [POST /objects/delete/\[object_id\]/\[hard_delete\]](#)
 - [Description](#)
 - [URL Arguments](#)
 - [Example](#)
- [Server management](#)
 - [GET /servers/getPyMISPVersion](#)
 - [Result](#)
 - [Example](#)
 - [GET /servers/getVersion](#)
 - [Result](#)
 - [Example](#)
- [Sightings](#)
 - [POST /sightings/add/](#)
- [User management](#)
 - [POST /admin/users/add](#)
 - [POST admin/users/edit/](#)
 - [POST admin/users/delete/](#)
 - [Parameters](#)
 - [Example](#)
 - [GET admin/users](#)
 - [Description](#)
 - [Output](#)
 - [Example](#)
 - [GET admin/users/view/](#)
 - [Description](#)
 - [Parameters](#)
 - [Output](#)
 - [Example](#)
 - [POST admin/users/add/](#)
- [Discussion API](#)
- [Organisation management](#)
- [Special Cases](#)
 - [XML Export](#)
 - [JSON query format](#)
 - [XML query format](#)
 - [XML download and URL parameters](#)
 - [CSV export](#)
 - [Update 2.4.82](#)
- [RPZ export](#)
- [Text export](#)
- [RESTful searches with XML result export](#)
- [Export attributes of event with specified type as XML](#)
- [Filtering event metadata](#)
- [Download attachment or malware sample](#)
- [Download malware sample by hash](#)
- [Upload malware samples using the "Upload Sample" API](#)
- [Proposals API](#)
- [Sharing groups](#)

- [Enable, disable and fetching feeds via the API](#)
- [Sightings API](#)
- [Warninglists API](#)
 - [GET warninglists/index](#)
 - [Description](#)
 - [Parameters](#)
 - [Output](#)
 - [Example](#)
 - [GET warninglists/view/1](#)
 - [Description](#)
 - [Parameters](#)
 - [Output](#)
 - [Example](#)
- [Attribute statistics API](#)
- [Additional statistics](#)
- [MISP modules](#)
 - [Description](#)
 - [GET /modules/](#)
 - [Example](#)
 - [Output](#)
 - [POST /modules/queryEnrichment](#)
 - [Example](#)

Automation API

Automation functionality is designed to automatically generate signatures for intrusion detection systems. To enable signature generation for a given attribute, Signature field of this attribute must be set to Yes. Note that not all attribute types are applicable for signature generation, currently we only support [NIDS](#) signature generation for IP, domains, host names, user agents etc., and hash list generation for MD5/SHA1 values of file artefacts. Support for more attribute types is planned. To make this functionality available for automated tools an authentication key is used. This makes it easier for your tools to access the data without further form-based-authentication. The [API](#) key can be found and managed under My Profile page (</users/view/me>) on a [MISP instance](#).

General

Automation URL

The documentation will include a default MISP URL in the examples. Don't forget to replace it with your MISP URL.

Default MISP URL in the documentation:

```
https://<misp url>/
```

Automation key

The authentication of the automation is performed via a secure key available in the MISP UI interface. Make sure you keep that key secret as it gives access to the entire database! The [API](#) key is available in the event actions menu under automation.

Since version 2.2 the usage of the authentication key in the URL is deprecated. Instead, pass the auth key in an Authorization header in the request. The legacy option of having the auth key in the URL is temporarily still supported but not recommended.

The authorization is performed by using the following header:

```
Authorization: YOUR API KEY
```

Accept and Content-Type headers

When performing your request, depending on the type of request, you might need to explicitly specify in what content type you want to get your results. This is done by setting one of the below Accept headers:

```
Accept: application/json  
Accept: application/xml
```

When submitting data in a POST, PUT or DELETE operation you also need to specify in what content-type you encoded the payload. This is done by setting one of the below Content-Type headers:

```
Content-Type: application/json  
Content-Type: application/xml
```

Example:

```
curl --header "Authorization: YOUR API KEY" --header "Accept: application/json"
```

By appending .json or .xml the content type can also be set without the need for a header.

Automation using PyMISP

PyMISP is a Python library to access MISP platforms via their REST [API](#).

PyMISP allows you to fetch events, add or update events/attributes, add or update samples or search for attributes.

[PyMISP is available](#) including a documentation with various examples.

Status Codes

To be done

- 50x
- 400 - 499

Error Handling

Wrong endpoint chosen

Example

```
curl --header "Authorization: YOUR API KEY " --header "Accept: application/json"
```

```
{"name": "Not Found", "message": "Not Found", "url": "\servers\gaaa"}
```

Search

It is possible to search in the database for a list of attributes or events based on a list of criterias.

To return attributes or events in a desired format, use the following URL and header settings:

URL:

```
YOUR_MISP_URL/attributes/restSearch  
YOUR_MISP_URL/events/restSearch
```

Headers:

```
Accept: application/json  
Content-type: application/json  
Authorization: YOUR_API_KEY
```

The next feature to take care of then is the body of the query. This is where you are going to put your filters.

As an example, if we want to export all the IP addresses that have a TLP marking and not marked as TLP:red, you can find below the corresponding filters to use:


```
{
  "returnFormat": "json",
  "type": {
    "OR": [
      "ip-src",
      "ip-dst"
    ]
  },
  "tags": {
    "NOT": [
      "tlp:red"
    ],
    "OR": [
      "tlp:%"
    ]
  }
}
```

Find below a non exhaustive list of parameters that can be used to filter data in your search (some parameters specific to given export formats are not mentioned):

- **returnFormat:** Set the return format of the search (Currently supported: json, xml, openioc, suricata, snort - more formats are being moved to restSearch with the goal being that all searches happen through this [API](#)). Can be passed as the first parameter after restSearch or via the JSON payload.
- **limit:** Limit the number of results returned, depending on the scope (for example 10 attributes or 10 full events).
- **page:** If a limit is set, sets the page to be returned. page 3, limit 100 will return records 201->300).
- **value:** Search for the given value in the attributes' value field.
- **type:** The attribute type, any valid [MISP attribute](#) type is accepted.
- **category:** The attribute category, any valid [MISP attribute](#) category is accepted.
- **org:** Search by the creator organisation by supplying the organisation identifier.
- **tags:** To include a tag in the results just write its names into this parameter. To exclude a tag prepend it with a '!'. To include a tag prepend it with a '!'.
- **quickfilter:** Enabling this (by passing "1" as the argument) will make the search ignore all of the other arguments, except for the auth key and value. MISP will return an xml / json (depending on the header sent) of all events that have a sub-string match on value in the event info, event orgc, or any of the attribute value1 / value2 fields, or in the attribute comment.
- **from:** Events with the date set to a date after the one specified in the from field (format: 2015-02-15). This filter will use the date of the event.
- **to:** Events with the date set to a date before the one specified in the to field (format: 2015-02-15). This filter will use the date of the event.
- **eventid:** The events that should be included / excluded from the search
- **withAttachments:** If set, encodes the attachments / zipped malware samples as base64 in the data field within each attribute
- **metadata:** Only the metadata (event, tags, relations) is returned, attributes and [proposals](#) are omitted.
- **uuid:** Restrict the results by uuid.

- **publish_timestamp**: Restrict the results by the timestamp of the last [publishing](#) of the event. The input can be a timestamp or a short-hand time description (7d or 24h for example). You can also pass a list with two values to set a time range (for example ["14d", "7d"]).
- **last**: (Deprecated synonym for publish_timestamp) Restrict the results by the timestamp of the last [publishing](#) of the event. The input can be a timestamp or a short-hand time description (7d or 24h for example). You can also pass a list with two values to set a time range (for example ["14d", "7d"]).
- **timestamp**: Restrict the results by the timestamp (last edit). Any event with a timestamp newer than the given timestamp will be returned. In case you are dealing with /attributes as scope, the attribute's timestamp will be used for the lookup. The input can be a timestamp or a short-hand time description (7d or 24h for example). You can also pass a list with two values to set a time range (for example ["14d", "7d"]).
- **published**: Set whether published or unpublished events should be returned. Do not set the parameter if you want both.
- **enforceWarninglist**: Remove any attributes from the result that would cause a hit on a warninglist entry.
- **to_ids**: By default (0) all attributes are returned that match the other filter parameters, regardless of their to_ids setting. To restrict the returned data set to to_ids only attributes set this parameter to 1. You can only use the special "exclude" setting to only return attributes that have the to_ids flag disabled.
- **deleted**: Default value 0. If set to 1, only deleted attributes will be returned. If set to [0,1] , both deleted and non-deleted attributes will be returned.
- **includeEventUuid**: Instead of just including the event ID, also include the event UUID in each of the attributes.
- **event_timestamp**: Only return attributes from events that have received a modification after the given timestamp. The input can be a timestamp or a short-hand time description (7d or 24h for example). You can also pass a list with two values to set a time range (for example ["14d", "7d"]).
- **sgReferenceOnly**: If this flag is set, sharing group objects will not be included, instead only the sharing group ID is set.
- **eventinfo**: Filter on the event's info field.
- **searchall**: Search for a full or a substring (delimited by % for substrings) in the event info, event tags, attribute tags, attribute values or attribute comment fields.
- **attackGalaxy**: Select the ATT&CK matrix like galaxy to use when using returnFormat = attack. Defaults to the Mitre ATT&CK library via mitre-attack-pattern.
- **order**: Only available for /events/restSearch. Sorts the results, can be useful in combination with limit. The accepted values to sort on are "Event.[any_field_in_the_events_table] [asc|desc]". You can also sort on multiple columns, see example below.

```
{
  "returnFormat": "json",
  "limit": "3",
  "order": "Event.attribute_count desc, Event.date desc"
}
```

Events management

/events

Accepted Methods

- GET
- POST
- PUT
- DELETE

Description

Receive, update or delete Events. There is also a good amount of special output formats that can be triggered.

GET /events

Description

Receive events based on criteria

URL Arguments

- event_id: Event id to receive
- event_uuid : Event uuid to receive

Output

```
[{"id":"1","org_id":"1","date":"2014-12-10","info":"OSINT - F-Secure W32\Regin
```

Example

```
curl --header "Authorization: YOUR API KEY" --header "Accept: application/json"
```

POST /events

Example

```
curl -i -H "Accept: application/json" -H "content-type: application/json" -H "
```

That is how an event JSON object should look like

```
{ "Event": { "date": "2015-01-01", "threat_level_id": "1", "info": "testevent", "publish"
```

DELETE /events

Description

Delete events based on criteria

URL Arguments

- event_id: Event id to receive
- event_uuid : Event uuid to receive

Output

```
{
  "name": "Event deleted.",
  "message": "Event deleted.",
  "url": "\/events\/delete\/1"
}
```

Example

curl --header "Authorization: YOUR [API KEY](#)" --header "Accept: application/json" -
-header "Content-Type: application/json" https://

```
curl --header "Authorization: YOUR API KEY " --header "Accept: application/json"
```

GET /events/index

Description

Return the event index. - Warning, there's a limit on the number of results

Output

```
[{"id": "1", "org_id": "1", "date": "2014-12-10", "info": "OSINT - F-Secure W32\Regin"
```

Example

```
curl --header "Authorization: YOUR API KEY " --header "Accept: application/json"
```

POST /events/AddTag

Add a tag or a tag collection to an existing event.

URL Arguments

- event (id)
- tag (id, name or collection_[collection_id])

Examples:

```
curl \
-d '{"event":"1210","tag":"t1p:green"}' \
-H "Authorization: YOUR API KEY" \
-H "Accept: application/json" \
-H "Content-type: application/json" \
-X POST https://192.168.0.223/events/addTag
```

```
curl \
-d '{"event":"1210","tag":"383"}' \
-H "Authorization: YOUR API KEY" \
-H "Accept: application/json" \
-H "Content-type: application/json" \
-X POST https://192.168.0.223/events/addTag
```

```
curl \
-d '{"event":"1210","tag":"collection_1"}' \
-H "Authorization: YOUR API KEY" \
-H "Accept: application/json" \
-H "Content-type: application/json" \
-X POST https://192.168.0.223/events/addTag
```

POST /events/removeTag

Remove a tag from an existing event. Note that removing a tag collection in one go is not possible.

URL Arguments

- event (id)
- tag (id, name).

Examples:

```
curl \
-d '{"event":"1210","tag":"t1p:amber"}' \
-H "Authorization: YOUR API KEY" \
-H "Accept: application/json" \
-H "Content-type: application/json" \
-X POST https://192.168.0.223/events/removeTag
```

```
curl \
-d '{"event": "1210", "tag": "987"}' \
-H "Authorization: YOUR API KEY" \
-H "Accept: application/json" \
-H "Content-type: application/json" \
-X POST https://192.168.0.223/events/removeTag
```

GET /events/pushEventToZMQ/

Description

Will [push](#) an Event to ZMQ

URL Arguments

- event_id

Example

```
curl --header "Authorization: YOUR API KEY" --header "Accept: application/json"
```

GET /events/nids NIDS rules export

Automatic export of all network related attributes is available under the Snort or Suricata rule format. Only published events and attributes marked as IDS Signature are exported.

You can configure your tools to automatically download the following file:

```
https://<misp url>/events/nids/suricata/download
https://<misp url>/events/nids/snort/download
```

The full [API](#) syntax is as follows:

```
https://<misp url>/events/nids/[format]/download/[eventid]/[frame]/[tags]/[from]
```

format

The export format, can be "suricata" or "snort"

eventid

Restrict the download to a single event

frame

Some commented out explanation framing the data. The reason to disable this would be if you would like to concatenate a list of exports from various select events in order to avoid unnecessary duplication of the comments.

tags

To include a tag in the results just write its names into this parameter. To exclude a tag prepend it with a '!'. You can also chain several tag commands together with the '&&' operator. Please be aware the colons (:) cannot be used in the tag search. Use semicolons instead (the search will automatically search for colons instead). For example, to include tag1 and tag2 but exclude tag3 you would use:

```
https://<misp url>/events/nids/snort/download/false/false/tag1&&tag2&&!tag3
```

from

Events with the date set to a date after the one specified in the from field (format: 2015-02-15). This filter will use the date of the event.

to

Events with the date set to a date before the one specified in the to field (format: 2015-02-15). This filter will use the date of the event.

last

Events published within the last x amount of time, where x can be defined in days, hours, minutes (for example 6d or 12h or 30m). This filter will use the published timestamp of the event.

The keywords false or null should be used for optional empty parameters in the URL.

An example for a Suricata export for all events excluding those tagged tag1, without all of the commented information at the start of the file would look like this:

```
https://<misp url>/events/nids/suricata/download/null/true/!tag1
```

Administration is able to maintain an allowedlist containing host, domain name and IP numbers to exclude from the [NIDS](#) export.

GET /events/hids Hash - HIDS database export

Automatic export of MD5/SHA1 checksums contained in file-related attributes. This list can be used to feed forensic software when searching for suspicious files. Only published events and attributes marked as IDS Signature are exported.

You can configure your tools to automatically download all the MD5 hashes from MISP:

```
https://<misp url>/events/hids/md5/download
```

Or the SHA1 hashes:

```
https://<misp url>/events/hids/sha1/download
```

The [API](#)'s full format is as follow:

```
https://<misp url>/events/hids/[format]/download/[tags]/[from]/[to]/[last]
```

format

The export format, can be "md5" or "sha1"

tags

To include a tag in the results just write its names into this parameter. To exclude a tag prepend it with a '!'. You can also chain several tag commands together with the '&&' operator. Please be aware the colons (:) cannot be used in the tag search. Use semicolons instead (the search will automatically search for colons instead). For example, to include tag1 and tag2 but exclude tag3 you would use:

```
https://<misp url>/events/hids/md5/download/tag1&&tag2&&!tag3
```

from

Events with the date set to a date after the one specified in the from field (format: 2015-02-15). This filter will use the date of the event.

to

Events with the date set to a date before the one specified in the to field (format: 2015-02-15). This filter will use the date of the event.

last

Events published within the last x amount of time, where x can be defined in days, hours, minutes (for example 5d or 12h or 30m). This filter will use the published timestamp of the event.

The keywords false or null should be used for optional empty parameters in the URL.

For example, to only show sha1 values from events tagged tag1, use:

```
https://<misp url>/events/hids/sha1/download/tag1
```

GET /events/stix STIX export

You can export MISP events in MITRE's STIX format (to read more about [STIX](#)). The STIX XML export is currently very slow and can lead to timeouts with larger events or collections of events. The STIX JSON return format does not suffer from this issue.

Usage of the [API](#):

```
https://<misp url>/events/stix/download
```

Search parameters can be passed to the function via URL parameters or by POSTing an xml or json object (depending on the return type). The following parameters can be passed to the STIX export tool: id, withAttachments, tags. Both id and tags can use the && (and) and ! (not) operators to build queries. Using the URL parameters, the syntax is as follows:


```
https://<misp url>/events/stix/download/[id]/[withAttachments]/[tags]/[from]/[to]/[last]
```

id

The event's ID

withAttachments

Encode attachments where applicable

tags

To include a tag in the results just write its names into this parameter. To exclude a tag prepend it with a '!'. You can also chain several tag commands together with the '&&' operator. Please be aware the colons (:) cannot be used in the tag search. Use semicolons instead (the search will automatically search for colons instead).

For example, to include tag1 and tag2 but exclude tag3 you would use:

```
https://<misp url>/events/stix/download/false/true/tag1&&tag2&&!tag3
```

from

Events with the date set to a date after the one specified in the from field (format: 2015-02-15). This filter will use the date of the event.

to

Events with the date set to a date before the one specified in the to field (format: 2015-02-15). This filter will use the date of the event.

last

Events published within the last x amount of time, where x can be defined in days, hours, minutes (for example 5d or 12h or 30m). This filter will use the published timestamp of the event.

You can post an XML or JSON object containing additional parameters in the following formats.

If you use JSON query objects:

```
https://<misp url>/events/stix/download.json
```

```
{"request": {"id": ["!51", "!62"], "withAttachment": false, "tags": ["APT1", "!OSINT"]}}
```

If you use XML query objects:

```
https://<misp url>/events/stix/download
```

```
<request><id>!51</id><id>!62</id><withAttachment>false</withAttachment><tags>APT1</tags></request>
```

Various ways to narrow down the search results of the STIX export

For example, to retrieve all events tagged "APT1" but excluding events tagged "OSINT" and excluding events #51 and #62 without any attachments:

```
https://<misp url>/events/stix/download/!51&&!62/false/APT1&&!OSINT/2015-02-15
```

To export the same events using a POST request use:

```
https://<misp url>/events/stix/download.json
```

Together with this JSON object in the POST message:

```
{"request": {"id": ["!51", "!62"], "tags": ["APT1", "!OSINT"], "from": "2015-02-15"}}
```

XML is automatically assumed when using the STIX export:

```
https://<misp url>/events/stix/download
```

The same search could be accomplished using the following POSTed XML object (note that ampersands need to be escaped, or alternatively separate id and tag elements can be used):

```
<request><id>!51</id><id>!62</id><tags>APT1</tags><tags>!OSINT</tags><from>2015
```

Tag management

POST /tags/add

Description

Add a tag on the instance

URL Arguments

Mandatory

- name

Optional

- colour : A valid hexadecimal colour, for example #51961a, if not set, a random colour is chosen
- exportable : whether the tag is exported when synchronising with other instances, default true

- `hide_tag` : if set, the tag will not be selectable, default false
- `org_id` : if set, only users from this organisation will be able to add the tag to objects
- `user_id` : if set, only this user will be able to add the tag to objects

Example

```
curl \
-d '{"name":"tag_only_name"}' \
-H "Authorization: YOUR API KEY" \
-H "Accept: application/json" \
-H "Content-type: application/json" \
-X POST https://192.168.0.223/tags/add
```

```
curl \
-d '{"name":"tag_doc","colour":"#51961a","exportable":1,"hide_tag":0,"org_
-H "Authorization: YOUR API KEY" \
-H "Accept: application/json" \
-H "Content-type: application/json" \
-X POST https://192.168.0.223/tags/add
```

POST /tags/attachTagToObject

Description

Attaches a tag to an object by a given UUID. Note that adding a tag collection via this endpoint is not possible. Please refer to `/events/addTag` and `/attributes/addTag` for that functionality.

This endpoint exists for convenience reasons and might be slightly less performant than `/events/addTag` and `/attributes/addTag`.

URL Arguments

- UUID
- tag (as id or name)

Response

```
{
  "name": "Tag tlp3Awhite(7) successfully attached to Attribute(153).",
  "message": "Tag tlp3Awhite(7) successfully attached to Attribute(153).",
  "url": "\tags\attachTagToObject"
}
```

Example

```
curl --header "Authorization: YOUR API KEY" --header "Accept: application/json"
```

```
curl --header "Authorization: YOUR API KEY " -d '{"uuid":"5a0d68b3-6da0-4ced-82
```

```
curl \
-d '{"uuid":"e76949e6-5ccb-4483-bef2-0e4cac73d236","tag":"6"}' \
-H "Authorization: YOUR API KEY" \
-H "Accept: application/json" \
-H "Content-type: application/json" \
-X POST https://192.168.0.223/tags/attachTagToObject
```

POST /tags/removeTagFromObject

Description

Removes a tag from an object (attribute or event) with given UUID.

This endpoint exists for convenience reasons and might be slightly less performant than /events/removeTag and /attributes/removeTag.

URL Arguments

- UUID
- tag (as id or name)

Response

```
{
  "name": "Tag tlp3Awhite(7) successfully removed from Attribute(153).",
  "message": "Tag tlp3Awhite(7) successfully removed from Attribute(153).",
  "url": "\tags\removeTagFromObject"
}
```

Example

```
curl --header "Authorization: YOUR API KEY " --header "Accept: application/json
```

```
curl \
-d '{"uuid":"85752e06-7644-40c8-8190-f8bbe9e7b2c7","tag":"tlp:white"}' \
-H "Authorization: YOUR API KEY" \
-H "Accept: application/json" \
-H "Content-type: application/json" \
-X POST https://192.168.0.223/tags/removeTagFromObject
```

```
curl \
-d '{"uuid":"85752e06-7644-40c8-8190-f8bbe9e7b2c7","tag":7}' \
-H "Authorization: YOUR_API_KEY" \
-H "Accept: application/json" \
-H "Content-type: application/json" \
-X POST https://192.168.0.223/tags/removeTagFromObject
```

GET /tags/tagStatistics/

Description

Will give an overview of the used attribute tags

Output

```
{
  "tags": {
    "Type:OSINT": "1",
    "tlp:white": "1",
    "osint:source-type=\"technical-report\"": "1",
    "misp-galaxy:threat-actor=\"Lazarus Group\"": "1",
    "misp-galaxy:rat=\"FALLCHILL\"": "1"
  },
  "taxonomies": []
}
```

Example

```
curl --header "Authorization: YOUR_API_KEY " --header "Accept: application/json"
```

Attribute management

POST /attributes/add/

Adds an Attribute to an event

URL Arguments

- event id

Output

Example

```
curl --header "Authorization: YOUR_API_KEY " --header "Accept: application/json"
```

GET /attributes

Get an attribute

URL Arguments

- attribute uuid

URL Attributes

Output

```
{ "Attribute": { "id": "39", "event_id": "1", "object_id": "0", "object_relation": null, "
```

Example

```
curl --header "Authorization: YOUR API KEY " --header "Accept: application/json"
```

POST /attributes/delete/

Description

Delete attributes.

URL Arguments

- attribute uuid
- attribute id
- attribute id/1 <-- hard delete

Output

```
{ "message": "Attribute deleted." }
```

Example

```
curl -X POST --header "Authorization: YOUR API KEY" --header "Accept: application/json"
```

```
curl -X POST --header "Authorization: YOUR API KEY " --header "Accept: application/json"
```

Hard delete:

```
curl -X POST --header "Authorization: YOUR API KEY" --header "Accept: applicat:
```

POST /attributes/addTag

Add a tag or a tag collection to an existing attribute.

URL Arguments

- attribute (id)
- tag (id, name or collection_[collection_id])

Examples:

```
curl \
-d '{"attribute":"256919","tag":"t1p:green"}' \
-H "Authorization: YOUR API KEY" \
-H "Accept: application/json" \
-H "Content-type: application/json" \
-X POST https://192.168.0.223/attributes/addTag
```

```
curl \
-d '{"attribute":"256919","tag":"987"}' \
-H "Authorization: YOUR API KEY" \
-H "Accept: application/json" \
-H "Content-type: application/json" \
-X POST https://192.168.0.223/attributes/addTag
```

```
curl \
-d '{"attribute":"256919","tag":"collection_1"}' \
-H "Authorization: YOUR API KEY" \
-H "Accept: application/json" \
-H "Content-type: application/json" \
-X POST https://192.168.0.223/attributes/addTag
```

POST /attributes/removeTag

Remove a tag from an existing event. Note that removing a tag collection in one go is not possible.

URL Arguments

- attribute (id)
- tag (id, name).

Examples:

```
curl \
-d '{"event":"1210","tag":"t1p:amber"}' \
-H "Authorization: YOUR API KEY" \
-H "Accept: application/json" \
-H "Content-type: application/json" \
-X POST https://192.168.0.223/events/removeTag
```

```
curl \
-d '{"event":"1210","tag":"987"}' \
-H "Authorization: YOUR API KEY" \
-H "Accept: application/json" \
-H "Content-type: application/json" \
-X POST https://192.168.0.223/events/removeTag
```

GET /attributes/attributeStatistics

Description

Will give an overview of the used attribute types

Output

```
{
  "attachment": "1",
  "comment": "1",
  "filename": "2",
  "float": "2",
  "ip-dst": "90",
  "ip-dst|port": "3",
  "link": "3",
  "md5": "16",
  "port": "3",
  "sha1": "2",
  "sha256": "2",
  "size-in-bytes": "1",
  "ssdeep": "2"
}
```

Example

```
curl --header "Authorization: YOUR API KEY " --header "Accept: application/json"
```

GET /attributes/describeTypes Describe types API

MISP can procedurally describe all attribute types and attribute categories it currently supports including the category - type mappings. To access this information simply send a GET request to:

Example

```
https://<misp url>/attributes/describeTypes
```

Depending on the headers passed the returned data will be a JSON object or an XML, with 3 main sections: types, categories, category_type_mappings.

POST /attributes/restSearch

Do not use this function with GET!

Parameters

- **returnFormat**: The format to return data in. Allowed formats:
 - **attack-sightings**: Returns ATTA&CK Sightings in json format for attributes with mitre-attack-pattern galaxies attached. For further details on the ATT&CK Sightings, please visit the related [MITRE website page](#).
 - **cache**: Hashes the attributes and returns them as txt. A hashing algorithm can be chosen by also adding the hash_type parameter. Supported hashing algorithms can be found on the [PHP website](#).
 - **count**: Returns the attribute count as txt.
 - **csv**
 - **hashes**: Returns hash attributes in txt format. For composite attributes, only the hash part is returned.
 - **json**
 - **netfilter**: Returns netfilter rules for IPs. Action can be set with the netfilter_action parameter. The default action is DROP.
 - **opendata**: Please refer to the related MISP project [blog post](#).
 - **openioc**
 - **rpz**
 - **snort**
 - **suricata**
 - **text**: Returns only the attribute values in text format.
 - **xml**
 - **yara**:
 - **yara-json**
- **value**: Search for the given value in the attributes' value field.
- **type**: The attribute type, any valid [MISP attribute](#) type is accepted.
- **category**: The attribute category, any valid [MISP attribute](#) category is accepted.
- **org**: Search by the creator organisation by supplying the organisation identifier.
- **tags**: Include or exclude attributes with certain tags. See example below. It is strongly recommended to specifically exclude the tags you want to avoid, even if the tags should be exclusive, for example tlp:red and tlp:green.

```
{
  "returnFormat": "json",
  "tags": {
    "NOT": [
      "tlp:red"
    ],
    "OR": [
      "tlp:green"
    ]
  }
}
```

- **from**: Will return attributes from events with the date set to a date after the one specified in the from field (format: 2015-02-15).

- **to**: Will return attributes with the date set to a date before the one specified in the to field (format: 2015-02-15).
- **last**: **Deprecated!!!** (synonym for publish_timestamp) Restrict the results by the timestamp of the last publication of the event. Any attribute with a last publication timestamp newer than the given timestamp will be returned. The input can be a timestamp or a short-hand time description (7d or 24h for example). You can also pass a list with two values to set a time range (for example ["14d", "7d"]).
- **eventid**: The events that should be included / excluded from the search.
- **withAttachments**: If set, encodes the attachments / zipped malware samples as base64 in the data field within each attribute
- **uuid**: Restrict the results by uuid.
- **publish_timestamp**: Restrict the results by the timestamp of the last publication of the event. Any attribute with a last publication timestamp newer than the given timestamp will be returned. The input can be a timestamp or a short-hand time description (7d or 24h for example). You can also pass a list with two values to set a time range (for example ["14d", "7d"]).
- **published**: Set whether published or unpublished events should be returned. Do not set the parameter if you want both.
- **timestamp**: **Deprecated!!!** (synonym for attribute_timestamp) Restrict the results by the timestamp (last edit). Any attribute with a timestamp newer than the given timestamp will be returned. The input can be a timestamp or a short-hand time description (7d or 24h for example). You can also pass a list with two values to set a time range (for example ["14d", "7d"]).
- **enforceWarninglist**: Remove any attributes from the result that would cause a hit on a warninglist entry.
- **to_ids**: By default (0) all attributes are returned that match the other filter parameters, irregardless of their to_ids setting. To restrict the returned data set to to_ids only attributes set this parameter to 1. You can only use the special "exclude" setting to only return attributes that have the to_ids flag disabled.
- **deleted**: Default value 0. If set to 1, only deleted attributes will be returned. If set to [0,1] , both deleted and non-deleted attributes will be returned.
- **includeEventUuid**: Instead of just including the event ID, also include the event UUID in each of the attributes.
- **event_timestamp**: Only return attributes from events that have received a modification after the given timestamp. The input can be a timestamp or a short-hand time description (7d or 24h for example). You can also pass a list with two values to set a time range (for example ["14d", "7d"]).
- **threat_level_id**: Only return attributes of events with the given threat level id(s). 1 = High, 2 = Medium, 3=Low, 4 = Undefined. See example below.

```
{
  "returnFormat": "json",
  "threat_level_id": [1,2]
}
```

- **includeEventTags**: If set to 1, the event tags of the event the attribute belongs to will be added to the attribute.
- **limit**: Limit the number of results returned, for example 10 attributes.

- **page:** If a limit is set, sets the page to be returned. page 3, limit 100 will return records 201->300).
- **requested_attributes:** Only for CSV export. Choose the fields you want in the csv output. Available fields are (*non-exhaustive list, more fields can be available depending on the values of other parameters*):
 - uuid
 - event_id
 - category
 - type
 - value
 - comment
 - to_ids
 - date
 - object_relation
 - attribute_tag
 - object_uuid
 - object_name
 - object_meta_category
 - event_info. Only available if includeContext parameter is set to 1.
 - event_member_org. Only available if includeContext parameter is set to 1.
 - event_source_org. Only available if includeContext parameter is set to 1.
 - event_distribution. Only available if includeContext parameter is set to 1.
 - event_threat_level_id. Only available if includeContext parameter is set to 1.
 - event_analysis. Only available if includeContext parameter is set to 1.
 - event_date. Only available if includeContext parameter is set to 1.
 - event_tag. Only available if includeContext parameter is set to 1.
 - event_timestamp. Only available if includeContext parameter is set to 1.
- **includeContext:** Adds extra event level context to the output. For each attribute more details are added to the Event object in the output. Please note that this significantly bloats the output data. Example below.

```

"Event": {
  "id": "31",
  "orgc_id": "1",
  "org_id": "1",
  "date": "2021-03-11",
  "threat_level_id": "1",
  "info": "Correlation 2",
  "published": true,
  "uuid": "0bfe7bf3-f793-4761-8450-8b30ca9d9964",
  "analysis": "0",
  "timestamp": "1616972381",
  "distribution": "1",
  "publish_timestamp": "1616972392",
  "sharing_group_id": "0",
  "extends_uuid": "",
  "Tag": [],
  "Orgc": {
    "id": "1",
    "name": "SHARINGORG",
    "uuid": "26867ddf-5a9b-4af0-b552-e4020a913b95",
    "local": true
  }
}

```

- **headerless**: Only for CSV export. The CSV created when this setting is set to true will not contain the header row.
- **includeWarninglistHits**: Adds a warnings block to an attribute if it has warninglist hits. See example below.

```

"warnings": [
  {
    "match": "10.0.0.0/8",
    "value": "10.0.0.1",
    "warninglist_name": "List of RFC 5735 CIDR blocks",
    "warninglist_id": "46"
  },
  {
    "match": "10.0.0.0/8",
    "value": "10.0.0.1",
    "warninglist_name": "List of RFC 1918 CIDR blocks",
    "warninglist_id": "44"
  }
]

```

- **object_relation**: Search on the object_relation field of attributes. You can search for 'malware-sample' attributes of file objects for example. Searching for multiple values at the same time is possible as well.

```

{
  "returnFormat": "json",
  "object_relation": ["malware-sample", "institution-name"]
}

```

- **includeSightings**: Adds a list of sightings for attributes that have sightings. See example below.

```

"Sighting": [
  {
    "id": "1",
    "attribute_id": "29",
    "event_id": "31",
    "org_id": "1",
    "date_sighting": "1617017091",
    "uuid": "48d21518-6b2a-4615-8c4e-91f8e4f08fe7",
    "source": "",
    "type": "0",
    "attribute_uuid": "b3c25257-7f47-41af-a29b-89188e583b5c",
    "Organisation": {
      "id": "1",
      "uuid": "26867ddf-5a9b-4af0-b552-e4020a913b95",
      "name": "SHARINGORG"
    }
  }
]

```

- **includeCorrelations:** Adds a list of correlated attributes for attributes that have correlations. See example below.

```

"RelatedAttribute": [
  {
    "id": "31",
    "event_id": "30",
    "object_id": "0",
    "object_relation": null,
    "category": "Network activity",
    "type": "ip-dst",
    "uuid": "f3b54c94-89ff-4fcf-9f47-52f70c6540b8",
    "timestamp": "1616961683",
    "distribution": "5",
    "sharing_group_id": "0",
    "to_ids": false,
    "comment": "",
    "value": "10.0.0.1",
    "Event": {
      "id": "30",
      "uuid": "8cca9f2f-9281-49fd-9b30-e16a8dbf6855",
      "threat_level_id": "1",
      "analysis": "0",
      "info": "Correlation 1",
      "extends_uuid": "",
      "distribution": "1",
      "sharing_group_id": "0",
      "published": false,
      "date": "2021-03-11",
      "orgc_id": "1",
      "org_id": "1"
    }
  }
]

```

- **includeDecayScore:** If set to 1, decay score information will be included for attributes that are affected by decaying. See example below. Note that includeEventTags will be set to 1 automatically if includeDecayScore is true.

```

"decay_score": [
  {
    "score": 77.40239901751683,
    "base_score": 80,
    "decayed": false,
    "DecayingModel": {
      "id": "2",
      "name": "NIDS Simple Decaying Model"
    }
  }
],

```

- **decayingModel:** Allows you to set the decaying model(s) to use to calculate the decay score. You can use a model that is not enabled. The value should be set to the id of the model. If this value is not set, a decay score entry will be added for all enabled decaying models that apply to the attribute type.
- **excludeDecayed:** Filter out all expired IOCs. Note that includeDecayScore will be set to 1 automatically if excludeDecayed is true.
- **modelOverrides:** JSON that can be used to modify Model parameters on-the-fly. Example can be found below.

```

{
  "type": "ip-src",
  "tags": ["tlp:", "phishing:"],
  "includeDecayScore": 1,
  "excludeDecayed": 1,
  "modelOverrides": {
    "threshold": 30
  }
  "decayingModel": [84, 12],
}

```

- **includeFullModel:** If set to 1, includes the full decaying model details instead of just the id and name.
- **score:** Overrides the model threshold value with the one you set. This means attributes for which the decay score calculated for all relevant models is lower than this value, will be considered decayed.
- **attribute_timestamp:** Restrict the results by the timestamp (last edit). Any attribute with a timestamp newer than the given timestamp will be returned. The input can be a timestamp or a short-hand time description (7d or 24h for example). You can also pass a list with two values to set a time range (for example ["14d", "7d"]).
- **first_seen:** Restrict the results by the first_seen timestamp of the attribute. Any attribute with a first_seen timestamp newer than the given timestamp will be returned. The input can be a timestamp or a short-hand time description (7d or 24h for example). You can also pass a list with two values to set a time range (for example ["14d", "7d"]).
- **last_seen:** Restrict the results by the last_seen timestamp of the attribute. Any attribute with a first_seen timestamp newer than the given timestamp will be returned. The input can be a timestamp or a short-hand time description (7d or 24h for example). You can also pass a list with two values to set a time range (for example ["14d", "7d"]).

- **searchall**: Search for a full or a substring (delimited by % for substrings) in the attribute tags, attribute values or attribute comment fields.

Example

```
curl \
-d '{"returnFormat":"json","value":"foobar"}' \
-H "Authorization: YOUR API KEY" \
-H "Accept: application/json" \
-H "Content-type: application/json" \
-X POST https://192.168.0.220/attributes/restSearch
```

```
{"response": {"Attribute": [{"id":"44","event_id":"30","object_id":"0","object_
```

Objects management

POST /objects/delete/[object_id]/[hard_delete]

Description

Delete an object.

URL Arguments

- **object_id** : mandatory
- **hard_delete** : if set to 1 or true, the object will be hard deleted. Defaults to false.

Example

```
curl \
-d '{}' \
-H "Authorization: YOUR API KEY" \
-H "Accept: application/json" \
-H "Content-type: application/json" \
-X POST https://192.168.0.223/objects/delete/18732/1
```

Server management

GET /servers/getPyMISPVersion

Result

```
{"version":"2.4.85"}
```

Example

```
curl --header "Authorization: YOUR API KEY " --header "Accept: application/json"
```

GET /servers/getVersion

Result

```
{"version":"2.4.85","perm_sync":true}
```

Example

```
curl --header "Authorization: YOUR API KEY " --header "Accept: application/json"
```

Sightings

POST /sightings/add/

- attribute_id
- attribute_uuid

The different sightings types are:

```
0 => 'sighting',
1 => 'false-positive',
2 => 'expiration'
```

User management

MISP allows administrators to create and manage users via its REST [API](#)

```
https://<misp url>/admin/users/view/[user id]
```

POST /admin/users/add

To create a new user, send a POST request to:

Sample input

```
{
  "email":"andras.iklody@circl.lu",
  "org_id":1,
  "role_id":1
}
```

To view the mandatory and optional fields, use a GET request on the above URL.

Sample output

```
{
  "name": "\\admin\\users\\add API description",
  "description": "POST a User object in JSON format to this API to create a user",
  "mandatory_fields": [
    "email",
    "org_id",
    "role_id"
  ],
  "optional_fields": [
    "password",
    "external_auth_required",
    "external_auth_key",
    "enable_password",
    "nids_sid",
    "server_id",
    "pgpkey",
    "certif_public",
    "autoalert",
    "contactalert",
    "disabled",
    "change_pw",
    "termsaccepted",
    "newsread"
  ],
  "url": "\\admin\\users\\add"
}
```

POST admin/users/edit/

To edit an existing user send a POST request to:

```
https://<misp url>/admin/users/edit/[user id]
```

Only the fields POSTed will be updated, the rest is left intact. To view all possible parameters, simply send a GET request to the above URL.

POST admin/users/delete/

You can also delete users by POSTing to the below URL, but keep in mind that disabling users (by setting the disabled flag via an edit) is always preferred to keep user associations to events intact.

Parameters

- [user id]

Example

```
https://<misp url>/admin/users/delete/[user id]
```

GET admin/users

Description

Will output all users

Output

```
[
  {
    "User": {
      "id": "1",
      "password": "F0000000000",
      "org_id": "1",
      "server_id": "0",
      "email": "admin@admin.test",
      "autoalert": false,
      "authkey": "YOUR API KEY",
      "invited_by": "0",
      "pgpkey": null,
      "certif_public": "",
      "nids_sid": "4000000",
      "termsaccepted": true,
      "newsread": "0",
      "role_id": "1",
      "change_pw": "0",
      "contactalert": false,
      "disabled": false,
      "expiration": null,
      "current_login": "1515752313",
      "last_login": "1515748671",
      "force_logout": false,
      "date_created": null,
      "date_modified": null,
      "org_ci": "ORGNAME"
    },
    "Role": {
      "id": "1",
      "name": "admin",
      "perm_auth": true
    },
    "Organisation": {
      "id": "1",
      "name": "ORGNAME"
    }
  }
]
```

Example

```
curl --header "Authorization: YOUR API KEY " --header "Accept: application/json"
```

GET admin/users/view/

Description

Will return a single user. To view a user simply send a GET request.

Parameters

- id

Output

```
{
  "User": {
    "id": "1",
    "password": "*****",
    "org_id": "1",
    "server_id": "0",
    "email": "admin@admin.test",
    "autoalert": false,
    "authkey": "YOUR API KEY",
    "invited_by": "0",
    "gpgkey": null,
    "certif_public": "",
    "nids_sid": "4000000",
    "termsaccepted": true,
    "newsread": "0",
    "role_id": "1",
    "change_pw": "0",
    "contactalert": false,
    "disabled": false,
    "expiration": null,
    "current_login": "1515752313",
    "last_login": "1515748671",
    "force_logout": false,
    "orgAdmins": []
  }
}
```

Example

```
curl --header "Authorization: YOUR API KEY " --header "Accept: application/json"
```

POST admin/users/add/

Discussion API

If you would like to fetch a discussion thread including all of its posts, simply send a GET request to:

```
https://<misp url>/threads/view/<thread id>
```

Using the following headers:

```
Authorization: [Your auth key]
Content-type: application/json
Accept: application/json
```

To get all posts related to an event simply send a GET request to:

```
https://<misp url>/threads/viewEvent/<event id>
```

Organisation management

MISP allows administrators to create and manage organisations via its REST [API](#)

The [API](#) is available in JSON format so make sure you use the following headers:

```
Authorization: [Your auth key]
Content-type: application/json
Accept: application/json
```

To fetch all organisations send a GET request to:

```
https://<misp url>/organisations
```

To view an individual organisation, send a get request to:

```
https://<misp url>/organisations/view/id
```

The management of users happens via three apis:

```
https://<misp url>/admin/organisations/add
https://<misp url>/admin/organisations/edit/[org id]
https://<misp url>/admin/organisations/delete/[org id]
```

To delete an organisation simply send a POST or DELETE request to the above URL.

For creating or modifying an organisation, simply POST a JSON containing the relevant fields to the appropriate [API](#). The only mandatory field is the organisation name, with a host of optional parameters

An example for a simple organisation object:

```
{
  "name": "Blizzard",
  "nationality": "US"
}
```

Not setting a field will assume the default settings for the given field in the case of a new organisation whilst it would retain the existing setting for existing organisations. The above example would create the following object in MISP:

```
{
  "Organisation": {
    "id": "1108",
    "name": "Blizzard",
    "alias": "",
    "anonymise": false,
    "date_created": "2017-01-22 17:32:29",
    "date_modified": "2017-01-22 17:32:29",
    "description": "",
    "type": "",
    "nationality": "US",
    "sector": "",
    "created_by": "1",
    "uuid": "5884de9d-04f0-4d7d-bf15-0b88c0a83865",
    "contacts": "",
    "local": true,
    "landingpage": ""
  }
}
```

To query the add or edit APIs for the valid parameters, simply send a GET requests to either [API](#). The result currently looks like this (which might change when new fields are added):

```
{
  "name": "\\admin\\organisations\\add API description",
  "description": "POST an Organisation object in JSON format to this API to c",
  "mandatory_fields": [
    "name"
  ],
  "optional_fields": [
    "anonymise",
    "description",
    "type",
    "nationality",
    "sector",
    "uuid",
    "contacts",
    "local"
  ],
  "url": "\\admin\\organisations\\add"
}
```

Special Cases

XML Export

An automatic export of all events and attributes (except file attachments) is available under a custom XML format.

You can configure your tools to automatically download the following file:

```
https://<misp url>/events/xml/download
```

If you only want to fetch a specific event append the eventid number:

```
https://<misp url>/events/xml/download/1
```

You can post an XML or JSON object containing additional parameters in the JSON query format or XML query format. Query parameters provide a way to filter the output to specific parameters.

JSON query format

The URL is appended with json:

```
https://<misp url>/events/xml/download.json
```

The query parameters can be the following:

```
{"request": {"eventid":["!51","!62"],"withAttachment":false,"tags":["APT1","!OS
```

XML query format

The URL is path is:

```
https://<misp url>/events/xml/download
```

The query parameters can be the following:

```
<request><eventid>!51</eventid><eventid>!62</eventid><withAttachment>false</wi
```

XML download and URL parameters

The XML download also accepts two additional the following optional parameters in the url:

```
https://<misp url>/events/xml/download/[eventid]/[withattachments]/[tags]/[from
```

eventid

Restrict the download to a single event

withattachments

A boolean field that determines whether attachments should be encoded and a second parameter that controls the eligible tags.

tags

To include a tag in the results just write its names into this parameter. To exclude a tag prepend it with a '!'. You can also chain several tag commands together with the '&&' operator. Please be aware the colons (:) cannot be used in the tag search. Use semicolons instead (the search will automatically

search for colons instead). For example, to include tag1 and tag2 but exclude tag3 you would use:

```
https://<misp url>/events/xml/download/false/true/tag1&&tag2&&!tag3
```

from

Events with the date set to a date after the one specified in the from field (format: 2015-02-15). This filter will use the date of the event.

to

Events with the date set to a date before the one specified in the to field (format: 2015-02-15). This filter will use the date of the event.

last

Events published within the last x amount of time, where x can be defined in days, hours, minutes (for example 5d or 12h or 30m). This filter will use the published timestamp of the event.

The keywords false or null should be used for optional empty parameters in the URL. Also check out the User Guide to read about the [REST API](#).

CSV export

An automatic export of attributes is available as CSV. Only attributes that are flagged "to_ids" will get exported.

You can configure your tools to automatically download the following file:

```
https://<misp url>/events/csv/download
```

This will download all the valid attributes in your [MISP instance](#) (might take some time).

You can also configure your tools to download the attributes from a specific event. Here is the old legacy CSV export that will work like exporting all attributes:

```
https://<misp url>/events/csv/download/<event-id>
```

You can specify additional flags for CSV exports as follows:

POST to:

```
https://<misp url>/events/csv/download
```

Headers:

```
Authorization: <your auth key>
Content-type: application/json
```

Body:

```
{ "parameter1": "value1", "parameter2": 1, "parameter3": ["value3", "value4", "!va
```

eventid

Restrict the download to a single event

ignore

Setting this flag to true will include attributes that are not marked "to_ids".

tags

Simply add a list of tags that should be included or negated (by prepending the tag name with a "!"). Any event with a negated tag will be ignored, even if an included tag is matching. An example is included further down.

category

The attribute category, any valid [MISP attribute](#) category is accepted.

type

The attribute type, any valid [MISP attribute](#) type is accepted.

includeContext

Include the event data with each attribute.

from

Events with the date set to a date after the one specified in the from field (format: 2015-02-15). This filter will use the date of the event.

to

Events with the date set to a date before the one specified in the to field (format: 2015-02-15). This filter will use the date of the event.

last

Events published within the last x amount of time, where x can be defined in days, hours, minutes (for example 5d or 12h or 30m). This filter will use the published timestamp of the event.

For example, to only download a csv generated of the "domain" type and the "Network activity" category attributes all events except for the one and further restricting it to events that are tagged "tag1" or "tag2" but not "tag3", only allowing attributes that are IDS flagged use the following syntax:

POST to:

```
https://<misp url>/events/csv/download
```

Headers:

```
Authorization: <your auth key>
Content-type: application/json
```

Body:


```
{ "tags": ["tag1", "tag2", "!tag3"], "category": "Network activity", "type": "domain" }
```

Alternatively you can fall back to the deprecated syntax of passing parameters in a GET request via the URL, however this is discouraged:

```
https://<misp url>/events/csv/download/[eventid]/[ignore]/[tags]/[category]/[type]
```

If you use the deprecated URL parameter method, keep in mind that the keywords false or null should be used for optional empty parameters. To export the attributes of all events that are of the type "domain", use the following syntax:

```
https://<misp url>/events/csv/download/false/false/false/false/domain
```

Update 2.4.82

Since version 2.4.82, the new export format allows to select more columns using the following query format:

```
https://<misp-instance>/events/csv/download/<event-id>?attributes=timestamp,type
```

The order of columns will be honoured including those related to object level information.

To select object level columns, simply prepend the given object column's name by object_, such as:

```
https://<misp-instance>/events/csv/download/<event-id>?attributes=timestamp,type,object_uuid,object_name
```

The following columns will be returned (all columns related to objects will be prefixed with object_):

```
timestamp,type,uuid,value,object_uuid,object_name
```

includeContext option includes the tags for the event for each line.

RPZ export

You can export RPZ zone files for DNS level firewall by using the RPZ export functionality of MISP. The file generated will include all of the IDS flagged domain, hostname and IP-src/IP-dst attribute values that you have access to.

It is possible to further restrict the exported values using the following filters:

tags

To include a tag in the results just write its names into this parameter. To exclude a tag prepend it with a '!'. You can also chain several tag commands together with the '&&' operator. Please be aware the colons (:) cannot be used in the tag search when passed through the URL. Use semicolons instead (the search will automatically search for colons instead).

id

The event's ID

from

Events with the date set to a date after the one specified in the from field (format: 2015-02-03)

to

Events with the date set to a date before the one specified in the to field (format: 2015-02-03)

MISP will inject header values into the zone file as well as define the action taken for each of the values that can all be overwritten. By default these values are either the default values shipped with the application, or ones that are overwritten by your site administrator. The values are as follows:

Value name	Default value
RPZ_policy	DROP
RPZ_walled_garden	127.0.0.1
RPZ_serial	\$date00
RPZ_refresh	2h
RPZ_retry	30m
RPZ_expiry	30d
RPZ_minimum_ttl	1h
RPZ_ttl	1w
RPZ_ns	localhost.
RPZ_ns_alt	
RPZ_email	root.localhost

To override the above values, either use the URL parameters as described below:

```
https://<misp url>/attributes/rpz/download/[tags]/[eventId]/[from]/[to]/[policy]  
um_ttl]/[ttl]
```

Or POST an XML or JSON object with the above listed options:

```
<request><tags>OSINT&&!OUTDATED</tags><policy>walled-garden</policy><walled_ga
```

```
{"request": {"tags": ["OSINT", "!OUTDATED"], "policy": "walled-garden", "walleo
```

Text export

An export of all attributes of a specific type to a plain text file. By default only published and IDS flagged attributes are exported.

You can configure your tools to automatically download the following files:

```
https://<misp url>/attributes/text/download/md5
https://<misp url>/attributes/text/download/sha1
https://<misp url>/attributes/text/download/sha256
https://<misp url>/attributes/text/download/filename
https://<misp url>/attributes/text/download/filename|md5
https://<misp url>/attributes/text/download/filename|sha1
https://<misp url>/attributes/text/download/filename|sha256
https://<misp url>/attributes/text/download/ip-src
https://<misp url>/attributes/text/download/ip-dst
https://<misp url>/attributes/text/download/hostname
https://<misp url>/attributes/text/download/domain
https://<misp url>/attributes/text/download/email-src
https://<misp url>/attributes/text/download/email-dst
https://<misp url>/attributes/text/download/email-subject
https://<misp url>/attributes/text/download/email-attachment
https://<misp url>/attributes/text/download/url
https://<misp url>/attributes/text/download/http-method
https://<misp url>/attributes/text/download/user-agent
https://<misp url>/attributes/text/download/regkey
https://<misp url>/attributes/text/download/regkey|value
https://<misp url>/attributes/text/download/AS
https://<misp url>/attributes/text/download/snort
https://<misp url>/attributes/text/download/pattern-in-file
https://<misp url>/attributes/text/download/pattern-in-traffic
https://<misp url>/attributes/text/download/pattern-in-memory
https://<misp url>/attributes/text/download/yara
https://<misp url>/attributes/text/download/vulnerability
https://<misp url>/attributes/text/download/attachment
https://<misp url>/attributes/text/download/malware-sample
https://<misp url>/attributes/text/download/link
https://<misp url>/attributes/text/download/comment
https://<misp url>/attributes/text/download/text
https://<misp url>/attributes/text/download/other
https://<misp url>/attributes/text/download/named pipe
https://<misp url>/attributes/text/download/mutex
https://<misp url>/attributes/text/download/target-user
https://<misp url>/attributes/text/download/target-email
https://<misp url>/attributes/text/download/target-machine
https://<misp url>/attributes/text/download/target-org
https://<misp url>/attributes/text/download/target-location
https://<misp url>/attributes/text/download/target-external
```

To restrict the results by tags, use the usual syntax. Please be aware the colons (:) cannot be used in the tag search. Use semicolons instead (the search will automatically search for colons instead). To get ip-src values from events tagged tag1 but not tag2 use:

```
https://<misp url>/attributes/text/download/ip-src/tag1&&
```

It is possible to restrict the text exports on additional flags. The first allows the user to restrict based on event ID, whilst the second is a boolean switch allowing non IDS flagged attributes to be exported. Additionally, choosing "all" in the type field will return all eligible attributes.

```
https://<misp url>/attributes/text/download/[type]/[tags]/[event_id]/[allowNonI
```

type

The attribute type, any valid [MISP attribute](#) type is accepted.

tags

To include a tag in the results just write its names into this parameter. To exclude a tag prepend it with a '!'. You can also chain several tag commands together with the '&&' operator. Please be aware the colons (:) cannot be used in the tag search. Use semicolons instead (the search will automatically search for colons instead).

allowNonIDS

Include attributes that would normally be excluded due to the IDS flag not being set or due to being allowlisted

from

Set the lowest "date" field value that should be included in the export (format YYYY-MM-DD)

to

Set the highest "date" field value that should be included in the export (format YYYY-MM-DD)

last

Set the timeframe of the export based on the "timestamp" value. The parameter uses a time + metric notation (valid examples: "2w", "60m", "24h")

For example, to include tag1 and tag2 but exclude tag3 you would use:

```
https://<misp url>/attributes/text/download/all/tag1&&tag2&&!tag3
```

event_id

Restrict the results to the given event IDs.

allowNonIDS

Allow attributes to be exported that are not marked as "to_ids".

from

Events with the date set to a date after the one specified in the from field (format: 2015-02-15). This filter will use the date of the event.

to

Events with the date set to a date before the one specified in the to field (format: 2015-02-15). This filter will use the date of the event.

last

Events published within the last x amount of time, where x can be defined in days, hours, minutes (for example 5d or 12h or 30m). This filter will use the published timestamp of the event.

The keywords false or null should be used for optional empty parameters in the URL.

For example, to retrieve all attributes for event #5, including non IDS marked attributes too, use the following line:

```
https://<misp url>/attributes/text/download/all/null/5/true
```

RESTful searches with XML result export

It is possible to search the database for attributes based on a list of criteria.

To return an event with all of its attributes, relations, shadowAttributes, use the following syntax:

```
https://<misp url>/events/restSearch/download/[value]/[type]/[category]/[org]/
```

value

Search for the given value in the attributes' value field.

type

The attribute type, any valid [MISP attribute](#) type is accepted.

category

The attribute category, any valid [MISP attribute](#) category is accepted.

org

Search by the creator organisation by supplying the organisation identifier.

tags

To include a tag in the results just write its names into this parameter. To exclude a tag prepend it with a '!'. You can also chain several tag commands together with the '&&' operator. Please be aware the colons (:) cannot be used in the tag search. Use semicolons instead (the search will automatically search for colons instead).

For example, to include tag1 and tag2 but exclude tag3 you would use:

```
https://<misp url>/events/restSearch/download/null/null/null/null/tag1&&tag2&&
```

quickfilter

Enabling this (by passing "1" as the argument) will make the search ignore all of the other arguments, except for the auth key and value. MISP will return an xml / json (depending on the header sent) of all events that have a sub-string match on value in the event info, event org, or any of the attribute value1 / value2 fields, or in the attribute comment.

from

Events with the date set to a date after the one specified in the from field (format: 2015-02-15). This filter will use the date of the event.

to

Events with the date set to a date before the one specified in the to field (format: 2015-02-15). This filter will use the date of the event.

last

Events published within the last x amount of time, where x can be defined in days, hours, minutes (for example 5d or 12h or 30m). This filter will use the published timestamp of the event.

eventid

The events that should be included / excluded from the search

withAttachments

Include the attachments/encrypted samples in the export

metadata

Only fetch the event metadata (event data, tags, relations) and skip the attributes

limit

Limit the number of results returned; use together with page.

page

If a limit is set, sets the page to be returned, starting at 1; page 3, limit 100 will return records 201->300). When requesting a page beyond the number of available pages, the returned results list will be empty.

The keywords false or null should be used for optional empty parameters in the URL.

For example, to find any event with the term "red october" mentioned, use the following syntax (the example is shown as a POST request instead of a GET, which is highly recommended):

POST to:

```
https://<misp url>/events/restSearch/download
```

POST message payload (XML):

```
<request><value>red october</value><searchall>1</searchall><eventid>!15</eventid>
```

POST message payload (JSON):

```
{"request": {"value": "red october", "searchall": 1, "eventid": "!15"}}
```

To just return a list of attributes, use the following syntax:

value

Search for the given value in the attributes' value field.

type

The attribute type, any valid [MISP attribute](#) type is accepted.

category

The attribute category, any valid [MISP attribute](#) category is accepted.

org

Search by the creator organisation by supplying the organisation identifier.

tags

To include a tag in the results just write its names into this parameter. To exclude a tag prepend it with a '!'. You can also chain several tag commands together with the '&&' operator. Please be aware the colons (:) cannot be used in the tag search. Use semicolons instead (the search will automatically search for colons instead).

from

Events with the date set to a date after the one specified in the from field (format: 2015-02-15). This filter will use the date of the event.

to

Events with the date set to a date before the one specified in the to field (format: 2015-02-15). This filter will use the date of the event.

last

Events published within the last x amount of time, where x can be defined in days, hours, minutes (for example 5d or 12h or 30m). This filter will use the published timestamp of the event.

eventid

The events that should be included / excluded from the search.

uuid

The returned events must include an attribute with the given UUID, or alternatively the event's UUID must match the value(s) passed.

The keywords false or null should be used for optional empty parameters in the URL.

https://<misp url>/attributes/restSearch/download/[value]/[type]/[category]/[org]

Value, type, category and org are optional. It is possible to search for several terms in each category by joining them with the '&&' operator. It is also possible to negate a term with the '!' operator. Please be aware the colons (:) cannot be used in the tag search. Use semicolons instead (the search will automatically search for colons instead). For example, in order to search for all attributes created by your organisation that contain 192.168 or 127.0 but not 0.1 and are of the type ip-src, excluding the events that were tagged tag1 use the following syntax:

```
https://<misp url>/attributes/restSearch/download/192.168.1.1|ip-src/1
```

You can also use search for IP addresses using CIDR. Make sure that you use '|' (pipe) instead of '/' (slashes). Please be aware the colons (:) cannot be used in the tag search. Use semicolons instead (the search will automatically search for colons instead). See below for an example:

```
https://<misp url>/attributes/restSearch/download/192.168.1.1|16/ip-src/null/C:
```

Export attributes of event with specified type as XML

If you want to export all attributes of a pre-defined type that belong to an event, use the following syntax:

```
https://<misp url>/attributes/returnAttributes/download/[id]/[type]/[sigOnly]
```

sigOnly is an optional flag that will block all attributes from being exported that don't have the IDS flag turned on. It is possible to search for several types with the '&&' operator and to exclude values with the '!' operator. For example, to get all IDS signature attributes of type md5 and sha256, but not filename|md5 and filename|sha256 from event 25, use the following:

```
https://<misp url>/attributes/returnAttributes/download/25/md5&&sha256&&!filename
```

Filtering event metadata

As described in the REST section, it is possible to retrieve a list of events along with their metadata by sending a GET request to the /events [API](#). However, this [API](#) in particular is a bit more versatile. You can pass search parameters along to search among the events on various fields and retrieve a list of matching events (along with their metadata). Use the following URL:

```
https://<misp url>/events/index
```

POST a JSON object with the desired lookup fields and values to receive a JSON back. An example for a valid lookup:

```
Authorization: <your API key>
Accept: application/json
Content-type: application/json
```

Body:


```
{"searchinfo":"Locky", "searchpublished":1, "searchdistribution":0}
```

The list of valid parameters:

searchpublished:

Filters on published or unpulished events [0,1] - negatable

searchinfo:

Filters on strings found in the event info - negatable

searchtag:

Filters on attached tag names - negatable

searcheventid:

Filters on specific event IDs - negatable

searchthreatlevel:

Filters on a given event threat level [1,2,3,4] - negatable

searchdistribution:

Filters on the distribution level [0,1,2,3] - negatable

searchanalysis:

Filters on the given analysis phase of the event [0,1,2,3] - negatable

searchattribute:

Filters on a contained attribute value - negatable

searchorg:

Filters on the creator organisation - negatable

searchemail:

Filters on the creator user's email address (admin only) - negatable

searchDatefrom:

Filters on the date, anything newer than the given date in YYYY-MM-DD format is taken - non-negatable

searchDateuntil:

Filters on the date, anything older than the given date in YYYY-MM-DD format is taken - non-negatable

Download attachment or malware sample

If you know the attribute ID of a malware-sample or an attachment, you can download it with the following syntax:

```
https://<misp url>/attributes/downloadAttachment/download/[Attribute_id]
```

Download malware sample by hash

You can also download samples by knowing its MD5 hash. Simply pass the hash along as a JSON/XML object or in the URL (with the URL having overruling the passed objects) to receive a JSON/XML object back with the zipped sample base64 encoded along with some contextual information.

You can also use this [API](#) to get all samples from events that contain the passed hash. For this functionality, just pass the "allSamples" flag along. Note that if you are getting all samples from matching events, you can use all supported hash types (md5, sha1, sha256) for the lookup.

You can also get all the samples from an event with a given event ID, by passing along the eventID parameter. Make sure that either an event ID or a hash is passed along, otherwise an error message will be returned. Also, if no hash is set, the allSamples flag will get set automatically.

`https://attributes/downloadSample/[hash]/[allSamples]/[eventID]`

POST message payload (XML):

```
<request><hash>7c12772809c1c0c3deda6103b10fdfa0</hash><allSamples>1</allSamples>
```

POST message payload (json):

```
{"request": {"hash": "7c12772809c1c0c3deda6103b10fdfa0", "allSamples": 1, "eventID": null}}
```

A description of all the parameters in the passed object:

hash

A hash in MD5 format. If allSamples is set, this can be any one of the following: md5, sha1, sha256.

allSamples

If set, it will return all samples from events that have a match for the hash provided above.

eventID

If set, it will only fetch data from the given event ID.

Upload malware samples using the "Upload Sample" API

```
https://<misp url>/events/upload_sample/[Event_id]
```

This [API](#) will allow you to populate an event that you have modify rights to with malware samples (and all related hashes). Alternatively, if you do not supply an event ID, it will create a new event for you.

The files have to be base64 encoded and POSTed as explained below. All samples will be zipped and password protected (with the password being "infected"). The hashes of the original file will be captured as additional attributes.

For sample upload (for objects in general) there is no check for duplicates.

The event ID is optional. MISP will accept either a JSON or an XML object posted to the above URL.

The general structure of the expected objects is as follows:

```
{
  "request": {
    "files": [
      {
        "filename": filename1,
        "data": base64encodedfile1,
        "optional_parameter1": "optional_parameter1",
        "optional_parameter2": "optional_parameter2",
        "optional_parameter3": "optional_parameter3"
      }
    ]
  }
}
```

JSON:

```
{
  "request": {
    "files": [
      {
        "filename": "test1.txt",
        "data": "dGVzdA==",
        "optional_parameter1": "optional_parameter1",
        "optional_parameter2": "optional_parameter2",
        "optional_parameter3": "optional_parameter3"
      }
    ]
  }
}
```

XML:

```
<request>
  <files>
    <filename>test3.txt</filename>
    <data>dGVzdA==</data>
  </files>
  <optional_parameter1>optional_parameter1</optional_parameter1>
  <optional_parameter2>optional_parameter2</optional_parameter2>
  <optional_parameter3>optional_parameter3</optional_parameter3>
</request>
```

The following optional parameters are expected:

event_id

The Event's ID is optional. It can be either supplied via the URL or the POSTed object, but the URL has priority if both are provided. Not supplying an event ID will cause MISP to create a single new event for all of the POSTed malware samples. You can define the default settings for the event, otherwise a set of default settings will be used.

distribution

The distribution setting used for the attributes and for the newly created event, if relevant. [0-3]

to_ids

You can flag all attributes created during the transaction to be marked as "to_ids" or not.

category

The category that will be assigned to the uploaded samples. Valid options are: Payload delivery, Artifacts dropped, Payload Installation, External Analysis.

info

Used to populate the event info field if no event ID supplied. Alternatively, if not set, MISP will simply generate a message showing that it's a malware sample collection generated on the given day.

analysis

The analysis level of the newly created event, if applicable. [0-2]

threat_level_id: The threat level ID of the newly created event, if applicable.

[0-3]

comment

This will populate the comment field of any attribute created using this [API](#).

The **threat_level_id** is mapped as such:

```
0 = high
1 = medium
2 = low
3 = undefined
```

Proposals API

You can interact with the [proposals](#) via the [API](#) directly since version 2.3.148.

HTTP	URL	Explanation	E
GET	/shadow_attributes/view/[proposal_id]	View a proposal	N/A
POST	/shadow_attributes/add/[event_id]	Propose a new attribute to an event	Shadow object
POST	/shadow_attributes/edit/[attribute_id]	Propose an edit to an attribute	Shadow object
POST	/shadow_attributes/accept/[proposal_id]	Accept a proposal	N/A
POST	/shadow_attributes/discard/[proposal_id]	Discard a proposal	N/A

When posting a shadow attribute object, use the following format

JSON:

```
{ "request": { "ShadowAttribute": { "value": "5.5.5.5", "to_ids": false, "type": "ip-src" } } }
```

XML:

```
<request><ShadowAttribute><value>5.5.5.5</value><to_ids>0</to_ids><type>ip-src</type></ShadowAttribute></request>
```

None of the above fields are mandatory, but at least one of them has to be provided.

Sharing groups

MISP allows [sharing groups](#) to be retrieved via the [API](#).

```
https://<misp url>/sharing_groups/index.json
```

Based on the [API](#) key used, the list of visible [sharing groups](#) will be returned in a JSON file. The JSON includes the organization parts of a given sharing group along with the associated server.

Enable, disable and fetching feeds via the API

The [MISP feeds](#) can be enabled via the [API](#).

A feed can be enabled by POSTing on the following URL (feed_id is the id of the feed):

```
/feeds/enable/feed_id
```

A feed can be disabled by POSTing on the following URL (feed_id is the id of the feed):

```
/feeds/disable/feed_id
```

All feeds can be cached via the [API](#):

```
/feeds/cacheFeeds/all
```

or you can replace `all` by the feed format to fetch like `misp` or `freetext`. `all` can be replaced with the `id` value of the feed to fetch a specific feed.

To fetch a feed or all feeds:

```
/feeds/fetchFromFeed/feed_id  
/feeds/fetchFromAllFeeds
```

This [API](#) can be also used to download feeds at regular interval via cronjobs or alike.

Sightings API

MISP allows Sightings data to be conveyed in several ways.

The most basic way is to POST a blank message to the Sightings [API](#) with the attribute ID or attribute UUID. This will create a sightings entry with the creation of the entry as the timestamp for the organisation of the authenticated user.

```
https://<misp url>/sightings/add/[attribute_id]  
https://<misp url>/sightings/add/[attribute_uuid]
```

Alternatively, it is possible to POST a JSON object and gain additional granularity. The following fields are recognised by the [API](#):

id

The attribute's ID

uuid

The attribute's UUID

value

Will create a sighting for any attribute with the given value or for composite attributes, for the value matching any element of the attribute value

values

Expects a list, MISP will create sightings for any attribute matching any of the given values or for composite attributes, for any of the values matching any element of the attribute value

timestamp

Unix timestamp of the sighting, overrides the current time

Some examples:

To create a sighting for attribute #9001:

```
{"id": "9001"}
```

To create a sighting for any attribute with the value being teamliquid.net or 173.231.136.216 with the time of sighting being :

```
{"values": ["teamliquid.net", "173.231.136.216"], "timestamp": 1460558710}
```

It is also possible to POST a STIX indicator with sighting data to the following URL (keep in mind that the content type has to be XML):

```
https://<misp url>/sightings/add/stix
```

MISP will use the sightings related observables to gather all values and create sightings for each attribute that matches any of the values. If no related observables are provided in the Sighting object, then MISP will fall back to the Indicator itself and use its observables' values to create the sightings. The time of the sighting is the current time, unless the timestamp attribute is set on the Sightings object, in which case that is taken.

An example STIX sightings document:

```

<stix:STIX_Package
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xmlns:stix="http://stix.mitre.org/stix-1"
  xmlns:indicator="http://stix.mitre.org/Indicator-2"
  xmlns:stixCommon="http://stix.mitre.org/common-1"
  xmlns:cybox="http://cybox.mitre.org/cybox-2"
  xmlns:AddressObj="http://cybox.mitre.org/objects#AddressObject-2"
  xmlns:DomainNameObj="http://cybox.mitre.org/objects#DomainNameObject-1"
  xmlns:cyboxVocabs="http://cybox.mitre.org/default_vocabularies-2"
  xmlns:stixVocabs="http://stix.mitre.org/default_vocabularies-1"
  xmlns:example="http://example.com/"
  xsi:schemaLocation="
    http://stix.mitre.org/stix-1 ../stix_core.xsd
    http://stix.mitre.org/Indicator-2 ../indicator.xsd
    http://cybox.mitre.org/objects#DomainNameObject-1 http://cybox.mitre.org/X
    http://stix.mitre.org/common-1 http://stix.mitre.org/XMLSchema/common/1.1.
    http://cybox.mitre.org/default_vocabularies-2 ../cybox/cybox_default_vocab
    http://stix.mitre.org/default_vocabularies-1 ../stix_default_vocabularies.
    http://cybox.mitre.org/objects#AddressObject-2 ../cybox/objects/Address_Ob
    id="example:STIXPackage-33fe3b22-0201-47cf-85d0-97c02164528d"
    timestamp="2014-05-08T09:00:00.000000Z"
    version="1.1.1"
  >
  <stix:STIX_Header>
    <stix:Title>Example watchlist that contains IP information.</stix:Title>
    <stix:Package_Intent xsi:type="stixVocabs:PackageIntentVocab-1.0">Indic
  </stix:STIX_Header>
  <stix:Indicators>
    <stix:Indicator xsi:type="indicator:IndicatorType" id="example:Indicato
      <indicator:Type xsi:type="stixVocabs:IndicatorTypeVocab-1.1">Domain V
      <indicator:Observable id="example:Observable-87c9a5bb-d005-4b3e-8081.
        <cybox:Object id="example:Object-12c760ba-cd2c-4f5d-a37d-18212eac
          <cybox:Properties xsi:type="DomainNameObj:DomainNameObjectTyp
            <DomainNameObj:Value condition="Equals" apply_condition="
          </cybox:Properties>
        </cybox:Object>
      </indicator:Observable>
      <indicator:Sightings>
        <indicator:Sighting timestamp="2014-05-08T09:00:00.000000Z">
          <indicator:Source>
            <stixCommon:Identity>
              <stixCommon:Name>FooBar Inc.</stixCommon:Name>
            </stixCommon:Identity>
          </indicator:Source>
          <indicator:Related_Observables>
            <indicator:Related_Observable>
              <stixCommon:Observable id="example:Observable-45b3acdf-1888-4
                <cybox:Object id="example:Object-a3d36250-42fa-4653-9172-87
                  <cybox:Properties xsi:type="DomainNameObj:DomainNameObjec
                    <DomainNameObj:Value>malicious2.example.com</DomainName
                  </cybox:Properties>
                </cybox:Object>
              </stixCommon:Observable>
            </indicator:Related_Observable>
          </indicator:Related_Observables>
        </indicator:Sighting>
      </indicator:Sightings>
    </stix:Indicator>
  </stix:Indicators>
</stix:STIX_Package>

```

POSTing this as the message's body to MISP will sight any attributes visible to the user with the value "malicious2.example.com". For composite types, a match on a component will also trigger a sighting (so for example for attributes of type domain|ip a domain match would be sufficient).

If no Related observables are set in the Sighting itself, MISP will fall back to the [observable](#) directly contained in the indicator. So in the following example:

```
<stix:STIX_Package
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xmlns:stix="http://stix.mitre.org/stix-1"
  xmlns:indicator="http://stix.mitre.org/Indicator-2"
  xmlns:stixCommon="http://stix.mitre.org/common-1"
  xmlns:cybox="http://cybox.mitre.org/cybox-2"
  xmlns:AddressObject="http://cybox.mitre.org/objects#AddressObject-2"
  xmlns:DomainNameObj="http://cybox.mitre.org/objects#DomainNameObject-1"
  xmlns:cyboxVocabs="http://cybox.mitre.org/default_vocabularies-2"
  xmlns:stixVocabs="http://stix.mitre.org/default_vocabularies-1"
  xmlns:example="http://example.com/"
  xsi:schemaLocation="
    http://stix.mitre.org/stix-1 ../stix_core.xsd
    http://stix.mitre.org/Indicator-2 ../indicator.xsd
    http://cybox.mitre.org/objects#DomainNameObject-1 http://cybox.mitre.org/X
    http://stix.mitre.org/common-1 http://stix.mitre.org/XMLSchema/common/1.1.
    http://cybox.mitre.org/default_vocabularies-2 ../cybox/cybox_default_vocabu
    http://stix.mitre.org/default_vocabularies-1 ../stix_default_vocabularies.
    http://cybox.mitre.org/objects#AddressObject-2 ../cybox/objects/Address_Obj
  id="example:STIXPackage-33fe3b22-0201-47cf-85d0-97c02164528d"
  timestamp="2014-05-08T09:00:00.000000Z"
  version="1.1.1"
>
<stix:STIX_Header>
  <stix:Title>Example watchlist that contains IP information.</stix:Title>
  <stix:Package_Intent xsi:type="stixVocabs:PackageIntentVocab-1.0">Indic
</stix:STIX_Header>
<stix:Indicators>
  <stix:Indicator xsi:type="indicator:IndicatorType" id="example:Indicato
    <indicator:Type xsi:type="stixVocabs:IndicatorTypeVocab-1.1">Domain V
    <indicator:Observable id="example:Observable-87c9a5bb-d005-4b3e-8081.
      <cybox:Object id="example:Object-12c760ba-cd2c-4f5d-a37d-18212ea
        <cybox:Properties xsi:type="DomainNameObj:DomainNameObjectTyp
          <DomainNameObj:Value condition="Equals" apply_condition="
        </cybox:Properties>
      </cybox:Object>
    </indicator:Observable>
    <indicator:Sightings>
      <indicator:Sighting timestamp="2014-05-08T09:00:00.000000Z">
        <indicator:Source>
          <stixCommon:Identity>
            <stixCommon:Name>FooBar Inc.</stixCommon:Name>
          </stixCommon:Identity>
        </indicator:Source>
        </indicator:Sighting>
      </indicator:Sightings>
    </stix:Indicator>
  </stix:Indicators>
</stix:STIX_Package>
```

MISP would create sightings for attributes matching any of the following:
malicious1.example.com, malicious2.example.com, malicious3.example.com

Warninglists API

GET warninglists/index

Description

Return the index of warninglists enabled on the [MISP instance](#)

Parameters

- id

Output

```
...  
{"Warninglists":[{"Warninglist":{"id":"17","name":"List of known Office 365 URI  
...
```

Example

```
curl --header "Authorization: YOUR API KEY " --header "Accept: application/jso
```

GET warninglists/view/1

Description

Return the a warninglist by id

Parameters

- id

Output

```
to long
```

Example

```
curl --header "Authorization: YOUR API KEY " --header "Accept: application/jso
```

Attribute statistics API

If you are interested in the attribute type or attribute category data distribution on your instance, MISP offers an [API](#) that will create an aggregates list. To access the [API](#), simply send a GET request to:

```
https://<misp url>/attributes/attributeStatistics/[context]/[percentage]
```

Where the following parameters can be set:

Context

Set whether you are interested in the type or category statistics of your instance. This parameter can be either set to "type" or "category", with type being the default setting if the parameter is not set.

Percentage

An optional field, if set, it will return the results in percentages instead of the count.

The results are always returned as JSON.

Sample output of the types in percentages from CIRCL's [MISP instance](#):

```

{
  "AS": "0.015%",
  "attachment": "0.177%",
  "btc": "0.005%",
  "campaign-name": "0.005%",
  "comment": "1.47%",
  "domain": "15.992%",
  "domain|ip": "0.005%",
  "email-attachment": "0.207%",
  "email-dst": "0.121%",
  "email-src": "0.192%",
  "email-subject": "0.146%",
  "filename": "3.698%",
  "filename|md5": "0.349%",
  "filename|sha1": "0.894%",
  "filename|sha256": "0.652%",
  "hostname": "17.558%",
  "http-method": "0.045%",
  "ip-dst": "7.087%",
  "ip-src": "2.707%",
  "link": "5.748%",
  "malware-sample": "0.702%",
  "malware-type": "0.005%",
  "md5": "21.064%",
  "mutex": "0.278%",
  "named pipe": "0.03%",
  "other": "1.495%",
  "pattern-in-file": "0.192%",
  "pattern-in-memory": "0.303%",
  "pattern-in-traffic": "0.051%",
  "regkey": "0.126%",
  "regkey|value": "0.187%",
  "sha1": "8.921%",
  "sha256": "5.597%",
  "snort": "0.045%",
  "target-machine": "0.248%",
  "target-org": "0.01%",
  "target-user": "0.106%",
  "text": "0.934%",
  "threat-actor": "0.005%",
  "url": "2.258%",
  "user-agent": "0.081%",
  "vulnerability": "0.182%",
  "whois-registrant-email": "0.01%",
  "x509-fingerprint-sha1": "0.01%",
  "yara": "0.086%"
}

```

Additional statistics

Additional statistics are available as JSON which are the statistics also usable via the user interface. A ".json" can be appended to the following URLs:

- <https://<misp url>/users/statistics/tags.json>
- <https://<misp url>/users/statistics.json>
- <https://<misp url>/users/statistics/attributehistogram.json>
- <https://<misp url>/users/statistics/orgs.json>

An example output of <https://<misp url>/users/statistics.json>:

```
{
  "stats": {
    "event_count": 5233,
    "event_count_month": 21,
    "attribute_count": 645498,
    "attribute_count_month": 723,
    "correlation_count": 207152,
    "proposal_count": 48944,
    "user_count": 1073,
    "org_count": 587,
    "thread_count": 191,
    "thread_count_month": 0,
    "post_count": 337,
    "post_count_month": 0
  }
}
```

MISP modules

Description

It is possible to call misp-modules directly from [API](#). If the module needs credentials, [API](#) will get the information directly from MISP configuration.

GET /modules/

Retrieve a list of all modules enabled.

Example

```
curl --header "Authorization: <APIKEY> " --header "Accept: application/json" -.
```

Output

```
[
  {
    "name": "passivetotal",
    "type": "expansion",
    "mispattributes": {
      "input": [
        "hostname",
        "domain",
        "ip-src",
        "ip-dst"
      ],
      "output": [
        "ip-src",
        "ip-dst",
        "hostname",
        "domain"
      ]
    },
    "meta": {
      "description": "PassiveTotal expansion service to expand values with multi",
      "config": [
        "username",
        "password"
      ],
      "author": "Alexandre Dulaunoy",
      "version": "0.1"
    }
  },
  {
    "name": "sourcecache",
    "type": "expansion",
    "mispattributes": {
      "input": [
        "link"
      ],
      "output": [
        "link"
      ]
    },
    "meta": {
      "description": "Module to cache web pages of analysis reports, OSINT sou",
      "author": "Alexandre Dulaunoy",
      "version": "0.1"
    }
  },
  {
    "name": "dns",
    "type": "expansion",
    "mispattributes": {
      "input": [
        "hostname",
        "domain"
      ],
      "output": [
        "ip-src",
        "ip-dst"
      ]
    },
    "meta": {
      "description": "Simple DNS expansion service to resolve IP address from M",
      "author": "Alexandre Dulaunoy",
      "version": "0.1"
    }
  }
]
```



POST /modules/queryEnrichment

Call any enabled module.

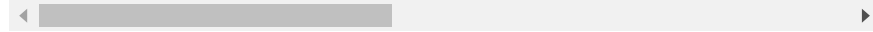
Example

Content of dns.json

```
{
  "hostname": "www.foo.be",
  "module": "dns"
}
```

Query using MISP [API](#)

```
curl --header "Authorization: <APIKEY> " --header "Accept: application/json" --
```



The output will be following JSON:

```
{
  "results": [
    {
      "types": [
        "ip-src",
        "ip-dst"
      ],
      "values": [
        "188.65.217.78"
      ]
    }
  ]
}
```

Last modified: Sun Feb 28 2021 09:22:59 GMT+0100 (Central European Standard Time)

PyMISP - Python Library to access MISP

PyMISP is a Python library to access MISP platforms via their REST [API](#).

PyMISP allows you to fetch events, add or update events/attributes, add or update samples or search for attributes.

Note that you need to have Auth Key access in your [MISP instance](#) to use PyMISP

Capabilities

- Add, get, update, publish, delete events
- Add or remove tags
- Add file attributes: hashes, registry key, patterns, pipe, mutex
- Add network attributes: IP dest/src, hostname, domain, url, UA, ...
- Add Email attributes: source, destination, subject, attachment, ...
- Upload/download samples
- Update sightings
- [Proposals](#): add, edit, accept, discard
- Full text search and search by attributes
- Get STIX event
- Export statistics And even more, just look at the [api.py](#) file

Installation

You can install PyMISP by either using pip or by getting the last version from the [GitHub repository](#)

Install from pip

```
pip install pymisp
```

Install the latest version from the repository

```
git clone https://github.com/MISP/PyMISP.git && cd PyMISP
python setup.py install
```

Note that you will also need to install [requests](#) if you don't have it already.

Getting started

You now need to get your automation key. You can find it on the automation page:

```
https://<misp url>/events/automation
```

or on your profile

```
https://<misp_url>/users/view/me
```

If you did not install using the repository, you can still fetch it to get examples to work on:

```
git clone https://github.com/MISP/PyMISP.git
```

In order to use these, you need to create a file named `keys.py` in the examples folder and edit it to put the url of your [MISP instance](#) and your automation key.

```
cd examples
cp keys.py.sample keys.py
vim keys.py
```

Once you are done with it, you are ready to start.

This is how **keys.py** looks:

```
#!/usr/bin/env python
# -*- coding: utf-8 -*-

misp_url = 'https:///'
misp_key = 'Your MISP auth key' # The MISP auth key can be found on the MISP web
misp_verifycert = True
```

Using PyMISP

To have a better understanding of how to use PyMISP, we will have a look at one of the existing examples: `add_named_attribute.py`. This script allows us to add an attribute to an existing event while knowing only its type (the category is determined by default).

```
#!/usr/bin/env python
# -*- coding: utf-8 -*-

from pymisp import PyMISP
from keys import misp_url, misp_key
import argparse
```

First of all, it is obvious that we need to import PyMISP. Then we also need to know both the instance with which we will work and the [API](#) key to use: Both should be stored in the `keys.py` file. Finally we import `argparse` library so the script can handle arguments.

```
# For python2 & 3 compat, a bit dirty, but it seems to be the least bad one
try:
    input = raw_input
except NameError:
    pass
```


Just a few lines to be sure that python 2 and 3 are supported

```
def init(url, key):
    return PyMISP(url, key, True, 'json', debug=True)
```

This function will create a PyMISP object that will be used later to interact with the [MISP instance](#). As seen in the [api.py](#), a PyMISP object need to know both the URL of the [MISP instance](#) and the [API](#) key to use. It can also take additional and not mandatory data, such as the use or not of SSL or the name of the export format.

```
if __name__ == '__main__':
    parser = argparse.ArgumentParser(description='Create an event on MISP.')
    parser.add_argument("-e", "--event", type=int, help="The id of the event to")
    parser.add_argument("-t", "--type", help="The type of the added attribute")
    parser.add_argument("-v", "--value", help="The value of the attribute")
    args = parser.parse_args()
```

Then the function starts by preparing the awaited arguments:

- event: The event that will get a new attribute
- type: The type of the attribute that will be added. See [here](#) for more information
- value: The value of the new attribute

```
misp = init(misp_url, misp_key)
```

Thanks to the previously created function, we create a PyMISP object.

```
event = misp.get_event(args.event)
event = misp.add_named_attribute(event, args.type, args.value)
```

In order to add the new argument, we first need to fetch the event in the MISP database using the [get_event](#) function which only need the event_id. Then only once we have it, we can call the function [add_named_attribute](#) that will add the argument.

```
print(event)
```

Finally the new event is printed, so we can check that the attribute was correctly added, and that a category was attached to it automatically.

Existing examples

As the name implies you will find several example scripts in the examples folder. For each you can get help if you do `scriptname.py -h`

Let us have a look at some of these examples:

add_named_attribute.py

Allow to add an argument to an existing event by giving only the type of the attribute. The category will be set with a default value.

Arguments:

- **event**: The id of the event to update.
- **type**: The type of the added attribute.
- **value**: The value of the attribute.

add_user.py

Allow to add a user by giving the mandatory fields as entries.

Arguments:

- **email**: Email linked to the account.
- **org_id**: Organisation linked to the user.
- **role_id**: Role linked to the user.

add_user_json.py

Add the user described in the given json. If no file is provided, returns a json listing all the fields used to describe a user.

Arguments:

- **json_file**: The name of the json file describing the user you want to create.

create_events.py

Allow a user to create a new event on the [MISP instance](#).

Arguments:

- **distrib**: The distribution setting used for the attributes and for the newly created event, if relevant. [0-3].
- **info**: Used to populate the event info field if no event ID supplied.
- **analysis**: The analysis level of the newly created event, if applicable. [0-2]
- **threat**: The threat level ID of the newly created event, if applicable. [1-4]

del.py

Delete an event or an attribute from a [MISP instance](#). The event has the priority: if both are set, only the event will be deleted.

Arguments:

- **event**: Event ID to delete.
- **attribute**: Attribute ID to delete.

delete_user.py

Delete the user with the given id. Keep in mind that disabling users (by setting the disabled flag via an edit) is always preferred to keep user associations to events intact.

Arguments:

- **user_id**: The id of the user you want to delete.

edit_user.py

Edit the email of the user designed by the user_id.

Arguments:

- **user_id**: The name of the json file describing the user you want to modify.
- **email**: Email linked to the account.

edit_user_json.py

Edit the user designed by the user_id. If no file is provided, returns a json listing all the fields used to describe a user.

Arguments:

- **user_id**: The name of the json file describing the user you want to modify.
- **json_file**: The name of the json file describing your modifications.

get.py

Get an event from a [MISP instance](#) in json format.

Arguments:

- **event**: Event ID to get.
- **output**: Output file

last.py

Download latest events from a [MISP instance](#). A output file can be created to store these events.

Arguments:

- **last**: can be defined in days, hours, minutes (for example 5d or 12h or 30m).
- **output**: Output file

searchall.py

Get all the events matching a value.

Arguments:

- **search**: String to search.
- **quiet**: Only display URLs to MISP
- **output**: Output file

sharing_groups.py

Get a list of the [sharing groups](#) from the [MISP instance](#). No argument.

sighting.py

Add sighting.

Arguments:

- **json_file**: The name of the json file describing the attribute you want to add sighting to.

stats.py

Output attributes statistics from a [MISP instance](#). No argument.

suricata.py

Download Suricata events.

Arguments:

- **all**: Download all suricata rules available.
- **event**: Download suricata rules from one event.

tags.py

Get tags from [MISP instance](#). No argument.

tagstatistics.py

Get statistics from tags.

Arguments:

- **percentage**: An optional field, if set, it will return the results in percentages, otherwise it returns exact count.
- **namesort**: An optional field, if set, values are sort by the namespace, otherwise the sorting will happen on the value.

up.py

Update an existing event regarding the data inside a given json file.

Arguments:

- **event**: Event ID to modify.
- **input**: Input file

upload.py

Send malware sample to MISP.

Arguments:

- **upload**: File or directory of files to upload.
- **event**: Not supplying an event ID will cause MISP to create a single new event for all of the POSTed malware samples.
- **distrib**: The distribution setting used for the attributes and for the newly created event, if relevant. [0-3].
- **ids**: You can flag all attributes created during the transaction to be marked as \"to_ids\" or not.
- **categ**: The category that will be assigned to the uploaded samples. Valid options are: Payload delivery, Artefacts dropped, Payload Installation, External Analysis.
- **info**: Used to populate the event info field if no event ID supplied.
- **analysis**: The analysis level of the newly created event, if applicable. [0-2]
- **threat**: The threat level ID of the newly created event, if applicable. [1-4]
- **comment**: Comment for the uploaded file(s).

users_list.py

Get a list of the [sharing groups](#) from the [MISP instance](#). No argument.

Going further

feed-generator

It is used to generate the CIRCL [OSINT](#) feed. This script export the events as json, based on tags, organisation, events, ... It automatically update the dumps and the metadata file.

Here is an example of a config file:

```
url = ''
key = ''
ssl = True
outputdir = 'output'
# filters = {'tag' : 'tlp : white|feed-export|!privint', 'org': 'CIRCL'}
filters = {}

valid_attribute_distribution_levels = ['0', '1', '2', '3', '4', '5']
```

Consuming feed

As the feed is a simple set of MISP json files, the files can be easily imported directly into any [MISP instance](#). The script below processes the manifest file of an [OSINT](#) feed and reimport them in a MISP directly.

```
#!/usr/bin/env python
# -*- coding: utf-8 -*-

from pymisp import PyMISP
import requests

url = 'https://www.circl.lu/doc/misp/feed-osint/'
osintcircl = requests.get('{}manifest.json'.format(url))

misp = PyMISP('http://misp.test/', 'key', False, 'json')
for uri in osintcircl.json():
    req = requests.get('{}{}.json'.format(url, uri))
    misp.add_event(req.json())
```

ioc-2-misp

Allow to import OpenIOC files into MISP easily. It is also possible to set specific tags on these events.

Situational Awareness

- `attribute_treemap.py` generate a tree-map showing the distribution of the attributes on the [MISP instance](#).
- `tags_*`: these functions help having statistics and graphs about the tag repartition.

Simple example on fetching the last events

```
#!/usr/bin/env python
# -*- coding: utf-8 -*-

from pymisp import PyMISP
from keys import misp_url, misp_key, misp_verifycert
import argparse
import os
import json

# Usage for pipe masters: ./last.py -l 5h | jq .

def init(url, key):
    return PyMISP(url, key, misp_verifycert, 'json')

def download_last(m, last, out=None):
    result = m.download_last(last)
    if out is None:
        if 'response' in result:
            print(json.dumps(result['response']))
        else:
            print('No results for that time period')
            exit(0)
    else:
        with open(out, 'w') as f:
            f.write(json.dumps(result['response']))

if __name__ == '__main__':
    parser = argparse.ArgumentParser(description='Download latest events from a MISP instance')
    parser.add_argument("-l", "--last", required=True, help="can be defined in a MISP instance")
    parser.add_argument("-o", "--output", help="Output file")

    args = parser.parse_args()

    if args.output is not None and os.path.exists(args.output):
        print('Output file already exists, abort.')
        exit(0)

    misp = init(misp_url, misp_key)

    download_last(misp, args.last, args.output)
```

Last modified: Sun Feb 28 2021 09:22:59 GMT+0100 (Central European Standard Time)

Create an event based on a report

[warning] A specific permission is required to create an event.

For this example, we will use a report found on [Bleeping Computer](#), so considered as [OSINT](#).

Researcher finds the Karma Ransomware being distributed via Pay-per-Install Network

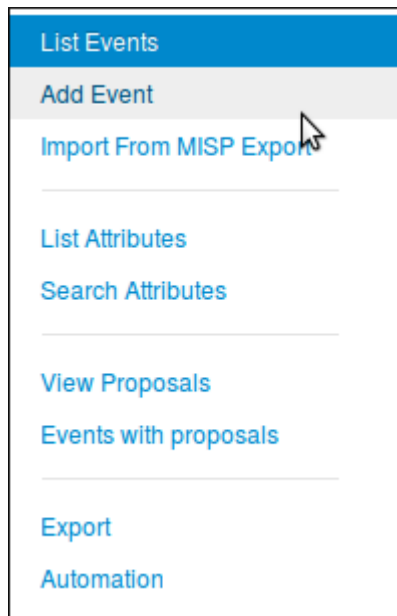
By [Lawrence Abrams](#)

November 14, 2016 07:01 PM 2

A security researcher named [slipstream/RoL](#) has discovered the Karma Ransomware, which pretends to be a Windows optimization program called Windows-TuneUp. What is worse is that this sample was discovered as software that would potentially be distributed by a pay-per-install software monetization company when people install free software downloaded from the Internet.

Adding an event

First of all, we need to create a new event. To do so, we click the "Add Event" option when on the Events list view.



Then we get the add event form.

Add Event

Date

2016-11-16

Distribution i

All communities

Threat Level i

High

Analysis i

Initial

Event Info

Quick Event Description or Tracking Info

GFI sandbox

Browse...

No file selected.

Add

Let's fill it with the data we already have:

- Date: Here we will put the date of the report, so 2016-11-14
- Distribution: Depending on the event, we might want it to be more or less spread accross the MISP instances. For this one, since it is a public report, there is no reason to limit the diffusion so "All communities".
- Threat Level: Self explanatory. Since the ransomware in the report is not using a huge exploit, we can use low, or undefined as we don't really know. we'll go for the latter since it can be edited.
- Analysis: Give the current stage of the analysis. Since the report is published, we can assume that the analysis is completed.
- Event Info: The event's info is in fact the name or title of the event, so it seems legit to put the title of the report here as well. Since it is public information, we also prefix it with "OSINT".
- GFI sandbox: Since we don't have any sample or anything here, we leave this alone.

Add Event

Date

2016-11-14

Distribution ⁱ

All communities

Threat Level ⁱ

Undefined

Analysis ⁱ

Completed

Event Info

OSINT - Researcher finds the Karma Ransomware being distributed vi

GFI sandbox

Browse...

No file selected.

Add

Then just press the blue "Add" button and here we have a brand new event.
Empty.

The event has been saved

View Event

View Correlation Graph

View Event History

Edit Event

Delete Event

Add Attribute

Add Attachment

Populate from...

Merge attributes from...

Publish Event

Publish (no email)

Contact Reporter

Download as...

List Events

Add Event

OSINT - Researcher finds the Karma Ransomware being dis...

Event ID801

Uuid582d6967-3054-4108-a7ac-40c6950d210f

OrgCIRCL

Owner orgCIRCL

Contributors

Email

Tags

Date2016-11-14

Threat LevelUndefined

AnalysisCompleted

DistributionAll communities

InfoOSINT - Researcher finds the Karma Ransomware being distributed via Pay-per-Install Network

PublishedNo

Sightings0 (0)

Pivots

Attributes

Discussion

✖ 801: OSINT ...

« previous

next »

view all

+

📄

🔍

🔗

Filters:

All

File

Network

Financial

Proposal

Correlation

War

Date

Org

Category

Type

Value

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

« previous

next »

view all

(Displayed information can change depending on your role on the [MISP instance](#))

Adding Attributes

Now it is time to populate this event. But before even adding [IoC](#), we are going to add global information about the report itself: the link of the report and a short explanation or introduction. To do so, we need to click on the "Add Attribute" option in the side menu. This will show us this view:

Add Attribute

Category ⓘ
(choose one)

Type ⓘ
(first choose category)

Distribution ⓘ
Inherit event

Value

Contextual Comment

☐ for Intrusion Detection System ☐ Batch Import

Submit

- First we are going to add the link of the report. Since it has been written by an other researcher, it will be considered as an "External analysis", we choose this category.
- Concerning the type, regarding the kind of data we are adding it is obvious that we will choose the "link" type.
- The distribution field can be a little tricky. We can either choose one of the option that was already available at event level or "Inherit event". If we choose the latter, the attribute will be shared the same way as the event it is included in (here to "All communities"). On the other hand, if we choose manually a distribution for the attribute, the most restrictive between event distribution and attribute distribution will be applied. That is to say: if both event and attribute distributions are the same, there will be no change (similar to "Inherit event"). However, if for instance the event distribution is "all communities" while the attribute is limited to "This [community](#) only", the event will indeed be distributed to all communities but without this particular attribute which will be limited to this [community](#) only. The same works the other way around, if the attribute can be distributed to "all communities" while the related event is limited to this [community](#), the attribute being dependant of the event, it will be shared to this [community](#) only, basing its distribution on the event (most restrictive) one.
- The value is simply the data we want to add, here it is the link of the report.
- The contextual comment is a field that will not be used for correlation and is mainly there to add some complementary information on the attribute. Can be a port for an IP, or an indication of any type. Here there is no particular information to add, except maybe tell that it is the source of the report, so let us put this information.
- "for Intrusion Detection System" is used to set the IDS flag or not. If set, the attribute will be used as an IDS signature when exporting the [NIDS](#) data. In this case, we have no reason to check it.
- The Batch Import is a useful option when we need to add several [IoC](#) of the same category/type which allow you to add them at once by separated by a line break between each line in the value field. However it is of no use here.

Add Attribute

Category ⓘ

External analysis

Type ⓘ

link

Distribution ⓘ

Inherit event

Value

http://www.bleepingcomputer.com/news/security/researcher-finds-the-karma-ransomware-being-distributed-via-pay-per-install-network/

Contextual Comment

Source Report

☐ for Intrusion Detection System

☐ Batch Import

Submit

All fields are properly filled ? Then let's press the "submit" button, and Ta-dah !

The attribute has been saved

View Event

View Correlation Graph

View Event History

Edit Event

Delete Event

Add Attribute

Add Attachment

Populate from...

Merge attributes from...

Publish Event

Publish (no email)

Contact Reporter

Download as...

List Events

Add Event

OSINT - Researcher finds the Karma Ransomware being dis...

Event ID	801
UUID	5d3dd967-3054-4108-a7ac-40cd950d210f
Org	CIRCL
Owner org	CIRCL
Contributors	
Email	
Tags	
Date	2016-11-14
Threat Level	Undefined
Analysis	Completed
Distribution	All communities
Info	OSINT - Researcher finds the Karma Ransomware being distributed via Pay per Install Network
Published	No
Sightings	0 (0)

Pivots

Attributes

Discussion

801: OSINT...

< previous next > view all

	Date	Org	Category	Type	Filters	File	Network	Financial	Proposal	Correlation	Warnings	Include deleted attributes	Show context fields	
<input type="checkbox"/>	Date	Org	Category	Type	Value									Comment
<input type="checkbox"/>	2016-11-17		External analysis	link		http://www.bleepingcomputer.com/news/security/researcher-finds-the-karma-ransomware-being-distributed-via-pay-per-install-network/								Source Report

Now we can do a similar procedure to add an introduction to the report (that is to say the first paragraph of the report). We will simply change the type for text. But this time, we will access the add attribute form by clicking on the small + symbol next to the attribute table.

<div><div>+</div></div>	
<input type="checkbox"/>	<div>DateOrg</div>
<input type="checkbox"/>	2016-11-17

The same form as before will appear in a popup.

Add Attribute

Category ⓘ

Type ⓘ

(choose one)

(first choose category)

Distribution ⓘ

Inherit event

Value

Contextual Comment

☐ for Intrusion Detection System

☐ Batch Import

Submit

Cancel

Again, we fill it with the required data.

Add Attribute

Category ⓘ

Type ⓘ

External analysis

text

Distribution ⓘ

Inherit event

Value

A security researcher named slipstream/RoL has discovered the Karma Ransomware, which pretends to be a Windows optimization program called Windows-TuneUp. What is worse is that this sample was discovered as software that would potentially be distributed by a pay-per-install software monetization company when people install free software downloaded from the Internet.

Contextual Comment

Source Report

☐ for Intrusion Detection System

☐ Batch Import

Submit

Cancel

Then we submit it by clicking on the blue button *Et voilà!*

+				Filters: All File Network Financial Proposal Correlation Warnings In	
<input type="checkbox"/>	Date	Org	Category	Type	Value
Show context fields					Events
<input type="checkbox"/>	2016-11-17	External analysis	link	http://www.bleepingcomputer.com/news/security/researcher-finds-the-karma-ransomware-being-distributed-via-pay-per-install-network/	Source Report No
<input type="checkbox"/>	2016-11-17	External analysis	text	A security researcher named slipstream/RoL has discovered the Karma Ransomware, which pretends to be a Windows optimization program called Windows-TuneUp. What is worse is that this sample was discovered as software that would potentially be distributed by a pay-per-install software monetization company when people install free software downloaded from the Internet.	Source Report No

Okay, now it is time to add some [Indicators](#) of Compromise. In this report, they are mainly listed at the end.

Files associated with the Karma Ransomware

Windows-TuneUp.exe

Registry entries associated with the Karma Ransomware

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer "auth"  
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\ "Saffron"= "%Desktop%\# DECRYPT MY FILES #.html"  
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\ "Safron"= "%Desktop%\# DECRYPT MY FILES #.txt"
```

IOCs:

SHA256: 6545ae2b8811884ad257a7fb25b1eb0cb63cfc66a742fa76fd44bdd05b74fe8
SHA256: cf5fda29f8e1f135aa68620ce7298e930be2cb93888e3f04c9cd0b13f5bc4092

Network Communication:

karma2xgg6ccmupd.onion
windows-tuneup.com/web293/xUser.php

Let's try to define which category/type those **IoC** belong to.

First, Windows-TuneUp.exe is without a doubt a *filename*, and the associated category may be *Payload delivery*.

Second the registry entries (type *regkey*) seems to be from *Artifacts dropped* category

Then the hashes that are already said to be *SHA 256*, and a quick test on VirusTotal also reveals that they correspond to the filename seen earlier. so we can add both as an association *filename|SHA256*. Once again, the category will be *Payload delivery*.

And finally the network communication. No doubt here for the category: *Network activity*, and the type might be *url* but for the example, we will let MISP decide for us.

So we begin with the filename. No real change from before for this one, except that we will set the IDS flag to true.

Add Attribute

Category ⁱ Payload delivery Type ⁱ filename

Distribution ⁱ Inherit event

Value

Windows-TuneUp.exe

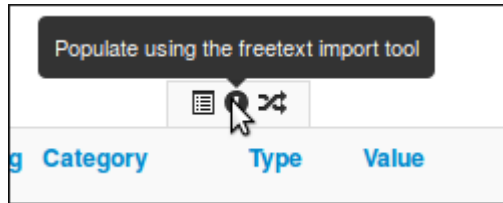
Contextual Comment

☒ for Intrusion Detection System ☐ Batch Import

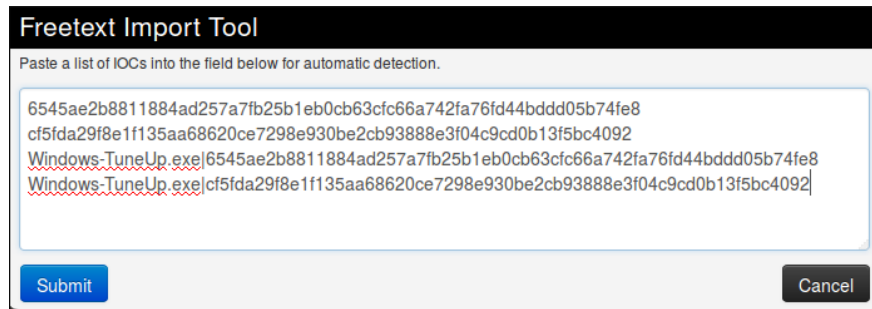
Submit Cancel

Freetext Import Tool

Then we can add the hashes in a similar way. We will have them both alone and combined with the filename. In order to do it quickly, we are going to use the freetext import tool, hidden there



It will open a popup with a text area field where we will paste our **IoC**, one per line. As said previously, we add both the hashes alone and with the filename.



The screenshot shows a web-based interface titled "Freetext Import Tool". Below the title is a instruction: "Paste a list of IOCs into the field below for automatic detection." There is a large text area containing three lines of text: a long hexadecimal hash, a shorter hexadecimal hash, and two lines that combine a filename "Windows-TuneUp.exe" with the two hashes. The text in the area is: "6545ae2b8811884ad257a7fb25b1eb0cb63cfc66a742fa76fd44bddd05b74fe8", "cf5fda29f8e1f135aa68620ce7298e930be2cb93888e3f04c9cd0b13f5bc4092", "Windows-TuneUp.exe|6545ae2b8811884ad257a7fb25b1eb0cb63cfc66a742fa76fd44bddd05b74fe8", and "Windows-TuneUp.exe|cf5fda29f8e1f135aa68620ce7298e930be2cb93888e3f04c9cd0b13f5bc4092". At the bottom of the interface are two buttons: "Submit" and "Cancel".

Freetext Import Tool

Paste a list of IOCs into the field below for automatic detection.

6545ae2b8811884ad257a7fb25b1eb0cb63cfc66a742fa76fd44bddd05b74fe8
cf5fda29f8e1f135aa68620ce7298e930be2cb93888e3f04c9cd0b13f5bc4092
Windows-TuneUp.exe|6545ae2b8811884ad257a7fb25b1eb0cb63cfc66a742fa76fd44bddd05b74fe8
Windows-TuneUp.exe|cf5fda29f8e1f135aa68620ce7298e930be2cb93888e3f04c9cd0b13f5bc4092

Submit Cancel

Then when we press the submit button, we are redirected on this page to control the sent data.

Freetext Import Results

Below you can see the attributes that are to be created. Make sure that the categories and the types are correct, often several options will be offered based on an inconclusive automatic resolution.

☐ Proposals instead of attributes

Value	Similar Attributes	Category	Type	IDS	Comment	Actions
6545ae2b8811884ad257a		Payload deliverv	sha256	<input checked="" type="checkbox"/>		✕
cf5fda29f8e1f135aa68620		Payload deliverv	sha256	<input checked="" type="checkbox"/>		✕
Windows-TuneUp.exe 654		Payload deliverv	filename sha256	<input checked="" type="checkbox"/>		✕
Windows-TuneUp.exe cf5f		Payload deliverv	filename sha256	<input checked="" type="checkbox"/>		✕

Submit

sha256

→

authenthash

Change all

Update all comment fields

Change all

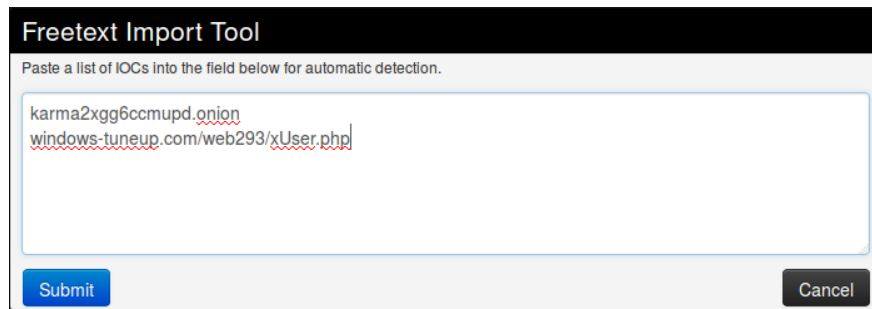
Here, MISP detected by itself what should be the category and type associated to our IoC and surprise! It matches our suppositions. Plus, it also put the IDS flag, so it is perfect. But before submitting, please double check to be sure all the values are correct and no information was lost (That can happen when the data are not formatted as expected by MISP).

If the results of MISP were not what we expected, we can still modify it, however MISP will only suggest suitable category/type regarding the format of your data. We can change for each attribute individually or all at the same time using the option on the bottom right of the form. The same principle also applies for the comments, individually or for all.

Category	Type	IDS
		<input type="checkbox"/>
Payload delivery	sha256	<input checked="" type="checkbox"/>
Payload delivery	sha256	<input checked="" type="checkbox"/>
Artifacts dropped	authentihash	<input checked="" type="checkbox"/>
Payload installation	sha512/256	<input checked="" type="checkbox"/>
External analysis		
Payload delivery	filename/sha256	<input checked="" type="checkbox"/>

(Yes I have two cursors, MISP is magic!)

We only have the network [indicators](#) left, and as said before, we will let MISP determined for us which type is the best for the data we have.



The screenshot shows a web interface titled "Freetext Import Tool". Below the title bar, there is a text input field with the placeholder text "Paste a list of IOCs into the field below for automatic detection." The field contains two lines of text: "karma2xgg6ccmupd.onion" and "windows-tuneup.com/web293/xUser.php". Both lines are underlined with red dashed lines. At the bottom of the interface, there are two buttons: a blue "Submit" button on the left and a grey "Cancel" button on the right.

Freetext Import Results

Below you can see the attributes that are to be created. Make sure that the categories and the types are correct, often several options will be offered to you.

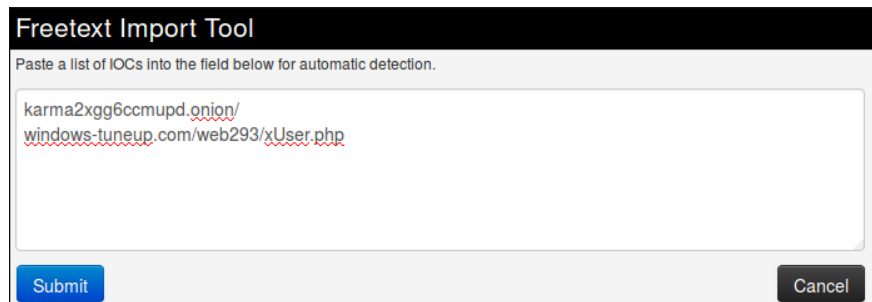
☐ Proposals instead of attributes

Value	Similar Attributes	Category	Type	IDS
<input type="text" value="karma2xgg6ccmupd.onion"/>		<input type="text" value="Payload delivery"/>	filename	<input checked="" type="checkbox"/>
<input type="text" value="windows-tuneup.com/web293/xUser.php"/>		<input type="text" value="Network activity"/>	url	<input checked="" type="checkbox"/>

Submit

Update all comment fields

Oh well, that was unexpected. In fact, it is not that surprising regarding the format of the tor address that look more like a filename than like a url but it is still a problem, since we can't change the type nor the category to a more consistent one. This is indeed one of the limitation of freetext import. To solve this issue, we will use a simple trick: we will add a slash at the end of the tor address so it won't be confused for a filename.



The screenshot shows a web application titled "Freetext Import Tool". Below the title is a text input field containing two lines of text: "karma2xgg6ccmupd.onion/" and "windows-tuneup.com/web293/xUser.php". The text in the input field is underlined with a red dashed line. Below the input field are two buttons: a blue "Submit" button on the left and a grey "Cancel" button on the right.

Freertext Import Results

Below you can see the attributes that are to be created. Make sure that the categories and the types are correct, often several options will be

☐ Proposals instead of attributes

Value	Similar Attributes	Category	Type
<input type="text" value="karma2xgg6ccmupd.onion/"/>		<input type="text" value="Network activity"/>	<input type="text" value="url"/>
<input type="text" value="windows-tuneup.com/web293/xUser.php"/>		<input type="text" value="Network activity"/>	<input type="text" value="url"/>

Thanks to the added character, the first string is recognised as an url which is more consistent with the reality. The second also seems okay, so we can now submit both.

Batch Import

The Freetext Import works properly only with a string of data without any spaces in one line. But if you have lines of text with spaces between values, like e.g.

Associated Files:

```
%Appdata%\Microsoft\Windows\Start Menu\Programs\Startup\Info.hta
%Appdata%\Microsoft\Windows\Start Menu\Programs\Startup\cmb_ransomware.exe
%Appdata%\Info.hta
%UserProfile%\Desktop\FILES ENCRYPTED.txt
C:\Users\Public\Desktop\FILES ENCRYPTED.txt
```

you can still import them at once using the "Add Attribute" option. Click on *Add Attribute*, copy the data and paste it into the *Value* box. Choose the right category and type. Now check both checkboxes for *Intrusion Detection System* and *Batch Import*. The option *Batch Import* will import your data line for line just like the *Freetext Import* option without losing any information. Like this:

Home

Event Actions

Galaxies

Input Filters

Global Actions

View Event

View Correlation Graph

View Event History

Edit Event

Delete Event

Add Attribute

Add Object

Add Attachment

Populate from...

Enrich Event

Merge attributes from...

Publish Event

Publish (no email)

Publish event to ZMQ

Contact Reporter

Download as...

List Events

Add Event

Add Attribute

Did you consider adding an object instead of a composite attribute?

Category ⓘ

Type ⓘ

Artifacts dropped

regkey/value

Distribution ⓘ

Inherit event

Value

%Appdata%\Microsoft\Windows\Start Menu\Programs\Startup\Info.hta
%Appdata%\Microsoft\Windows\Start Menu\Programs\Startup
\cmb_ransomware.exe
%Appdata%\Info.hta
%UserProfile%\Desktop\FILES ENCRYPTED.txt
C:\Users\Public\Desktop\FILES ENCRYPTED.txt

Contextual Comment

☒ for Intrusion Detection System

☒ Batch Import

Notices:

[gdpr]: This attribute is likely to contain personal data and the data subject could be potentially directly identifiable. Please verify. Where applicable, please ensure that you have taken the necessary steps to ensure transparency towards the data subjects in

Submit

And that is all we can get for the main informations and **IoC** in this report. If we search more carefully, there might still be some information left in it, like the filename of the ransomnote for instance, but we will stop here for this example.

Modify the event

If you want to modify your event from the home page, you can either double click on the event or click the edit symbol located in the column **Actions** on the right side. You will be redirected to the editing mode of the selected event.

Last modified: Sun Feb 28 2021 09:22:59 GMT+0100 (Central European Standard Time)

- [Taxonomies](#)
- [Contributing to Taxonomy](#)
- [Reserved Taxonomy](#)
- [Adding Taxonomy in MISP](#)
- [Adding a private taxonomy](#)
- [How to use Taxonomy in MISP](#)
 - [Filtering the distribution of events among MISP instances](#)
 - [MISP Taxonomies - tools](#)
 - [Other use cases using MISP taxonomies](#)
- [Future functionalities related to MISP taxonomies](#)

Taxonomies

In MISP 2.4.X, a flexible mechanism has been introduced to support various [taxonomy of classification](#).

You can access the taxonomy by going into 'Event Actions' and select 'List Taxonomies'. For fresh install, make sure to click 'Update Taxonomies' to view available taxonomies.

A [complete list of the available taxonomies PDF](#) are available on the MISP project website.

List Taxonomies					
Update Taxonomies					
Taxonomies					
<div> <div>previous</div> <div>next</div> </div>					
ID	Namespace	Description	Version	Enabled	Actions
8	nato	NATO classification markings.	1	Yes	[-] [x]
7	euci	EU classified information (EUCI) means any information or material designated by a EU security classification, the unauthorised disclosure of which could cause varying degrees of prejudice to the interests of the European Union or of one or more of the Member States.	1	Yes	[-] [x]
6	ohi-iam	A subset of Information Security Marking Metadata ISM as required by Executive Order (EO) 13526. As described by OHI.gov as Data Encoding Specifications for Information Security Marking Metadata in Controlled Vocabulary Enumeration Values for ISM.	3	No	[+] [x]
5	ecsiit	Incident Classification by the ecsiit.net project WP4 clearinghouse policy and updated by InterMQ.	1	Yes	[-] [x]
4	veris	Vocabulary for Event Recording and Incident Sharing (VERIS)	2	No	[+] [x]
3	tp	The Traffic Light Protocol - or short: TLP - was designed with the objective to create a favorable classification scheme for sharing sensitive information while keeping the control over its distribution at the same time.	1	Yes	[-] [x]
2	circl	CIRCL Taxonomy - Schemes of Classification in Incident Response and Detection	1	Yes	[-] [x]
1	admiralty-scale	The Admiralty Scale (also called the NATO System) is used to rank the reliability of a source and the credibility of an information.	1	Yes	[-] [x]

Page 1 of 1, showing 8 records out of 8 total, starting on record 1, ending on 8

The following taxonomies can be used in MISP (as local or distributed tags) or in other tools willing to share common taxonomies among security information sharing tools.

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/>

1. [Admiralty Scale](#): The Admiralty Scale (also called the NATO System) is used to rank the reliability of a source and the credibility of an information.
2. [adversary](#) An overview and description of the adversary infrastructure.
3. [CIRCL Taxonomy - Schemes of Classification in Incident Response and Detection](#) CIRCL Taxonomy is a simple scheme for incident classification and area topic where the incident took place.
4. [Cyber Kill Chain](#) from Lockheed Martin as described in [Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains](#).
5. DE German (DE) [Government classification markings \(VS\)](#) Taxonomy for the handling of protectively marked information in MISP with German (DE) Government classification markings (VS).
6. [DHS CIIP Sectors](#) DHS critical sectors as described in <https://www.dhs.gov/critical-infrastructure-sectors>.
7. [Diamond Model for Intrusion Analysis](#), a phase-based model developed by Lockheed Martin, aims to help categorise and identify the stage of an attack.
8. [Domain Name Abuse](#) - taxonomy to tag domain names used for cybercrime. Use europol-incident to tag abuse-activity
9. [eCSIRT](#) eCSIRT incident classification Appendix C of the eCSIRT EU project including IntelMQ updates.
10. [ENISA](#) ENISA Threat Taxonomy - A tool for structuring threat information [as published](#)
11. [Estimative Language](#) Estimative language - including likelihood or probability of event based on the Intelligence [Community](#) Directive 203 (ICD 203) (6.2. (a)).
12. [EU Marketop and Publicadmin][EU critical sectors](#) Market operators and public administrations that must comply to some notifications requirements under EU NIS directive.
13. [EUCI](#) EU classified information (EUCI) means any information or material designated by a EU security classification, the unauthorised disclosure of which could cause varying degrees of prejudice to the interests of the European Union or of one or more of the Member States [as described](#).
14. [Europol Incident](#) EUROPOL class of incident taxonomy
15. [Europol Events](#) - EUROPOL type of events taxonomy
16. [FIRST CSIRT Case](#) FIRST CSIRT Case Classification.
17. [FIRST Information Exchange Policy \(IEP\)](#) framework
18. [French gov information classification system](#)

19. [Information Security Indicators](#) Information security [indicators](#) have been standardized by the [ETSI Industrial Specification Group \(ISG\) ISI](#). These [indicators](#) provide the basis to switch from a qualitative to a quantitative culture in IT Security Scope of measurements: External and internal threats (attempt and success), user's deviant behaviours, nonconformities and/or vulnerabilities (software, configuration, behavioural, general security framework).
20. [Information Security Marking Metadata \(ISM\) V13](#) as described by DNI.gov.
21. [Malware](#) classification based on different categories. Based on a [SANS whitepaper about malware](#).
22. Malware Type and Platform classification based on Microsoft's implementation of the [Computer Antivirus Research Organization \(CARO\) Naming Scheme](#) and Malware Terminology. Based on [Microsoft Malware naming conventions](#), [Microsoft Glossary](#), [Microsoft Objective Criteria](#), and [CARO's definitions](#). Malware families are extracted from Microsoft SIRs since 2008 based on [Microsoft Malware, virus, and threat encyclopedia](#). Note that SIRs do NOT include all Microsoft malware families.
23. [MISP taxonomy](#) to infer with MISP behavior or operation.
24. [ms-caro-malware](#) Malware Type and Platform classification based on Microsoft's implementation of the Computer Antivirus Research Organization (CARO) Naming Scheme and Malware Terminology.
25. [NATO Classification Marking](#) Marking of Classified and Unclassified materials as described by the North Atlantic Treaty Organization, NATO.
26. [Open Threat Taxonomy v1.1 \(SANS\)](#) based on James Tarala of SANS (http://www.auditscripts.com/resources/open_threat_taxonomy_v1.1a.pdf).
27. [OSINT Open Source Intelligence - Classification](#)
28. [The Permissible Actions Protocol - or short: PAP](#) PAP was designed to indicate how the received information can be used. It's a protocol/taxonomy similar to TLP informing the recipients of information what they can do with the received information.
29. Status of events used in [Request Tracker](#).
30. Classification based on [malware stealth](#) techniques. Described in [Introducing Stealth Malware Taxonomy](#)
31. [TLP - Traffic Light Protocol](#) The Traffic Light Protocol - or short: TLP - was designed with the objective to create a favorable classification scheme for sharing sensitive information while keeping the control over its distribution at the same time.
32. Vocabulary for Event Recording and Incident Sharing [VERIS](#)

A taxonomy contains a series of tags that can be used as normal tags in your [MISP instance](#).

Tagging is a simple way to attach a classification to an event. In the early version of MISP, **tagging** was local to an instance. Classification must be globally used to be efficient. After evaluating different solutions of classification, we build a new scheme using the concept of machine tags.

Taxonomy is a classification of informations. Taxonomies are implemented in a simple JSON format. Anyone can create their own taxonomy or reuse an existing one.

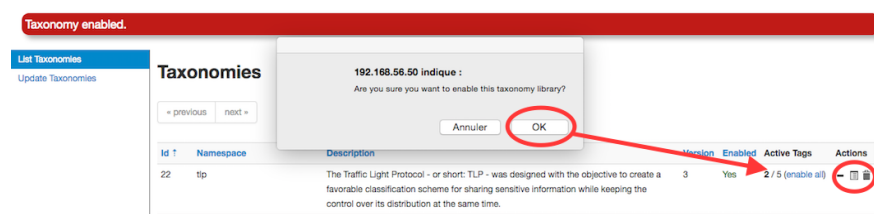
Taxonomies are in an [independent git repository](#).

These can be **freely reused** and **integrated** in other threat intel tools.

The advantage is that you can set a specific tag as being exportable. This means that you can **export** your classification with other [MISP instance](#) and **share** the same taxonomies. **Tagging** is a simple way to attach a classification to an event.

Classification must be globally used to be efficient.

If you want to enable a specific taxonomy, you can click on the cross to enable it.



Then you can even cherry-pick the tags you want to use on the system. If you want to use the whole taxonomy, select all and then click on the cross in the top left.

Contributing to Taxonomy

It is quite easy. Create a JSON file describing your taxonomy as triple tags.

```
1 {  
2   "namespace": "admiralty-scale",  
3   "description": "The Admiralty Scale (also called the NATO  
4     System) is used to rank the reliability of a source and  
5     the credibility of an information.",  
6   "version": 1,  
7   "predicates": [  
8     {  
9       "value": "source-reliability",  
10      "expanded": "Source Reliability"  
11    },  
12    {  
13      "value": "information-credibility",  
14      "expanded": "Information Credibility"  
15    }  
16  ],  
17  ....
```

```
1 {  
2   "values": [  
3     {  
4       "predicate": "source-reliability",  
5       "entry": [  
6         {  
7           "value": "a",  
8           "expanded": "Completely reliable"  
9         },  
10    ....  
11  ]  
12    },  
13  ]  
14 }
```


(e.g. check an existing one like [Admiralty Scale](#)), create a directory matching your name space, put your machinetag file in the directory and [pull](#) your request. [Publishing](#) your taxonomy is as easy as a simple git [pull](#) request on misp-taxonomies (<https://github.com/MISP/misp-taxonomies>). That's it. Everyone can benefit from your taxonomy and can be automatically enabled in information sharing tools like [MISP](#).

Reserved Taxonomy

The following taxonomy namespaces are reserved and used internally to MISP.

- [galaxy](#) mapping taxonomy with cluster:element:"value".

Adding Taxonomy in MISP

How are taxonomies integrated in MISP?

MISP administrators have only to import (or even cherry pick) the namespace or predicates they want to use as tags.

Tags can be exported to other instances.

Tags are also accessible via the MISP REST [API](#).

For more information, "[Information Sharing and Taxonomies Practical Classification of Threat Indicators using MISP](#)" presentation given to the last MISP training in Luxembourg.

Adding a private taxonomy

```
$ cd /var/www/MISP/app/files/taxonomies/  
$ mkdir privatetaxonomy  
$ cd privatetaxonomy  
$ vi machinetag.json
```

Create a JSON file describing your taxonomy as triple tags.

```
For example :  
mkdir sample  
cd sample  
vim machinetag.json
```

Sample JSON with triple tags. You can use the JSON validator to be sure that there is no syntax error.

```
{
  "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"
        }
      ]
    }
  ]
}
```

Go to MISP Web GUI [taxonomies/index](#) and update the taxonomies once you are happy with your file. The newly created taxonomy should be visible. Now you need to activate the tags within your taxonomy.

How to use Taxonomy in MISP

Filtering the distribution of events among MISP instances

Applying rules for distribution based on tags:

MISP Taxonomies - tools

- [machinetag.py](#) is a parsing tool to dump taxonomies expressed in Machine Tags (Triple Tags) and list all valid tags from a specific taxonomy.

```
% cd tools
% python machinetag.py
  admiralty-scale:source-reliability="a"
  admiralty-scale:source-reliability="b"
  admiralty-scale:source-reliability="c"
  admiralty-scale:source-reliability="d"
  admiralty-scale:source-reliability="e"
  admiralty-scale:source-reliability="f"
  admiralty-scale:information-credibility="1"
  admiralty-scale:information-credibility="2"
  admiralty-scale:information-credibility="3"
  admiralty-scale:information-credibility="4"
  admiralty-scale:information-credibility="5"
  admiralty-scale:information-credibility="6"
  ...
```

- [PyTaxonomies](#) - Python module to use the [MISP Taxonomies](#)

Other use cases using MISP taxonomies

Tags can be used to:

- Set events for further processing by external tools (e.g. VirusTotal auto-expansion using Viper).
- Ensure a classification manager classes the events before release (e.g. release of information from air-gapped/classified networks).
- Enrich IDS export with tags to fit your [NIDS](#) deployment.

Future functionalities related to MISP taxonomies

- Sighting support (thanks to NCSC-NL) is integrated in MISP allowing to auto expire [IOC](#) based on user detection.
- Adjusting taxonomies (adding/removing tags) based on their score or visibility via sighting.
- Simple taxonomy editors to help non-technical users to create their taxonomies.
- Filtering mechanisms in MISP to rename or replace taxonomies/tags at [pull](#) and [push synchronisation](#).
- More public taxonomies to be included

Last modified: Sun Feb 28 2021 09:22:59 GMT+0100 (Central European Standard Time)

- [Galaxies](#)
 - [Managing Galaxies in MISP](#)
 - [Adding a custom Galaxy repository in MISP \(WiP - notFunctional\)](#)
 - [Adding a new Galaxy](#)
 - [Context](#)
 - [Directory structure](#)
 - [The galaxy management GUI](#)
 - [The galaxy file](#)
 - [The cluster file](#)
 - [Implementation](#)
 - [Troubleshooting](#)
 - [Example](#)
 - [Simple galaxy](#)
 - [Matrix-shaped galaxy](#)
 - [Dependencies](#)
 - [Create a fork](#)
 - [Understanding directory structure](#)
 - [Removing a Galaxy to better understand the add](#)
 - [Using Galaxies in MISP Events - Example](#)
 - [Available Galaxies](#)
 - [Clusters](#)
 - [Vocabularies](#)
 - [Common](#)
 - [threat-actor](#)

Galaxies

Galaxies in MISP are a method used to express a large object called cluster that can be attached to MISP events or attributes. A cluster can be composed of one or more elements. Elements are expressed as key-values.

There are default vocabularies available in MISP galaxy but those can be overwritten, replaced or updated as you wish. Vocabularies are from existing standards (like [STIX](#), [Veris](#), [ATT&CK](#), MISP and so on) or custom ones you only use for your organization.

Existing clusters and vocabularies can be used as-is or as a template. MISP distribution can be applied to each cluster to permit a limited or broader distribution scheme.

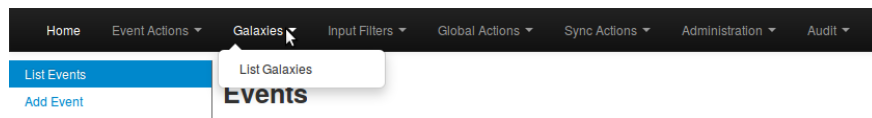
The objective is to have a common set of clusters for organizations starting analysis but that can be expanded to localized information (which is not shared) or additional information (that can be shared).

[MISP galaxy](#) is available on Github.

Managing Galaxies in MISP

[warning] You need to have a specific role to manage Galaxies on a [MISP instance](#).

Galaxies management is accessed using the Galaxies link on the top menu.










A list with all the galaxies existing on the server will appear.

Galaxies

« previous

next »

Id ↑	Name	Version	Description	Description
23	Preventive Measure	1	Preventive measures based on the ransomware document overview as published in https://docs.google.com/spreadsheets/d/1TWS238xacAto-ILKh1n5uTsdjJWdCEsGIM0Y0Hvmc5g/pubhtml# . The preventive measures are quite generic and can fit any standard Windows infrastructure and their security measures.	
22	Ransomware	1	Ransomware galaxy based on https://docs.google.com/spreadsheets/d/1TWS238xacAto-ILKh1n5uTsdjJWdCEsGIM0Y0Hvmc5g/pubhtml	
21	TDS	2	TDS is a list of Traffic Direction System used by adversaries	
20	Exploit-Kit	2	Exploit-Kit is an enumeration of some exploitation kits used by adversaries. The list includes document, browser and router exploit kits.It's not meant to be totally exhaustive but aim at covering the most seen in the past 5 years	
19	Tool	1	Threat actors tools is an enumeration of tools used by adversaries. The list includes malware but also common software regularly used by the adversaries.	
18	Threat Actor	1	Threat actors are characteristics of malicious actors (or adversaries) representing a cyber attack threat including presumed intent and historically observed behaviour.	
17	Microsoft Activity Group actor	1	Activity groups as described by Microsoft	

Page 1 of 1, showing 7 records out of 7 total, starting on record 1, ending on 7

Each galaxy can be explored using the **View** icon at the end of the line.

Tool galaxy

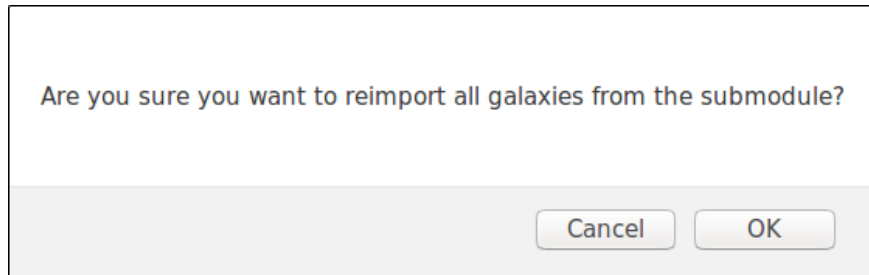
Galaxy ID	19
Name	Tool
Uuid	9b8037f7-bc8f-4de1-a797-37266619bc0b
Description	Threat actors tools is an enumeration of tools used by adversaries. The list includes malware but also common software regularly used by the adversaries.
Version	1

← previous	1	2	3	4	next →
----------------------------	-------------------	-------------------	-------------------	-------------------	------------------------

Value ↓	Synonyms	Activity	#Events	Description	Actions
EyePyramid Malware		<div><div></div></div>	0	Two Italians referred to as the "Ochlonero brothers" have been arrested and accused of using malware and a carefully-prepared spear-phishing scheme to spy on high-profile politicians and businessmen. This case has been called "EyePyramid", which we first discussed last week. (Conspiracy theories aside, the name came from a domain name and directory path that was found during the research.)	
Adwind	AlienSpy Frutas Unrecom Sockerat JSocket JRat Backdoor:Java/Adwind	<div><div></div></div>	1	Adwind is a backdoor written purely in Java that targets system supporting the Java runtime environment. Commands that can be used, among other things, to display messages on the system, open URLs, update the malware, download/execute files, and download/load plugins. A significant amount of additional functionality can be provided through downloadable plugins, including such things as remote control options and shell command execution.	

Here the metadata of the selected galaxy is shown. You also see a table with each available value as well as some complementary data such as a description of the value or the activity ([MISP Sightings](#)), that is to say the evolution of the use of each value.

Galaxies can be reimported from the submodules by clicking the "Update Galaxies" link on either the galaxies list or while browsing a specific galaxy. A popup will appear to confirm the reimportation.



All galaxies will always be updated, even while browsing a specific galaxy.

Adding a custom Galaxy repository in MISP (WiP - notFunctional)

Fork the [misp-galaxy](#) repository to your github account.

Once you have forked the repo you can do the following, assuming you have followed the [Standard MISP Install](#).

```
cd /var/www/MISP/app/files/  
sudo rm -rf misp-galaxy  
# Replace the following line with your fork  
sudo -u www-data git clone https://github.com/SteveClement/misp-galaxy.git
```

Once this is done double check if you can still see the Galaxies in the Web UI.

[warning] This will impact the UI "Update MISP" functionality in administration. Your git head might get [detached](#) in your misp-galaxy repo.

Adding a new Galaxy

Context

A galaxy is designed to provide more info than a tag. It comes in two formats: regular or matrix-shape. In a tag, you can only display one label and one color. In a galaxy, you can display:

- name
- synonymous
- description
- categories (for matrix-galaxies)

Directory structure

Galaxies are represented by two json files stored in:














```
/var/www/MISP/app/files/misp-galaxy/galaxies/mygalaxy.json  
/var/www/MISP/app/files/misp-galaxy/clusters/mygalaxy.json
```

The **/galaxies** file contains metatdatas and galaxy structure. The **/clusters** file contains actual data.

The galaxy managment GUI

Galaxies

« previous next »

Id 1	Icon 2	Name 3	Version 7	Namespace 4	Description 1
406		Dark Patterns	1	misp	Social Engineering - Dark Patterns
405		Surveillance Vendor	1	misp	List of vendors selling surveillance technologies including malware, interception devices or computer exploitation services
404		Misinformation Pattern	4	misinfosec	AMITT Tactic
403		Regions UN IM49	2	misp	Regions based on UN IM49.
402		Target Information	1	misp	Description of targets of threat actors.
401		o365-exchange-techniques	1	misp	o365-exchange-techniques - Office365Exchange related techniques by @johnLaTwC
400		attck4fraud	1	misp	attck4fraud - Principles of MITRE ATT&CK in the fraud domain
399		Election guidelines	1	misp	Universal Development and Security Guidelines as Applicable to Election Technology.
398		Malpedia	1	misp	Malware galaxy based on Malpedia archive.
397		Backdoor	1	misp	Malware Backdoor galaxy.
396		Stealer	1	misp	Malware stealer galaxy.
395		Mobile Attack - Relationship	4	mitre-attack	Mitre Relationship
394		Mobile Attack - Malware	5	deprecated	Name of ATT&CK software

In this windows, you will be able to check all your galaxies and if your newly created ones are OK.

The galaxy file

The galaxy file provides the framework for the data stored in the cluster file. For example:

```
{
  "description": "attck4fraud - Principles of MITRE ATT&CK in the fraud domain",
  "icon": "map",
  "kill_chain_order": {
    "fraud-tactics": [
      "Initiation",
      "Target Compromise",
      "Perform Fraud",
      "Obtain Fraudulent Assets",
      "Assets Transfer",
      "Monetisation"
    ]
  },
  "name": "attck4fraud",
  "namespace": "misp",
  "type": "financial-fraud",
  "uuid": "cc0c8ae9-aec2-42c6-9939-f4f82b051836",
  "version": 1
}
```

19 lines (19 sloc) | 452 Bytes

```
1 {
2   1 "description": "attck4fraud - Principles of MITRE ATT&CK in the fraud domain",
3   2 "icon": "map",
4   8 "kill_chain_order": {
5     "fraud-tactics": [
6       "Initiation",
7       "Target Compromise",
8       "Perform Fraud",
9       "Obtain Fraudulent Assets",
10      "Assets Transfer",
11      "Monetisation"
12    ]
13  },
14  3 "name": "attck4fraud",
15  4 "namespace": "misp",
16  5 "type": "financial-fraud",
17  6 "uuid": "cc0c8ae9-aec2-42c6-9939-f4f82b051836",
18  7 "version": 1
19 }
```

- **description:** generalities about the galaxy (1)
- **icon:** the icon used in the MISP interface (2)
- **name:** the name of the galaxy (3)
- **namespace:** the namespace where is stored the galaxy. Namespace are used to regroup similar galaxies (4)
- **type: IMPORTANT field**, it MUST match the galaxy and cluster files name to actually chain both files together (5)
- **uuid:** as any MISP object, it has a uuid. **IMPORTANT**, it MUST be repeated in the uuid property of the cluster file (6)
- **version:** as usual in MISP, versioning, especially to force update (7)
- **kill_chain_order:** a special and optionnal field: it will be used if you want to create a matrix-galaxy. In this field, you insert a named table (*fraud-tactics* in the example above) containing the categories labels of you data. They will be used then in the cluster file (8)

More detail on galaxy fields here: <https://tools.ietf.org/html/draft-dulaunoy-misp-galaxy-format-06#page-9>

The cluster file

The cluster file provides the actual data of the galaxy. For example (Attck4fraud):

```
{
  "authors": [
    "Francesco Bigarella"
  ],
  "category": "guidelines",
  "description": "attck4fraud - Principles of MITRE ATT&CK in the fraud domain",
  "name": "attck4fraud",
  "source": "Open Sources",
  "type": "financial-fraud",
  "uuid": "cc0c8ae9-aec2-42c6-9939-f4f82b051836",
  "values": [
    {
      "description": "In the context of ATT&CK for Fraud, phishing is described",
      "meta": {
        "detection": "Email sender is spoofed; Email sender belongs to a domain",
        "examples": [
          "Phishing messages were sent to Amazon users posing as the Amazon cus",
          "Fake Apple invoices were sent to Apple App Store customers in order"
        ],
        "external_id": "FT1001",
        "kill_chain": [
          "fraud-tactics:Initiation"
        ],
        "mitigation": "Implementation of DKIM and SPF authentication to detect",
        "refs": [
          "https://blog.malwarebytes.com/cybercrime/2015/02/amazon-notice-ticke",
          "https://www.bleepingcomputer.com/news/security/widespread-apple-id-p"
        ],
        ...
      },
      "version": 3
    }
  ]
}
```

Introduction

```
384 lines (384 sloc) | 13.8 KB
Raw Blame History
1 {
2   1 "authors": [
3     "Francesco Bigarella"
4   ],
5   2 "category": "guidelines",
6   3 "description": "attck4fraud - Principles of MITRE ATT&CK in the fraud domain",
7   4 "name": "attck4fraud",
8   5 "source": "Open Sources",
9   6 "type": "financial-fraud",
10  7 "uuid": "cc0c8ae9-aec2-42c6-9939-f4f82b051836",
11  8 "values": [
12    {
13      "description": "In the context of ATT&CK for Fraud, phishing is described as the sending of fraudulent emails to a large audience",
14      "meta": {
15        9 "detection": "Email sender is spoofed; Email sender belongs to a domain recently created; Presence of typos or poor grammar ;",
16        "examples": [
17          "Phishing messages were sent to Amazon users posing as the Amazon customer support",
18          "Fake Apple invoices were sent to Apple App Store customers in order to obtain their Apple ID credentials"
19        ],
20        "external_id": "FT1001",
21        10 "kill_chain": [
22          "Fraud-tactics:Initiation"
23        ],
24        "mitigation": "Implementation of DKIM and SPF authentication to detected spoofed email senders; anti-phishing solutions.",
25        "refs": [
26          "https://blog.malwarebytes.com/cybercrime/2015/02/amazon-notice-ticket-number-phish-seeks-card-details/",
27          "https://www.bleepingcomputer.com/news/security/widespread-apple-id-phishing-attack-pretends-to-be-app-store-receipts/"
28        ],
29      }
30    ]
31  }
32 }
```

- **authors:** descriptive field (1)
- **category:** descriptive field (2)
- **description:** descriptive field (3)
- **name:** same as in /galaxy file, used in the Matrix display (4)
- **source:** descriptive field (5)
- **type:** IMPORTANT, this field MUST match the /galaxy and /cluster files names AND the type field in the /galaxy file name -5 in above paragraph- (6)
- **uuid:** IMPORTANT, this field MUST match the /galaxy uuid field -6 in above paragraph- (7)
- **values:** a table containing the actual values (8)
- **data fields:** fields used to describe single data are detailed here: <https://tools.ietf.org/html/draft-dulaunoy-misp-galaxy-format-06#page-9> (9)
- **kill_chain:** IMPORTANT, provide the column of the Matrix where the data will be displayed: (10)
 - **arg1:** MUST match /galaxy file's *killchain arg* (*_fraud-tactics* in the example)
 - **arg2:** name of the column of the data (*Initiation* in the example)
- **version:** same as for galaxies

More details on /cluster fields can be found here: <https://tools.ietf.org/html/draft-dulaunoy-misp-galaxy-format-06#page-9>

Implementation

- Once your files are ready, ALWAYS submit them in a json validator such as: <https://jsonformatter.curiousconcept.com/> . Do it before putting them into your instance, your sanity is at stake.
- Copy/paste your files in both folders (/galaxies and /clusters)
- Go to Galaxies/List galaxies and clic on Update galaxies
- Your new galaxy should be displayed on the screen with the others

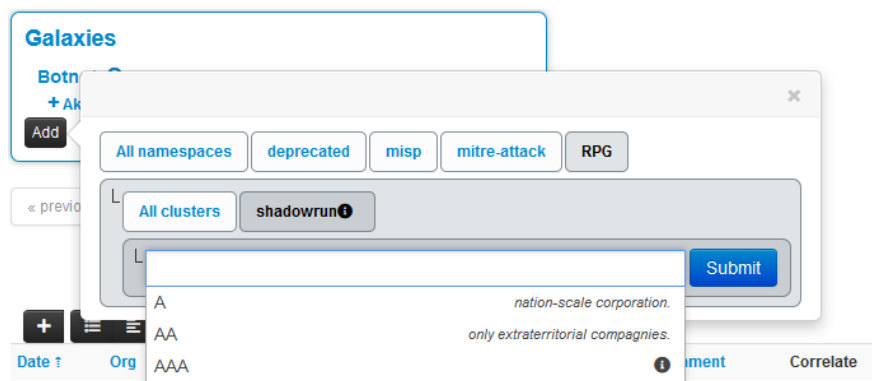
The screenshot shows the MISP (Malware Information System) interface. The top navigation bar includes links for Home, Event Actions, Galaxies, Input Filters, Global Actions, Sync Actions, Administration, and Audit. The left sidebar has links for List Galaxies, Update Galaxies, and Add Galaxy. The main content area displays the details for a galaxy named 'shadowrun galaxy'.

Galaxy Details:

- Galaxy ID: 41
- Name: shadowrun
- Namespace: RPG
- Uuid: 7a956b4d-613c-4c08-b5d6-19974682aea8
- Description: My Shadowrun test galaxy
- Version: 1

Below the details, there are navigation buttons: '< previous' and 'next >'. A table with the following columns is shown: Value, Synonyms, Activity, #Events, Description, Filter, and Actions. The table is currently empty, and a message at the bottom states: 'Page 1 of 1, showing 0 records out of 0 total, starting on record 0, ending on 0'.

- Your galaxy is available in the events for selecting in the right namespace



Attribute warning: This event doesn't contain any attribute. It's strongly advised to populate the event with attributes (indicated by a red bar at the bottom of the page).

Troubleshooting

- **The galaxy does not update, galaxy is empty**
 - Check json validation
 - Remove commas on last items of any {} or []
 - Update version of files
 - Check files names
 - Delete the galaxy in the GUI and update
- **Matrix is not displayed**
 - Check the kill_chain_order array in the /galaxies json
 - Check the chaining

Example

We will create a galaxy from scratch. To demonstrate MISP can handle any type of use-case, we will not work on malware but on Shadowrun pen and paper RPG. In this RPG, 2060's large megacorporations launch paramilitary actions against each other. They can belong to 3 main categories (ranked by international standards):

- AAA: extraterritorial corporation and seating at the top-10 council;
- AA: only extraterritorial compagnies;
- A: nation-scale corporation.

A corporation can act in several fields:

- energy
- IT
- biotechnology
- cyberotechnology (body enhancement)

It can work on several continent:

- Europe;
- Asia;
- Africa;
- Oceania;
- America.

All these context elements are enough to build a galaxy.

Simple galaxy

- the galaxy file: galaxies/shadowrun.json


```
{
  "description": "My Shadowrun test galaxy",
  "icon": "user-secret",
  "name": "shadowrun",
  "namespace": "RPG",
  "type": "shadowrun",
  "uuid": "7a956b4d-613c-4c08-b5d6-19974682aea8",
  "version": 1
}
```

Keep the uuid and type, it will be necessary later.

- Check your json
- Click on update and see your work:

The screenshot shows a web application interface for managing galaxies. The top navigation bar includes links for Home, Event Actions, Galaxies, Input Filters, Global Actions, Sync Actions, Administration, and Audit. On the left sidebar, there are links for 'it Galaxies', 'xdate Galaxies', 'rce Update Galaxies', and 'w Galaxy' (which is highlighted). The main content area displays the details for a galaxy named 'shadowrun galaxy'.

shadowrun galaxy

Galaxy ID	41
Name	shadowrun
Namespace	RPG
Uuid	7a956b4d-613c-4c08-b5d6-19974682aea8
Description	My Shadowrun test galaxy
Version	1

Navigation buttons: < previous, next >

Table headers: Value, Synonyms, Activity, #Events, Description, Filter, Actions.

Page 1 of 1, showing 0 records out of 0 total, starting on record 0, ending on 0

Navigation buttons: < previous, next >

- the cluster file: `clusters/shadowrun.json`

```

{
  "authors": [
    "myself"
  ],
  "category": "RPG",
  "description": "Shadowrun galaxy",
  "name": "shadowrun corporations",
  "source": "Internal",
  "type": "shadowrun",
  "uuid": "7a956b4d-613c-4c08-b5d6-19974682aea8",
  "values": [
    {
      "description": "extraterritorial corporation and seating at the top-10 co
      "meta": {
        "Corporate council seat": "Yes",
        "examples": [
          "Renraku",
          "Shiawase",
          "Aztechnology",
          "Ares Macrotechnologies",
          "Saeder Krupps"
        ]
      },
      "uuid": "43e1b900-5a03-11ea-9ad1-080027cbfd66",
      "value": "AAA"
    },
    {
      "description": "only extraterritorial compagnies.",
      "meta": {
        "Corporate council seat": "No",
        "examples": [
          "Shibata",
          "Monobe",
          "Zeta Impchem",
          "ESUS"
        ]
      },
      "uuid": "7aad2dd4-5a03-11ea-ad69-080027cbfd66",
      "value": "AA"
    },
    {
      "description": "nation-scale corporation.",
      "meta": {
        "Corporate council seat": "No",
        "examples": [
          "Genom",
          "KSAF",
          "Seretech",
          "Infocore",
          "MicroDek (ex-Microsoft)",
          "Tan Tien"
        ]
      },
      "uuid": "50c0d622-5c67-11ea-bd4b-0800275bbff6",
      "value": "A"
    },
    {
      "description": "energy sector: exploitation, , refining, selling",
      "meta": {
        "examples": [
          "Saeder Krupps"
        ],
        "subsectors": [
          "petroleum",
          "electricity",

```

```

        "gas",
        "bio"
    ]
},
"uuid": "293e7e5c-51a8-411f-9b47-d52ed62d4b78",
"value": "energy"
},
{
    "description": "cybertechnology sector: manufacturing, selling and implar
    "meta": {
        "Delta clinic (for implanting)": [
            "Yes",
            "No"
        ],
        "examples": [
            "headware",
            "bodyware",
            "eyeware",
            "earware",
            "cyberlimbs"
        ]
    },
    "uuid": "7e962290-cba7-49ad-95c2-115575c8a9d2",
    "value": "cybertechnology"
},
{
    "description": "Biotechnology: bioware, genetics, etc",
    "meta": {
        "examples": [
            "bioware",
            "genetics",
            "biodrones",
            "biocosmetics"
        ]
    },
    "uuid": "c899564c-bfe4-460f-a2ed-aae98e1355a3",
    "value": "biotechnology"
},
{
    "description": "IT: softwares, hardware, cybersec",
    "meta": {
        "examples": [
            "software dev",
            "hardware manufacturing",
            "intrusion countermeasures"
        ]
    },
    "uuid": "16c49ba4-8a79-4f67-a98a-07cdc08f8a2d",
    "value": "IT"
},
{
    "description": "Europe",
    "meta": {
        "examples": [
            "France",
            "Belgium",
            "Luxembourg",
            "Germany",
            "Italy"
        ]
    },
    "uuid": "8e745c22-9b14-4334-887a-0000eda58f75",
    "value": "Europe"
},
{
    "description": "Asia",

```

```

    "meta": {
      "examples": [
        "China",
        "Japan",
        "Thailand"
      ]
    },
    "uuid": "95d4ff78-42f8-4fe8-bb63-af2c7e500ec8",
    "value": "Asia"
  },
  {
    "description": "Russia and former USSR",
    "meta": {
      "examples": [
        "Russia",
        "kazakhstan"
      ]
    },
    "uuid": "87a3ac08-6ffc-45eb-826e-e8e0af392563",
    "value": "Russia"
  },
  {
    "description": "Africa",
    "meta": {
      "examples": [
        "Nigeria",
        "Malia",
        "Algeria"
      ]
    },
    "uuid": "aba705b7-fcb4-4bf4-81d4-b896314f53ed",
    "value": "Africa"
  },
  {
    "description": "Oceania",
    "meta": {
      "examples": [
        "Asutralia",
        "Polynesia"
      ]
    },
    "uuid": "ae28830b-b90f-48d9-8b89-acda0864ff4e",
    "value": "Oceania"
  },
  {
    "description": "America",
    "meta": {
      "examples": [
        "UCAS",
        "CAS",
        "Pueblo Corporate COuncil",
        "AZtlan"
      ]
    },
    "uuid": "d41c6222-4d10-43e9-9a8e-47d586eaf0e7",
    "value": "America"
  }
],
"version": 3
}

```

IMPORTANT:

- the ""uuid": "7a956b4d-613c-4c08-b5d6-19974682aea8", " is the same in both files
- the cluster filename is the same as the "type" field in the galaxy file
- CHECK YOUR JSON (<https://jsonformatter.curiousconcept.com/>) AND SAVE YOUR SANITY!

We check the thing by clicking on the update button in the galaxy GUI:

The screenshot shows the 'shadowrun galaxy' interface. On the left, there's a sidebar with links: 'List Galaxies', 'Update Galaxies', 'Force Update Galaxies', and 'View Galaxy' (which is highlighted). The main area displays the galaxy details for 'shadowrun galaxy' with the following information:

- Galaxy ID: 39
- Name: shadowrun
- Namespace: RPG
- Uuid: 7a956b4d-613c-4c08-b5d6-19974682aea8
- Description: My Shadowrun test galaxy
- Version: 1

Below the details, there's a table with columns: 'Value', 'Synonyms', 'Activity', '#Events', 'Description', and 'Actions'. The table contains three rows of data:

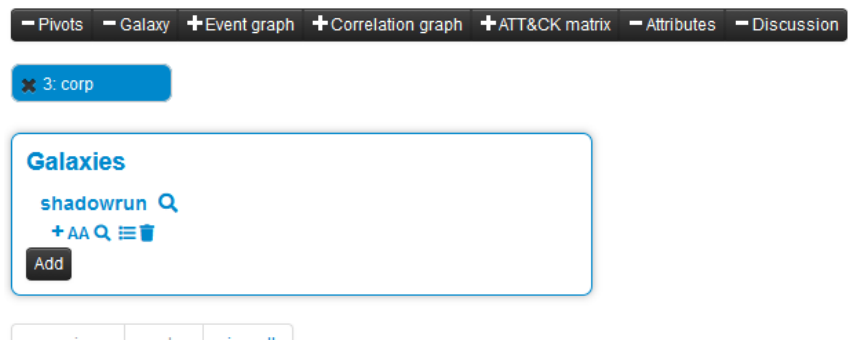
Value	Synonyms	Activity	#Events	Description	Actions
A			0	nation-scale corporation.	
AA			0	only extraterritorial companies.	
AAA			0	extraterritorial corporation and seating at the top-10 council.	

At the bottom, it says 'Page 1 of 1, showing 3 records out of 3 total, starting on record 1, ending on 3'.


We can test our work on the MISP GUI:



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



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

 **shadowrun galaxy**

Galaxy ID62

Nameshadowrun

NamespaceRPG



























Uuid7a956b4d-613c-4c08-b5d6-19974682aea8

DescriptionMy Shadowrun test galaxy

Version2

« previous

next »

Value i	Synonyms	Activity	#Events	Description	Filter	Actions
A		<div></div>	0	nation-scale corporation.		 
AA		<div></div>	0	only extraterritorial compagnies.		 
AAA		<div></div>	0	extraterritorial corporation and seating at the top-10 council.		 
Africa		<div></div>	0	Africa		 
America		<div></div>	0	America		 
Asia		<div></div>	0	Asia		 
Europe		<div></div>	0	Europe		 
IT		<div></div>	0	IT: softwares, hardware, cybersec		 
Oceania		<div></div>	0	Oceania		 
Russia		<div></div>	0	Russia and former USSR		 
biotechnology		<div></div>	0	Biotechnology: bioware, genetics, etc		 
cybertechnology		<div></div>	0	cybertechnology sector: manufacturing, selling and implanting modifications.		 
energy		<div></div>	0	energy sector: exploitation, , refining, selling		 

Page 1 of 1, showing 13 records out of 13 total, starting on record 1, ending on 13

« previous

next »

This is an initial install Powered by [MISP 2.4.120](#) Please configure and harden accordingly - 2020-03-02 10:55:00

Add a tag

All namespaces deprecated misp mitre-attack police policetaxo RPG

All clusters shadowrun

Submit

A nation-scale corporation.

AA only extraterritorial companies.

AAA

Africa Africa

America America

Asia Asia

Europe Europe

IT IT: softwares, hardware, cybersec

Oceania Oceania

Russia Russia and former USSR

Event Thread Link Code

Remark: we created a simple galaxy. We will later see how to create a Matrix-shaped one.

Matrix-shaped galaxy

To create a matrix-shaped galaxy, a new field is added:

- **kill_chain** for the /galaxy json
- **kill_chain_order** for the /cluster json

In the galaxy json, categories are listed:

```
"kill_chain": [
  "killchain_name": [
    "category_1",
    "category_2",
    "category_3"
  ]
]
```

The final galaxy file:

```
{
  "description": "My Shadowrun test matrix galaxy",
  "icon": "user-secret",
  "kill_chain_order": {
    "shadowrun": [
      "ranking",
      "sector",
      "area"
    ]
  },
  "name": "shadowrun_matrix",
  "namespace": "RPG",
  "type": "shadowrun",
  "uuid": "1b013b10-5c6e-11ea-8881-0800275bbff6",
  "version": 1
}
```

In the cluster json, reference to the categories are done:

```
"values": [
  {
    "description": "",
    "meta": {
      "kill_chain": [
        "killchain_name:category_1"
      ],

```

The final cluster file:

```

{
  "authors": [
    "myself"
  ],
  "category": "RPG",
  "description": "Shadowrun matrix galaxy",
  "name": "shadowrun corporations",
  "source": "Internal",
  "type": "shadowrun",
  "uuid": "1b013b10-5c6e-11ea-8881-0800275bbff6",
  "values": [
    {
      "description": "extraterritorial corporation and seating at the top-10 co
      "meta": {
        "kill_chain": [
          "shadowrun:ranking"
        ],
        "Corporate council seat": "Yes",
        "examples": [
          "Renraku",
          "Shiawase",
          "Aztechnology",
          "Ares Macrotechnologies",
          "Saeder Krupps"
        ]
      },
      "uuid": "43e1b900-5a03-11ea-9ad1-080027cbfd66",
      "value": "AAA"
    },
    {
      "description": "only extraterritorial compagnies.",
      "meta": {
        "kill_chain": [
          "shadowrun:ranking"
        ],
        "Corporate council seat": "No",
        "examples": [
          "Shibata",
          "Monobe",
          "Zeta Impchem",
          "ESUS"
        ]
      },
      "uuid": "7aad2dd4-5a03-11ea-ad69-080027cbfd66",
      "value": "AA"
    },
    {
      "description": "nation-scale corporation.",
      "meta": {
        "kill_chain": [
          "shadowrun:ranking"
        ],
        "Corporate council seat": "No",
        "examples": [
          "Genom",
          "KSAF",
          "Seretech",
          "Infocore",
          "MicroDek (ex-Microsoft)",
          "Tan Tien"
        ]
      },
      "uuid": "50c0d622-5c67-11ea-bd4b-0800275bbff6",
      "value": "A"
    },
  ],
}

```

```

{
  "description": "energy sector: exploitation, , refining, selling",
  "meta": {
    "kill_chain": [
      "shadowrun:sector"
    ],
    "examples": [
      "Saeder Krupps"
    ],
    "subsectors": [
      "petroleum",
      "electricity",
      "gas",
      "bio"
    ]
  },
  "uuid": "293e7e5c-51a8-411f-9b47-d52ed62d4b78",
  "value": "energy"
},
{
  "description": "cybertechnology sector: manufacturing, selling and implar",
  "meta": {
    "kill_chain": [
      "shadowrun:sector"
    ],
    "Delta clinic (for implanting)": [
      "Yes",
      "No"
    ],
    "examples": [
      "headware",
      "bodyware",
      "eyeware",
      "earware",
      "cyberlimbs"
    ]
  },
  "uuid": "7e962290-cba7-49ad-95c2-115575c8a9d2",
  "value": "cybertechnology"
},
{
  "description": "Biotechnology: bioware, genetics, etc",
  "meta": {
    "kill_chain": [
      "shadowrun:sector"
    ],
    "examples": [
      "bioware",
      "genetics",
      "biodrones",
      "biocosmetics"
    ]
  },
  "uuid": "c899564c-bfe4-460f-a2ed-aae98e1355a3",
  "value": "biotechnology"
},
{
  "description": "IT: softwares, hardware, cybersec",
  "meta": {
    "kill_chain": [
      "shadowrun:sector"
    ],
    "examples": [
      "software dev",
      "hardware manufacturing",
      "intrusion countermeasures"
    ]
  }
}

```

```

    ]
  },
  "uuid": "16c49ba4-8a79-4f67-a98a-07cdc08f8a2d",
  "value": "IT"
},
{
  "description": "Europe",
  "meta": {
    "kill_chain": [
      "shadowrun:area"
    ],
    "examples": [
      "France",
      "Belgium",
      "Luxembourg",
      "Germany",
      "Italy"
    ]
  },
  "uuid": "8e745c22-9b14-4334-887a-0000eda58f75",
  "value": "Europe"
},
{
  "description": "Asia",
  "meta": {
    "kill_chain": [
      "shadowrun:area"
    ],
    "examples": [
      "China",
      "Japan",
      "Thailand"
    ]
  },
  "uuid": "95d4ff78-42f8-4fe8-bb63-af2c7e500ec8",
  "value": "Asia"
},
{
  "description": "Russia and former USSR",
  "meta": {
    "kill_chain": [
      "shadowrun:area"
    ],
    "examples": [
      "Russia",
      "kazakhstan"
    ]
  },
  "uuid": "87a3ac08-6ffc-45eb-826e-e8e0af392563",
  "value": "Russia"
},
{
  "description": "Africa",
  "meta": {
    "kill_chain": [
      "shadowrun:area"
    ],
    "examples": [
      "Nigeria",
      "Malia",
      "Algeria"
    ]
  },
  "uuid": "aba705b7-fcb4-4bf4-81d4-b896314f53ed",
  "value": "Africa"
},

```

```
{
  "description": "Oceania",
  "meta": {
    "kill_chain": [
      "shadowrun:area"
    ],
    "examples": [
      "Asutralia",
      "Polynesia"
    ]
  },
  "uuid": "ae28830b-b90f-48d9-8b89-acda0864ff4e",
  "value": "Oceania"
},
{
  "description": "America",
  "meta": {
    "kill_chain": [
      "shadowrun:area"
    ],
    "examples": [
      "UCAS",
      "CAS",
      "Pueblo Corporate COuncil",
      "AZtlan"
    ]
  },
  "uuid": "d41c6222-4d10-43e9-9a8e-47d586eaf0e7",
  "value": "America"
}
],
"version": 4
}
```

The final result:

Ranking (2 items)	Sector (4 items)	Area (6 items)
A	IT	Africa
AA	biotechnology	America
AAA	cybertechnology	Asia
	energy	Europe
		Oceania
		Russia
Select Some Options		
Cancel		

Done! Eventually!

Dependencies

To create your own Galaxies the following tools are needed to run the validation scripts.

- jsonschema (>v2.4)
- jq
- moreutils (sponge)

On a Debian flavoured distribution you can potentially do this:

```
sudo apt install jq moreutils python3-jsonschema
sudo wget -O /usr/local/bin/jsonschema https://gist.githubusercontent.com/Steve
sudo chmod +x /usr/local/bin/jsonschema # This will only work with jsonschema >
```

Create a fork

To add your custom Galaxy it is preferable to [fork](#) the [misp-galaxy](#) repository. See above for details.

Understanding directory structure

Removing a Galaxy to better understand the add

Let's start with removing a single Galaxy.

```
cd /var/www/MISP/app/files/misp-galaxy
sudo -u www-data rm galaxies/android.json
sudo -u www-data rm clusters/android.json
sudo -u www-data /var/www/MISP/app/Console/cake Admin updateGalaxies force
```

After this you will have removed the android Galaxy Cluster.

Using Galaxies in MISP Events - Example

For this example, we will try to add a cluster to an existing event. This cluster contains information about threat actor known as Sneaky Panda.

Test Event

Event ID	790
Uuld	580b20cf-2d28-4b1c-bbc4-404a950d210f
Org	CIRCL
Owner org	CIRCL
Contributors	
Email	
Tags	admiralty-scale:information-credibility="1" x +
Date	2016-10-22
Threat Level	High
Analysis	Initial
Distribution	Your organisation only
Info	Test Event
Published	No
Sightings	1 (1)

☐ Pivots ☐ Galaxy ☐ Attributes ☐ Discussion

x 790: Test E...

Galaxies

Add new cluster

Here on the event view, we notice a blue frame under the metadatas with the title "Galaxies" and a button "Add new cluster". Let's click on the latter to begin.

Select Cluster Source
All Galaxies
Galaxy: Threat Actor
Galaxy: Tool
Cancel

A popup will appear proposing to explore a particular galaxy or all at the same time. Here, as we know we want to as a threat actor, we will choose the second option and scroll to find Sneaky Panda (We are courageous, aren't we?).

Select Cluster

search clusters...

Sandworm

ScarCruft

Scarlet Mimic

Shark Spider

Shell Crew

Silent Chollima

Sofacy

Spicy Panda

Stalker Panda

Stealth Falcon

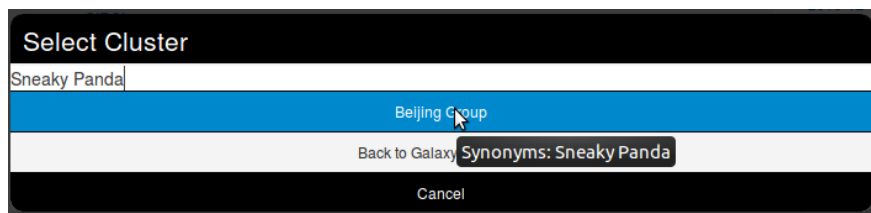
Stone Panda

Cancel

Wait. No Sneaky Panda? Hm that's strange. Or maybe it is only registred as a alias. Let's have a look! To do so we will use the search field which stay on top of the list. So what do we get? Beijing Group, is it an alias of our threat actor.

Select Cluster
Sneaky Panda
Beijing Group
Back to Galaxy Selection
Cancel

Pointing the cursor on it will give us the answer.



We have a match. So we select it and here we go.

Galaxies

Threat Actor

+ Beijing Group

Add new cluster

Clicking on the magnifying glass next to Threat actor redirects to the list of all threat actors Clicking on the magnifying glass next to Beijing Group redirects us to a page about this group Clicking on the addition symbol on the left of Beijing Group extends the module.

Available Galaxies

Clusters

[Android](#) - Android malware galaxy based on multiple open sources.

[Backdoor](#) - A list of backdoor malware.

[Banker](#) - A list of banker malware.

[Botnet](#) - botnet galaxy

[Branded vulnerability](#) - List of known vulnerabilities and attacks with a branding

[Cert eu govsector](#) - Cert EU GovSector

[Exploit kit](#) - Exploit-Kit is an enumeration of some exploitation kits used by adversaries. The list includes document, browser and router exploit kits.It's not meant to be totally exhaustive but aim at covering the most seen in the past 5 years

[Malpedia](#) - Malware galaxy cluster based on Malpedia.

[Microsoft activity group](#) - Activity groups as described by Microsoft

[Mitre attack pattern](#) - ATT&CK tactic

[Mitre course of action](#) - ATT&CK Mitigation

[Mitre enterprise attack attack pattern](#) - ATT&CK tactic

[Mitre enterprise attack course of action](#) - ATT&CK Mitigation

[Mitre enterprise attack intrusion set](#) - Name of ATT&CK Group

[Mitre enterprise attack malware](#) - Name of ATT&CK software

[Mitre enterprise attack tool](#) - Name of ATT&CK software

[Mitre intrusion set](#) - Name of ATT&CK Group

[Mitre malware](#) - Name of ATT&CK software

[Mitre mobile attack attack pattern](#) - ATT&CK tactic

[Mitre mobile attack course of action](#) - ATT&CK Mitigation

[Mitre mobile attack intrusion set](#) - Name of ATT&CK Group

[Mitre mobile attack malware](#) - Name of ATT&CK software

[Mitre mobile attack tool](#) - Name of ATT&CK software

[Mitre pre attack attack pattern](#) - ATT&CK tactic

Mitre pre attack intrusion set - Name of ATT&CK Group

Mitre tool - Name of ATT&CK software

Preventive measure - Preventive measures based on the ransomware document overview as published in

<https://docs.google.com/spreadsheets/d/1TWS238xacAto-fLK1n5uTsdijWdCEsGIM0Y0Hvmc5g/pubhtml#> . The preventive measures are quite generic and can fit any standard Windows infrastructure and their security measures.

Ransomware - Ransomware galaxy based on

<https://docs.google.com/spreadsheets/d/1TWS238xacAto-fLK1n5uTsdijWdCEsGIM0Y0Hvmc5g/pubhtml> and <http://pastebin.com/raw/GHgpWjar>

Rat - 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.

Sector - Activity sectors

Stealer - A list of malware stealer.

Tds - TDS is a list of Traffic Direction System used by adversaries

Threat actor - Known or estimated adversary groups targeting organizations and employees. Adversary groups are regularly confused with their initial operation or campaign.

Tool - threat-actor-tools is an enumeration of tools used by adversaries. The list includes malware but also common software regularly used by the adversaries.

Vocabularies

Common

Certainty level - Certainty level of an associated element or cluster.

Sector - List of activity sectors

Threat actor type - threat actor type vocab as defined by Cert EU.

Ttp category - ttp category vocab as defined by Cert EU.

Ttp type - ttp type vocab as defined by Cert EU.

threat-actor

Cert eu motive - Motive vocab as defined by Cert EU.

Intended effect - The IntendedEffectVocab is the default STIX vocabulary for expressing the intended effect of a threat actor

Motivation - The MotivationVocab is the default STIX vocabulary for expressing the motivation of a threat actor.

Planning and operational support - The PlanningAndOperationalSupportVocab is the default STIX vocabulary for expressing the planning and operational support functions available to a threat actor.

Sophistication - The ThreatActorSophisticationVocab enumeration is used to define the default STIX vocabulary for expressing the subjective level of sophistication of a threat actor.

Type - The ThreatActorTypeVocab enumeration is used to define the default STIX vocabulary for expressing the subjective type of a threat actor.

Last modified: Thu Mar 04 2021 14:48:45 GMT+0100 (Central European Standard Time)

- [MISP Objects](#)
 - [Using objects](#)
 - [Creating object](#)

MISP Objects

[MISP objects](#) to be used in MISP (2.4.80) system and can be used by other information sharing tool. [MISP objects](#) are in addition to MISP attributes to allow advanced combinations and concatenation of attributes. The creation of these objects and their associated attributes are based on real cyber security use-cases and existing practices in information sharing.

Using objects

Objects can be added by using the side menu:

View Event

View Correlation Graph

View Event History

Edit Event

Delete Event

Add Attribute

Add Object

Add Attachment

Populate from...

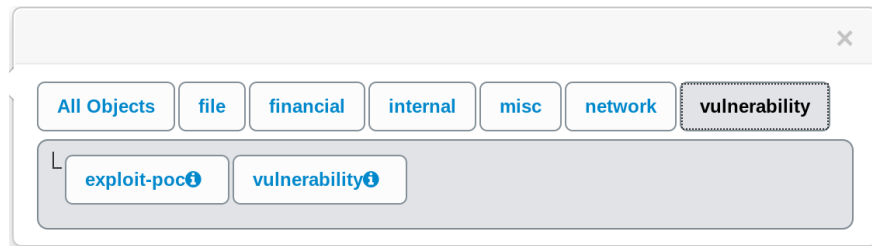
Merge attributes from...

This will open a popup where you can choose the type of object:

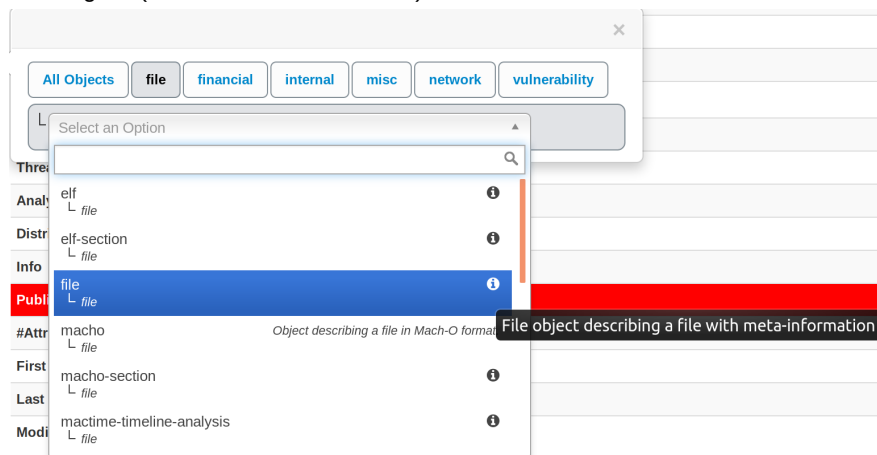
[Edit Event](#)
[Delete Event](#)
[Add Attribute](#)
[Add Object](#)
[Add Attachment](#)
[Populate from](#)

The screenshot shows a web interface with a sidebar on the left containing links: [Edit Event](#), [Delete Event](#), [Add Attribute](#), [Add Object](#), [Add Attachment](#), and [Populate from](#). The main area displays a form with two input fields: 'UUID' and 'Creator org', both containing redacted black text. Below these fields is a modal window with a close button (X) in the top right corner. The modal contains a horizontal row of seven buttons: 'All Objects', 'file', 'financial', 'internal', 'misc', 'network', and 'vulnerability'. The 'vulnerability' button is currently selected and highlighted with a blue background.

If there are only few templates available for this type, they will all be shown this way:



Otherwise you will be able to search and select the desired object within a scrolling list (a search field is available)



A description of each object is shown by hovering the info icon or directly besides it.

For this example we will try to add an ip|port object:

Add Ip|port Object

Object Template

ip|port v3

Description

An IP address and a port seen as a tuple (or as a triple) in a specific time frame.

Requirements

Required: ip
Required one of: del-port, src-port

Meta category

Network

Distribution

Inherent event

Comment

Save	Name	Type	Description	Category	Value	IDB	Distribution	Comment
<input checked="" type="checkbox"/>	Del-port	port	Destination port	Network activity	123	<input type="checkbox"/>	Inherent event	
<input checked="" type="checkbox"/>	ip src-port	IP Address	IP Address	Network activity	1.2.3.4	<input checked="" type="checkbox"/>	Inherent event	
<input type="checkbox"/>	Src-port	port	Source port	Network activity		<input type="checkbox"/>	Inherent event	
<input type="checkbox"/>	First-seen	datetime	First time the tuple has been seen	Other		<input type="checkbox"/>	Inherent event	
<input type="checkbox"/>	Last-seen	datetime	Last time the tuple has been seen	Other		<input type="checkbox"/>	Inherent event	
<input type="checkbox"/>	Text	text	Description of the tuple	Other		<input type="checkbox"/>	Inherent event	

Submit

Note: This screenshot displays an old version of the template For some objects, there might be attributes that required to be set. For instance in this object, there is a required attribute, "Ip", and it is also required to set one of the attributes between "dst-port" and "src-port". If these requirements are not met, the object will not be valid and therefore not added to the event. Also you can't add an object without setting any attribute.

After pressing "Submit, you are given the possibility to review your object before saving it.

Object pre-save review

Make sure that the below Object reflects your expectation before submitting it.

Name	ip-port					
Meta-category	network					
Distribution	Inherit event					
Comment						

Attribute	Category	Type	Value	To IDS	Comment	UUID	Distribution
dst-port	Network activity	port	123	No			Inherit event
ip	Network activity	ip-dst	1.2.3.4	Yes			Inherit event

Creating object

An object is designed using a JSON file which should respect a format described in [this document](#).

An object is basically a combination of two or more attributes that can be used together to represent real cyber security use-cases. These attributes are listed in a JSON object.

Each attribute is an JSON object defined by a name, a description, a misp-attribute and an ui-priority value.

- Name and description are self-explanatory.
- misp-attribute is an existing type of attribute in misp that matches the attribute.
- Concerning ui-priority, the higher the number is, the most it is expected to be seen.

There are also others options that can be added to define an attribute more precisely.

- sane_default is a list of default valid value for this attribute. The user can pick a value from this list or choose "Enter value manually"
- disable_correlation will disable correlation for this value. Useful for dates for instance
- recommended value for this field
- multiple, if set to true, allow the user to add multiple instances of this attribute.

Not all attributes are mandatory, but some can be required. If so, they need to be listed in a list called "required". The object will only be valid if the listed attributes are set. The same way, there are sometimes when only one attribute in a set is needed. This set can be put in a list called "requiredOneOf". If at least one of the attributes in this list is set, the object will be valid.

Last modified: Sun Feb 28 2021 09:22:59 GMT+0100 (Central European Standard Time)

- [Sightings](#)
 - [Explanation](#)
 - [Using sightings on an event \(GUI\)](#)
 - [Advanced sightings](#)
 - [At Event level](#)
 - [Using sightings on an event \(API\)](#)

Sightings

Basically, sighting is a system allowing people to react on attributes on an event. It was originally designed to provide an easy method for user to tell when they see a given attribute, giving it more credibility.

Now sightings have been improved to also provide a method to signal false positives, but also to give an expiration date for some attributes.

Explanation

As said before, Sighting is a way for a user to say that they have seen or notice an attribute and confirm its validity. An attribute can be spotted several times by the same user, that is why a single user can use sighting several times on a single attribute.

Sometimes, some attributes can be considered as false positives, even if the false positive list do not detect them (for instance, if the IDS flag is set to false) so they can also be notified. As well as concerning sighting, the same user can signal a single attribute as a false positive several times.

It also happens that some attributes are only valid a certain time (for instance, in case of a phishing campaign that is assumed to be up for only one week). In this case, people can also assign an expiration date to an attribute, but this time, there can be only one valid expiration date per *organisation*.

Using sightings on an event (GUI)

Sighting is applied to every attribute, under the column "Sightings", easily identifiable with its colored number. This column shows three icons and three values.

Date	Org	Category	Type	Value	Tags	Comment	Correlate	Related Events	IDS	Distribution	Sightings	Activity	Actions
2017-04-03		Network activity	ip-src	123.56.76.7					No	Inherit	(0/0/0)		

These three values show respectively:

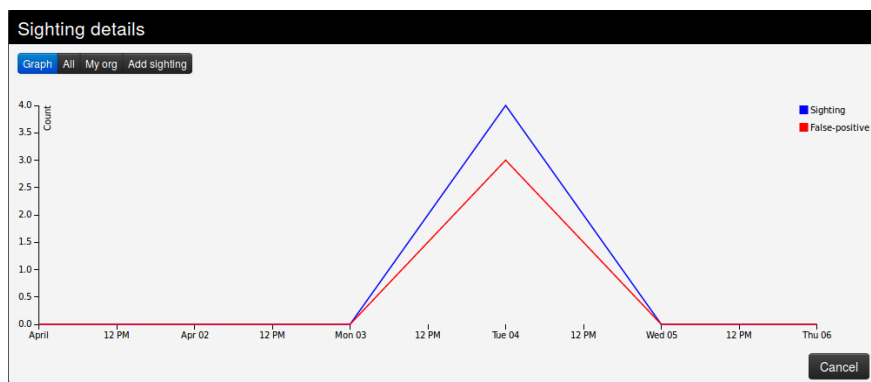
- The number of true positives detected with the attribute, in green. Malicious activity as described in the event.
- The number of times the attribute has been marked as false positive, in red. Non-malicious activity or incorrect detection.
- The number of different expiration dates that have been affected on this attribute, in orange

Concerning the three icons:

- The first one (Thumb up) allows to add a sighting (true positive) on an attribute.
- The second one (Thumb down) allows to mark the attribute as a false positive.
- The third one (Tool) opens a popup for advanced sightings, showing sightings details and allowing different actions.

Advanced sightings

- The first tab, "Graph", represents a line graph showing the evolution of sightings and false positives over time.



- The second tab gives a quick view of all the sightings applied to the attribute.

Sighting details

GraphAllMy orgAdd sighting

Date	Organisation	Type	Source	Event ID	Attribute ID	Actions
2017-04-22 08:14:03	Setec Astronomy	Expiration		1120	303398	
2017-04-07 08:09:28		Expiration		1120	303398	
2017-04-04 08:43:25		Sighting		1120	303398	
2017-04-04 08:10:47	Setec Astronomy	False-positive		1120	303398	
2017-04-04 08:10:46	Setec Astronomy	False-positive		1120	303398	
2017-04-04 08:10:45	Setec Astronomy	Sighting		1120	303398	
2017-04-04 08:10:31	Setec Astronomy	Sighting		1120	303398	
2017-04-04 07:50:00		False-positive		1120	303398	
2017-04-04 07:49:58		Sighting		1120	303398	

Cancel

- The third tab gives a quick view of the sightings applied to the attribute by your own organisation only.

Sighting details						
Graph All My org Add sighting						
Date	Organisation	Type	Source	Event ID	Attribute ID	Actions
2017-04-07 08:09:28		Expiration		1120	303398	
2017-04-04 08:43:25		Sighting		1120	303398	
2017-04-04 07:50:00		False-positive		1120	303398	
2017-04-04 07:49:58		Sighting		1120	303398	
						Cancel

- The last tab can be used to add either a sighting, mark the attribute as a false positive, or define an expiration date. You can precise both the date and time of day, as well as note a particular source where the sighting comes from.

The screenshot shows a web interface titled "Sighting details". At the top, there are tabs: "Graph", "All", "My org", and "Add sighting" (which is highlighted in blue). Below the tabs is the "Add Sighting" section. It contains a form with the following fields:

Type	Source	Sighting Date
<div><div>Sighting</div><div>Sighting</div><div>False-positive</div><div>Expiration</div></div>	honeypot, IDS sensor id, SIEM,...	2017-04-06 10:09:07

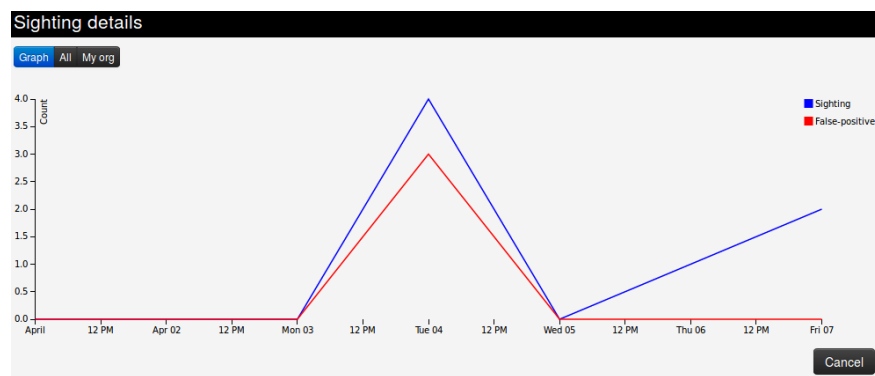
At the bottom right of the form, there are two buttons: "Add" (in blue) and "Cancel" (in grey).

At Event level

The total number of sightings is also visible as part of the metadata in front of the Sightings label, as well as a sparkline graph that summarize the evolution of sightings.



Clicking on the tool will show sighting details for the whole event.



Using sightings on an event (API)

Please have a look at the [automation API](#)

Last modified: Wed May 12 2021 13:53:36 GMT+0200 (Central European Summer Time)

- [MISP warninglists](#)
 - [MISP warning lists introduction: The dilemma of false-positive](#)
 - [Usage](#)
 - [Warninglists and data export](#)
 - [Check individual values for warning list hits](#)
 - [Updating warninglists](#)
 - [Creating a custom warninglist](#)

MISP warninglists

[MISP warninglists](#) are lists of well-known [indicators](#) that can be associated to potential false positives, errors or mistakes. There is a Python module available to work with warninglists in a Pythonic way called [PyMISPWarningLists](#). [MISP warninglists GitHub Repo](#)

MISP warning lists introduction: The dilemma of false-positive

- False-positives are a common issue in threat intelligence sharing.
- It's often a contextual issue:
 - False-positives might be different per [community](#) of users sharing information.
 - Organizations might have their own view on false-positives.

Usage

By default MISP will only trigger hits for warninglists if the attribute IDS flag is set. This behaviour can be changed by setting the MISP config parameter `MISP.warning_for_all` to true.

When an attribute matches a warninglist entry, an info/warning box is displayed at the event and attribute level, as can be seen in the screenshot below.

366

Individual warninglists can be enabled or disabled at instance level using the warninglists index page. Examples of default warning lists are known public DNS resolvers, multicast IP addresses, hashes for empty values, rfc1918, TLDs or known google domains.

Warninglists

< previous

next >

All	Enabled	Disabled						
ID / T	Name	Version	Description	Type	Valid attributes	Enter value to search	Filter	
						Entries	Enabled	Actions
60	List of known Windows address ranges	20201123	Windows address ranges: https://msc.ulm.edu/cg/universite-prpa.php#tbl	cidr	ip-src, ip-dst, domain/ip	44	X	
59	List of known domains to have external IP	0	Event contains one or more entries of known where my ip domain	hostname	domain, hostname, domain_ip, url	231	X	
58	Specialized list of IPv4 addresses belonging to common VPN providers and datacenters	20201123	Specialized list of IPv4 addresses belonging to common VPN providers and datacenters	cidr	ip-src, ip-dst, domain/ip	3008	X	
57	Specialized list of IPv4 addresses belonging to common VPN providers and datacenters	20201123	Specialized list of IPv4 addresses belonging to common VPN providers and datacenters	cidr	ip-src, ip-dst, domain/ip	13014	X	

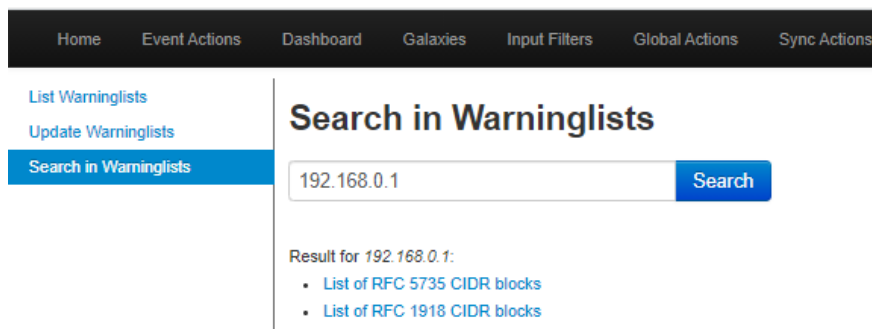
The warning lists can be expanded or added in JSON locally or via [pull](#) requests (<https://github.com/MISP/misp-warninglists>). Warning lists can also be used for critical or core infrastructure or personally identifiable information.

Warninglists and data export

The `enforceWarninglist` parameter of MISP `restSearch` can be used to exclude attributes that have a warninglist hit from the export. For more information on the MISP [API](#), please refer to the [Automation and MISP API chapter](#).

Check individual values for warning list hits

It is also possible to do a lookup for a specific value in the warninglists. This functionality is accessible by using the top menu "Input Filters" > "List Warninglists" and then using the link in the left side menu bar (or by browsing directly to `[misp_base_url]/warninglists/checkValue`). Only enabled warninglists will be searched.



The screenshot shows the MISP web interface. At the top is a navigation bar with links: Home, Event Actions, Dashboard, Galaxies, Input Filters, Global Actions, and Sync Actions. On the left side, there is a menu with three items: "List Warninglists", "Update Warninglists", and "Search in Warninglists" (which is highlighted with a blue background). The main content area is titled "Search in Warninglists". It features a search input field containing the IP address "192.168.0.1" and a blue "Search" button. Below the search field, the results are displayed under the heading "Result for 192.168.0.1:". There are two bullet points, each with a blue link: "List of RFC 5735 CIDR blocks" and "List of RFC 1918 CIDR blocks".

Updating warninglists

An update of the warninglists can be triggered via the GUI using the "Update Warninglists" button in the side menu bar when viewing any of the relevant warninglists pages, for example the index page.

Alternatively, it is also possible to trigger an update using a CLI command.

```
MISP/app/Console/cake Admin updateWarningLists
```

If you are updating an existing warninglist, make sure you incremented the version number before triggering the update on the MISP. You can also contribute to the existing warninglists by forking [MISP warninglists GitHub Repo](#), making changes and then creating a [pull](#) request.

Creating a custom warninglist

1. Create a new directory for your warninglist in `/var/www/MISP/app/files/warninglists`.
2. Add a file called `list.json` to the newly created directory and add the content you want. You can use any of the existing warning lists in <https://github.com/MISP/misp-warninglists> as reference.
3. Trigger an update of the warning lists on the instance to load in your new warning list.

Example use cases are a list of domain names owned by you or your organisation or employee email addresses.

Last modified: Sun Feb 28 2021 09:22:59 GMT+0100 (Central European Standard Time)

- [MISP noticelist](#)

MISP noticelist

Notice lists to inform MISP users of the legal, privacy, policy or even technical implications of using specific attributes, categories or objects. [MISP noticelist GitHub Repo](#)

MISP Noticelists are a simple JSON description to trigger warning notifications to make the user more aware of eventual implications of her actions.

Last modified: Sun Feb 28 2021 09:22:59 GMT+0100 (Central European Standard Time)

- [Attribute Categories vs. Types](#)
- [Categories](#)
- [Types](#)

Attribute Categories vs. Types

Category	Internal reference	Targeting data	Antivirus detection	Payload delivery
md5				X
sha1				X
sha256				X
filename				X
pdb				
filename md5				X
filename sha1				X
filename sha256				X
ip-src				X
ip-dst				X
hostname				X
domain				X
domain ip				
email				X
email-src				X
eppn				
email-dst				X
email-subject				X
email-attachment				X
email-body				X
float				
git-commit-id	X			
url				X
http-method				
user-agent				X
ja3-fingerprint-md5				X
jarm-fingerprint				X
favicon-mmh3				
hassh-md5				X
hasshserver-md5				X
regkey				
regkey value				

Category	Internal reference	Targeting data	Antivirus detection	Payload delivery
AS				X
snort				
bro				
zeek				
community-id				
pattern-in-file				X
pattern-in-traffic				X
pattern-in-memory				
pattern-filename				
pgp-public-key				
pgp-private-key				
yara				X
stix2-pattern				X
sigma				X
gene				
kusto-query				
mime-type				X
identity-card-number				
cookie				
vulnerability				X
cpe				X
weakness				X
attachment			X	X
malware-sample				X
link	X		X	X
comment	X	X	X	X
text	X		X	X
hex	X		X	X
other	X		X	X
named pipe				
mutex				
process-state				

Category	Internal reference	Targeting data	Antivirus detection	Paylo delive
target-user		X		
target-email		X		
target-machine		X		
target-org		X		
target-location		X		
target-external		X		
btc				
dash				
xmr				
iban				
bic				
bank-account-nr				
aba-rtn				
bin				
cc-number				
prtn				
phone-number				
threat-actor				
campaign-name				
campaign-id				
malware-type				X
uri				
authentihash				X
vhash				X
ssdeep				X
imphash				X
telfhash				X
pehash				X
impfuzzy				X
sha224				X
sha384				X
sha512				X

Category	Internal reference	Targeting data	Antivirus detection	Payload delivery
sha512/224				X
sha512/256				X
sha3-224				X
sha3-256				X
sha3-384				X
sha3-512				X
tlsh				X
cdhash				X
filename authentihash				X
filename vhash				X
filename ssdeep				X
filename imphash				X
filename impfuzzy				X
filename pehash				X
filename sha224				X
filename sha384				X
filename sha512				X
filename sha512/224				X
filename sha512/256				X
filename sha3-224				X
filename sha3-256				X
filename sha3-384				X
filename sha3-512				X
filename tlsh				X
windows-scheduled-task				
windows-service-name				
windows-service-displayname				
whois-registrant-email				X
whois-registrant-phone				
whois-registrant-name				

Category	Internal reference	Targeting data	Antivirus detection	Payload delivery
whois-registrant-org				
whois-registrar				
whois-creation-date				
x509-fingerprint-sha1				X
x509-fingerprint-md5				X
x509-fingerprint-sha256				X
dns-soa-email				
size-in-bytes				
counter				
datetime				
port				
ip-dst port				X
ip-src port				X
hostname port				X
mac-address				X
mac-eui-64				X
email-dst-display-name				X
email-src-display-name				X
email-header				X
email-reply-to				X
email-x-mailer				X
email-mime-boundary				X
email-thread-index				X
email-message-id				X
github-username				
github-repository				
github-organisation				
jabber-id				
twitter-id				
dkim				
dkim-signature				

Category	Internal reference	Targeting data	Antivirus detection	Payload delivery
first-name				
middle-name				
last-name				
date-of-birth				
place-of-birth				
gender				
passport-number				
passport-country				
passport-expiration				
redress-number				
nationality				
visa-number				
issue-date-of-the-visa				
primary-residence				
country-of-residence				
special-service-request				
frequent-flyer-number				
travel-details				
payment-details				
place-port-of-original-embarkation				
place-port-of-clearance				
place-port-of-onward-foreign-destination				
passenger-name-record-locator-number				
mobile-application-id				X
chrome-extension-id				X
cortex				
boolean				
anonymised	X	X	X	X

Category	Persistence mechanism	Network activity	Payload type	Attrib
md5				
sha1				
sha256				
filename	X			
pdb				
filename md5				
filename sha1				
filename sha256				
ip-src		X		
ip-dst		X		
hostname		X		
domain		X		
domain ip		X		
email		X		X
email-src		X		
eppn		X		
email-dst		X		
email-subject		X		
email-attachment				
email-body				
float				
git-commit-id				
url		X		
http-method		X		
user-agent		X		
ja3-fingerprint-md5		X		
jarm-fingerprint		X		
favicon-mmh3		X		
hassh-md5		X		
hasshserver-md5		X		
regkey	X			
regkey value	X			

Category	Persistence mechanism	Network activity	Payload type	Attrib
AS		X		
snort		X		
bro		X		
zeek		X		
community-id		X		
pattern-in-file		X		
pattern-in-traffic		X		
pattern-in-memory				
pattern-filename				
pgp-public-key				
pgp-private-key				
yara				
stix2-pattern		X		
sigma				
gene				
kusto-query				
mime-type				
identity-card-number				
cookie		X		
vulnerability				
cpe				
weakness				
attachment		X		
malware-sample				
link				
comment	X	X	X	X
text	X	X	X	X
hex	X	X		
other	X	X	X	X
named pipe				
mutex				
process-state				

Category	Persistence mechanism	Network activity	Payload type	Attrib
target-user				
target-email				
target-machine				
target-org				
target-location				
target-external				
btc				
dash				
xmr				
iban				
bic				
bank-account-nr				
aba-rtn				
bin				
cc-number				
prtn				
phone-number				
threat-actor				x
campaign-name				x
campaign-id				x
malware-type				
uri		X		
authentihash				
vhash				
ssdeep				
imphash				
telfhash				
pehash				
impfuzzy				
sha224				
sha384				
sha512				

Category	Persistence mechanism	Network activity	Payload type	Attrib
sha512/224				
sha512/256				
sha3-224				
sha3-256				
sha3-384				
sha3-512				
tlsh				
cdhash				
filename authentihash				
filename vhash				
filename ssdeep				
filename imphash				
filename impfuzzy				
filename pehash				
filename sha224				
filename sha384				
filename sha512				
filename sha512/224				
filename sha512/256				
filename sha3-224				
filename sha3-256				
filename sha3-384				
filename sha3-512				
filename tlsh				
windows-scheduled-task				
windows-service-name				
windows-service-displayname				
whois-registrant-email				x
whois-registrant-phone				x
whois-registrant-name				x

Category	Persistence mechanism	Network activity	Payload type	Attrib
whois-registrant-org				x
whois-registrar				x
whois-creation-date				x
x509-fingerprint-sha1		X		x
x509-fingerprint-md5		X		x
x509-fingerprint-sha256		X		x
dns-soa-email				x
size-in-bytes				
counter				
datetime				
port		X		
ip-dst port		X		
ip-src port		X		
hostname port		X		
mac-address		X		
mac-eui-64		X		
email-dst-display-name				
email-src-display-name				
email-header				
email-reply-to				
email-x-mailer				
email-mime-boundary				
email-thread-index				
email-message-id				
github-username				
github-repository				
github-organisation				
jabber-id				
twitter-id				
dkim		X		
dkim-signature		X		

Category	Persistence mechanism	Network activity	Payload type	Attrib
first-name				
middle-name				
last-name				
date-of-birth				
place-of-birth				
gender				
passport-number				
passport-country				
passport-expiration				
redress-number				
nationality				
visa-number				
issue-date-of-the-visa				
primary-residence				
country-of-residence				
special-service-request				
frequent-flyer-number				
travel-details				
payment-details				
place-port-of-original-embarkation				
place-port-of-clearance				
place-port-of-onward-foreign-destination				
passenger-name-record-locator-number				
mobile-application-id				
chrome-extension-id				
cortex				
boolean				
anonymised	X	X	X	X

Category	Support Tool	Social network	Person	Other
md5				
sha1				
sha256				
filename				
pdb				
filename md5				
filename sha1				
filename sha256				
ip-src				
ip-dst				
hostname				
domain				
domain ip				
email		X	X	
email-src		X		
eppn		X		
email-dst		X		
email-subject				
email-attachment				
email-body				
float				X
git-commit-id				
url				
http-method				
user-agent				
ja3-fingerprint-md5				
jarm-fingerprint				
favicon-mmh3				
hassh-md5				
hasshserver-md5				
regkey				
regkey value				

Category	Support Tool	Social network	Person	Other
AS				
snort				
bro				
zeek				
community-id				
pattern-in-file				
pattern-in-traffic				
pattern-in-memory				
pattern-filename				
pgp-public-key		X	X	X
pgp-private-key		X	X	X
yara				
stix2-pattern				
sigma				
gene				
kusto-query				
mime-type				
identity-card-number			X	
cookie				
vulnerability				
cpe				X
weakness				
attachment	X			
malware-sample				
link	X			
comment	X	X	X	X
text	X	X	X	X
hex	X			X
other	X	X	X	X
named pipe				
mutex				
process-state				

Category	Support Tool	Social network	Person	Other
target-user				
target-email				
target-machine				
target-org				
target-location				
target-external				
btc				
dash				
xmr				
iban				
bic				
bank-account-nr				
aba-rtn				
bin				
cc-number				
prtn				
phone-number			X	X
threat-actor				
campaign-name				
campaign-id				
malware-type				
uri				
authentihash				
vhash				
ssdeep				
imphash				
telfhash				
pehash				
impfuzzy				
sha224				
sha384				
sha512				

Category	Support Tool	Social network	Person	Other
sha512/224				
sha512/256				
sha3-224				
sha3-256				
sha3-384				
sha3-512				
tlsh				
cdhash				
filename authentihash				
filename vhash				
filename ssdeep				
filename imphash				
filename impfuzzy				
filename pehash				
filename sha224				
filename sha384				
filename sha512				
filename sha512/224				
filename sha512/256				
filename sha3-224				
filename sha3-256				
filename sha3-384				
filename sha3-512				
filename tlsh				
windows-scheduled-task				
windows-service-name				
windows-service-displayname				
whois-registrant-email		X		
whois-registrant-phone				
whois-registrant-name				
whois-registrant-org				

Category	Support Tool	Social network	Person	Other
whois-registrar				
whois-creation-date				
x509-fingerprint-sha1				
x509-fingerprint-md5				
x509-fingerprint-sha256				
dns-soa-email				
size-in-bytes				X
counter				X
datetime				X
port				X
ip-dst port				
ip-src port				
hostname port				
mac-address				
mac-eui-64				
email-dst-display-name				
email-src-display-name				
email-header				
email-reply-to				
email-x-mailer				
email-mime-boundary				
email-thread-index				
email-message-id				
github-username		X		
github-repository		X		
github-organisation		X		
jabber-id		X		
twitter-id		X		
dkim				
dkim-signature				
first-name			X	
middle-name			X	

Category	Support Tool	Social network	Person	Other
last-name			X	
date-of-birth			X	
place-of-birth			X	
gender			X	
passport-number			X	
passport-country			X	
passport-expiration			X	
redress-number			X	
nationality			X	
visa-number			X	
issue-date-of-the-visa			X	
primary-residence			X	
country-of-residence			X	
special-service-request			X	
frequent-flyer-number			X	
travel-details			X	
payment-details			X	
place-port-of-original-embarkation			X	
place-port-of-clearance			X	
place-port-of-onward-foreign-destination			X	
passenger-name-record-locator-number			X	
mobile-application-id				
chrome-extension-id				
cortex				
boolean				X
anonymised	X	X	X	X

Categories

- **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

Types

- **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
- **email-attachment**: File name of the email attachment.
- **email-body**: Email body
- **float**: A floating point value.
- **git-commit-id**: A git commit ID.
- **url**: url
- **http-method**: HTTP method used by the malware (e.g. POST, GET, ...).
- **user-agent**: The user-agent used by the malware in the HTTP request.
- **ja3-fingerprint-md5**: JA3 is a method for creating SSL/TLS client fingerprints that should be easy to produce on any platform and can be easily shared for threat intelligence.
- **jarm-fingerprint**: JARM is a method for creating SSL/TLS server fingerprints.
- **favicon-mmh3**: favicon-mmh3 is the murmur3 hash of a favicon as used in Shodan.
- **hassh-md5**: hassh is a network fingerprinting standard which can be used to identify specific Client SSH implementations. The fingerprints can be easily stored, searched and shared in the form of an MD5 fingerprint.
- **hasshserver-md5**: hasshServer is a network fingerprinting standard which can be used to identify specific Server SSH implementations. The fingerprints can be easily stored, searched and shared in the form of an MD5 fingerprint.
- **regkey**: Registry key or value
- **regkey|value**: Registry value + data separated by |
- **AS**: Autonomous system
- **snort**: An IDS rule in Snort rule-format. This rule will be automatically rewritten in the [NIDS](#) exports.
- **bro**: An [NIDS](#) rule in the Bro rule-format.
- **zeek**: An [NIDS](#) rule in the Zeek rule-format.
- **community-id**: a [community](#) ID flow hashing algorithm to map multiple traffic monitors into common flow id
- **pattern-in-file**: Pattern in file that identifies the malware
- **pattern-in-traffic**: Pattern in network traffic that identifies the malware
- **pattern-in-memory**: Pattern in memory dump that identifies the malware
- **pattern-filename**: A pattern in the name of a file

- **pgp-public-key**: A PGP public key
- **pgp-private-key**: A PGP private key
- **yara**: Yara signature
- **stix2-pattern**: STIX 2 pattern
- **sigma**: Sigma - Generic Signature Format for SIEM Systems
- **gene**: GENE - Go Evtx sigNature Engine
- **kusto-query**: Kusto query - Kusto from Microsoft Azure is a service for storing and running interactive analytics over Big Data.
- **mime-type**: A media type (also MIME type and content type) is a two-part identifier for file formats and format contents transmitted on the Internet
- **identity-card-number**: Identity card number
- **cookie**: HTTP cookie as often stored on the user web client. This can include authentication cookie or session cookie.
- **vulnerability**: A reference to the vulnerability used in the exploit
- **cpe**: Common Platform Enumeration - structured naming scheme for information technology systems, software, and packages.
- **weakness**: A reference to the weakness used in the exploit
- **attachment**: Please upload files using the *Upload Attachment* button.
- **malware-sample**: Please upload files using the *Upload Attachment* button.
- **link**: Link to an external information
- **comment**: Comment or description in a human language. This will not be correlated with other attributes
- **text**: Name, ID or a reference
- **hex**: A value in hexadecimal format
- **other**: Other attribute
- **named pipe**: Named pipe, use the format `.pipe\`
- **mutex**: Mutex, use the format `\BaseNamedObjects\`
- **process-state**: State of a process
- **target-user**: Attack Targets Username(s)
- **target-email**: Attack Targets Email(s)
- **target-machine**: Attack Targets Machine Name(s)
- **target-org**: Attack Targets Department or Organization(s)
- **target-location**: Attack Targets Physical Location(s)
- **target-external**: External Target Organizations Affected by this Attack
- **btc**: Bitcoin Address
- **dash**: Dash Address
- **xmr**: Monero Address
- **iban**: International Bank Account Number
- **bic**: Bank Identifier Code Number also known as SWIFT-BIC, SWIFT code or ISO 9362 code
- **bank-account-nr**: Bank account number without any routing number
- **aba-rtn**: ABA routing transit number
- **bin**: Bank Identification Number
- **cc-number**: Credit-Card Number
- **prtn**: Premium-Rate Telephone Number
- **phone-number**: Telephone Number
- **threat-actor**: A string identifying the threat actor
- **campaign-name**: Associated campaign name

- **campaign-id**: Associated campaign ID
- **malware-type**:
- **uri**: Uniform Resource Identifier
- **authentihash**: You are encouraged to use filename|authentihash instead. Authenticode executable signature hash, only use this if you don't know the correct filename
- **vhash**: You are encouraged to use filename|vhash instead. A checksum from VirusTotal, only use this if you don't know the correct filename
- **ssdeep**: You are encouraged to use filename|ssdeep instead. A checksum in the SSDeep format, only use this if you don't know the correct filename
- **imphash**: You are encouraged to use filename|imphash instead. A hash created based on the imports in the sample, only use this if you don't know the correct filename
- **telfhash**: You are encouraged to use a file object with telfash
- **pehash**: PEhash - a hash calculated based of certain pieces of a PE executable file
- **impfuzzy**: You are encouraged to use filename|impfuzzy instead. A fuzzy hash created based on the imports in the sample, only use this if you don't know the correct filename
- **sha224**: You are encouraged to use filename|sha224 instead. A checksum in sha224 format, only use this if you don't know the correct filename
- **sha384**: You are encouraged to use filename|sha384 instead. A checksum in sha384 format, only use this if you don't know the correct filename
- **sha512**: You are encouraged to use filename|sha512 instead. A checksum in sha512 format, only use this if you don't know the correct filename
- **sha512/224**: You are encouraged to use filename|sha512/224 instead. A checksum in sha512/224 format, only use this if you don't know the correct filename
- **sha512/256**: You are encouraged to use filename|sha512/256 instead. A checksum in sha512/256 format, only use this if you don't know the correct filename
- **sha3-224**: You are encouraged to use filename|sha3-224 instead. A checksum in sha3-224 format, only use this if you don't know the correct filename
- **sha3-256**: You are encouraged to use filename|sha3-256 instead. A checksum in sha3-256 format, only use this if you don't know the correct filename
- **sha3-384**: You are encouraged to use filename|sha3-384 instead. A checksum in sha3-384 format, only use this if you don't know the correct filename
- **sha3-512**: You are encouraged to use filename|sha3-512 instead. A checksum in sha3-512 format, only use this if you don't know the correct filename
- **tlsh**: You are encouraged to use filename|tlsh instead. A checksum in the Trend Micro Locality Sensitive Hash format, only use this if you don't know the correct filename
- **cdhash**: An Apple Code Directory Hash, identifying a code-signed Mach-O executable file

- **filename|authentihash**: A checksum in md5 format
- **filename|vhash**: A filename and a VirusTotal hash separated by a |
- **filename|ssdeep**: A checksum in ssdeep format
- **filename|imphash**: Import hash - a hash created based on the imports in the sample.
- **filename|impfuzzy**: Import fuzzy hash - a fuzzy hash created based on the imports in the sample.
- **filename|pehash**: A filename and a PEhash separated by a |
- **filename|sha224**: A filename and a sha-224 hash separated by a |
- **filename|sha384**: A filename and a sha-384 hash separated by a |
- **filename|sha512**: A filename and a sha-512 hash separated by a |
- **filename|sha512/224**: A filename and a sha-512/224 hash separated by a |
- **filename|sha512/256**: A filename and a sha-512/256 hash separated by a |
- **filename|sha3-224**: A filename and an sha3-224 hash separated by a |
- **filename|sha3-256**: A filename and an sha3-256 hash separated by a |
- **filename|sha3-384**: A filename and an sha3-384 hash separated by a |
- **filename|sha3-512**: A filename and an sha3-512 hash separated by a |
- **filename|tlsh**: A filename and a Trend Micro Locality Sensitive Hash separated by a |
- **windows-scheduled-task**: A scheduled task in windows
- **windows-service-name**: A windows service name. This is the name used internally by windows. Not to be confused with the windows-service-displayname.
- **windows-service-displayname**: A windows service's displayname, not to be confused with the windows-service-name. This is the name that applications will generally display as the service's name in applications.
- **whois-registrant-email**: The e-mail of a domain's registrant, obtained from the WHOIS information.
- **whois-registrant-phone**: The phone number of a domain's registrant, obtained from the WHOIS information.
- **whois-registrant-name**: The name of a domain's registrant, obtained from the WHOIS information.
- **whois-registrant-org**: The org of a domain's registrant, obtained from the WHOIS information.
- **whois-registrar**: The registrar of the domain, obtained from the WHOIS information.
- **whois-creation-date**: The date of domain's creation, obtained from the WHOIS information.
- **x509-fingerprint-sha1**: X509 fingerprint in SHA-1 format
- **x509-fingerprint-md5**: X509 fingerprint in MD5 format
- **x509-fingerprint-sha256**: X509 fingerprint in SHA-256 format
- **dns-soa-email**: RFC1035 mandates that DNS zones should have a SOA (Statement Of Authority) record that contains an email address where a PoC for the domain could be contacted. This can sometimes be used for attribution/linkage between different domains even if protected by whois privacy
- **size-in-bytes**: Size expressed in bytes
- **counter**: An integer counter, generally to be used in objects

- **datetime**: Datetime in the ISO 8601 format
- **port**: Port number
- **ip-dst|port**: IP destination and port number separated by a |
- **ip-src|port**: IP source and port number separated by a |
- **hostname|port**: Hostname and port number separated by a |
- **mac-address**: Mac address
- **mac-eui-64**: Mac EUI-64 address
- **email-dst-display-name**: Email destination display name
- **email-src-display-name**: Email source display name
- **email-header**: Email header
- **email-reply-to**: Email reply to header
- **email-x-mailer**: Email x-mailer header
- **email-mime-boundary**: The email mime boundary separating parts in a multipart email
- **email-thread-index**: The email thread index header
- **email-message-id**: The email message ID
- **github-username**: A github user name
- **github-repository**: A github repository
- **github-organisation**: A github organisation
- **jabber-id**: Jabber ID
- **twitter-id**: Twitter ID
- **dkim**: DKIM public key
- **dkim-signature**: DKIM signature
- **first-name**: First name of a natural person
- **middle-name**: Middle name of a natural person
- **last-name**: Last name of a natural person
- **date-of-birth**: Date of birth of a natural person (in YYYY-MM-DD format)
- **place-of-birth**: Place of birth of a natural person
- **gender**: The gender of a natural person (Male, Female, Other, Prefer not to say)
- **passport-number**: The passport number of a natural person
- **passport-country**: The country in which the passport was issued
- **passport-expiration**: The expiration date of a passport
- **redress-number**: The Redress Control Number is the record identifier for people who apply for redress through the DHS Travel Redress Inquiry Program (DHS TRIP). DHS TRIP is for travelers who have been repeatedly identified for additional screening and who want to file an inquiry to have erroneous information corrected in DHS systems
- **nationality**: The nationality of a natural person
- **visa-number**: Visa number
- **issue-date-of-the-visa**: The date on which the visa was issued
- **primary-residence**: The primary residence of a natural person
- **country-of-residence**: The country of residence of a natural person
- **special-service-request**: A Special Service Request is a function to an airline to provide a particular facility for A Passenger or passengers.
- **frequent-flyer-number**: The frequent flyer number of a passenger
- **travel-details**: Travel details
- **payment-details**: Payment details

- **place-port-of-original-embarkation**: The original port of embarkation
- **place-port-of-clearance**: The port of clearance
- **place-port-of-onward-foreign-destination**: A Port where the passenger is transiting to
- **passenger-name-record-locator-number**: The Passenger Name Record Locator is a key under which the reservation for a trip is stored in the system. The PNR contains, among other data, the name, flight segments and address of the passenger. It is defined by a combination of five or six letters and numbers.
- **mobile-application-id**: The application id of a mobile application
- **chrome-extension-id**: Chrome extension id
- **cortex**: Cortex analysis result
- **boolean**: Boolean value - to be used in objects
- **anonymised**: Anonymised value - described with the anonymisation object via a relationship.

Last modified: Wed Mar 24 2021 22:22:36 GMT+0100 (Central European Standard Time)

- [Sharing / Synchronisation](#)
- [Synchronisation](#)
 - [Concept](#)
 - [Pull vs Push synchronisation](#)
 - [Push](#)
 - [Pull](#)
 - [Benefits of using push and pull in conjunction](#)
 - [Adding a server](#)
 - [Test connection](#)
 - [Rules](#)
 - [Troubleshooting](#)
 - [Sharing and distribution](#)
 - [Distribution settings](#)
 - [Visibility of data - events objects and attributes](#)
 - [Community](#)
 - [Sharing-groups](#)
 - [Distribution mechanisms](#)
 - [General syncing rules](#)
 - [Syncing scenarios with communities distribution](#)
 - [Internal instance flag not set](#)
 - [Push from instance A to instance B - usual scenario](#)

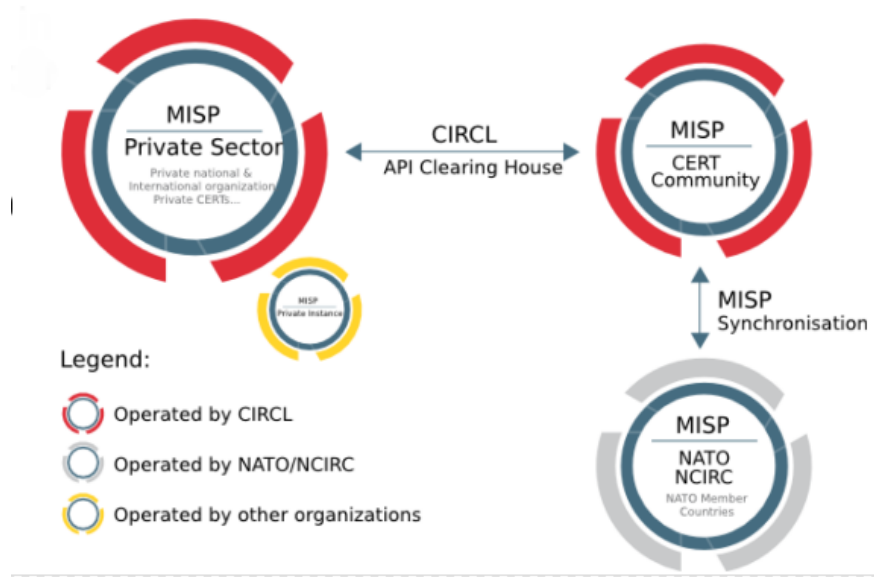
Sharing / Synchronisation

- MISP's core functionality is sharing where everyone can be a consumer and/or a contributor/producer.
- Quick benefit without the obligation to contribute
- Low barrier access to get acquainted to the system

Synchronisation

Concept

The following figure shows the concept how different MISP instances could tie together.



In MISP, two ways exist to get events from remote sources:

- **Use case 1:** From another MISP server (also called [MISP instance](#)), by synchronising two MISP servers.
- **Use case 2:** From a link, by using [Feeds](#).

The example below illustrates the [synchronisation](#) between two MISP servers (use case 1). An organisation B (OrgB) wants to synchronise its MISP server, called ServerB, with the MISP server of an organisation A (Org A), called ServerA. The following steps can be taken to synchronise ServerB with ServerA:

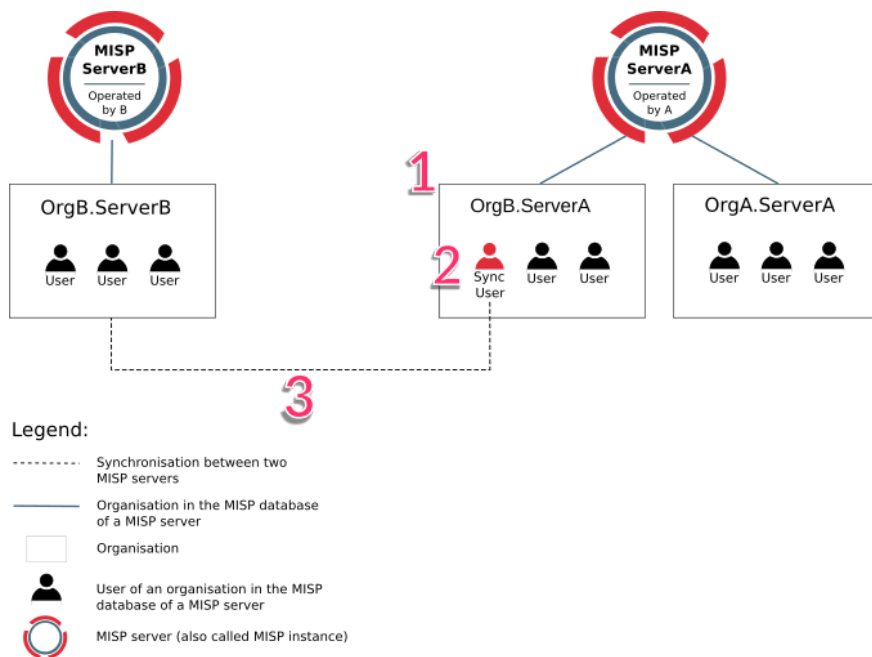


FIGURE: Illustration of the [synchronisation](#) between two MISP servers

- **Step 1:** Add OrgB as a local organisation on ServerA (OrgB.ServerA) using OrgB's existing UUID from their local organisation on ServerB.
- **Step 2:** Add a [Sync User](#) (syncuser@OrgB.ServerA) in the organisation OrgB.ServerA on the MISP ServerA.
- **Step 3:** [Set up a sync server](#) on MISP ServerB using the key (called Authkey) from the [sync user](#) (syncuser@OrgB.ServerA) created on MISP ServerA.

For additional information on the [synchronisation](#) process, refer to the [MISP GitHub issues](#), for example, [issue 2595](#).

Pull vs Push synchronisation

[Synchronisation](#) can be set up using the [pull](#) or [push](#) option. A combination of the two is possible as well. This section discusses the main practical differences between the two and the benefit of using both in conjunction.

To automatically execute [pull](#) and [push](#) synchronisations on a schedule, please use a scheduling service such as cron to execute the relevant command line functions mentioned in the related [administration](#) section.

For a table overview of which [community](#) distributions lead to a sync on [push](#) or [pull](#) scenarios as well as how the distribution level automatically decreases on sync, please refer to the [syncing scenarios with communities distribution](#) section.

Push

The [push](#) mechanism provides a seemingly real time experience. If a [push](#) connection is enabled, data created (and synchronized from other peers) will be synchronized as fast as possible. In practice, this means that an attempt to synchronise is made immediately after publication of an event.

A disadvantage of the [push](#) mechanism is that connection issues or dead workers might prevent the [push](#) from being successful.

Data with distribution set to 'Your organisation only' or 'This [community](#) only' will not be synchronised using the [push](#) mechanism (unless the internal instance flag is set for the server to be synced to).

Pull

In contrast to a [push](#), [pull synchronisation](#) is only performed on command. This could be a manual trigger by an admin from the servers page or a cron job executing a [pull](#) command. See [administration](#) for the available command line interface commands.

A [pull](#) will also fetch objects with a distribution set to 'this [community](#) only' and even your 'organisation only', if the auth key belongs to the organisation owning the related event.

Benefits of using push and pull in conjunction

- If an unexpected issue prevented the [push](#) from happening, the data can be pulled in later
- Different rules can be set for the [push](#) and [pull](#) sync

Adding a server

Servers can be added by users via

```
https://<misp url>/servers/add
```

The screenshot shows the MISP web interface. At the top is a navigation bar with links: Home, Event Actions, Galaxies, Input Filters, Global Actions, and Sync Actions. On the left is a sidebar with 'List Servers' and 'New Server' (highlighted with a red arrow). The main content area is titled 'Add Server' and contains two input fields: 'Base URL' and 'Instance name'. A red arrow points from the 'List Servers' button in the top right dropdown menu to the 'Add Server' title.

The Add Server Form has several input fields:

Add Server

Instance identification

Base URL

Instance name

1

2

You can set this instance up as an internal instance by checking the checkbox below. This means that any synchronisation between this instance and the remote will not be automatically degraded as it would in a normal synchronisation scenario. Please make sure that you own both instances and that you are OK with this otherwise dangerous change. This also requires that the current instance's host organisation and the remote sync organisation are the same.

☐ Internal instance 3

Instance ownership and credentials

Information about the organisation that will receive the events, typically the remote instance's host organisation.

Organisation Type

Local Organisation

Local organisation 4

CSI 5

Ask the owner of the remote instance for a sync account on their instance, log into their MISP using the sync user's credentials and retrieve your API key by navigating to Global actions -> My profile. This key is used to authenticate with the remote instance.

Authkey

Leave empty to use current key 6

Enabled synchronisation methods

☐ Push 7 ☐ Pull 8 ☐ Push Sightings 9 ☐ Caching Enabled 10 ☐ Push Galaxy Clusters 11 ☐ Pull Galaxy Clusters 12

Misc settings

☐ Unpublish Event 13
☐ Publish Without Email 14
☐ Self Signed 15
☐ Skip proxy (if applicable) 16

Server certificate file (*.pem): Not set.

[Add certificate file](#) [Remove certificate file](#) 17

Client certificate file: Not set.

[Add certificate file](#) [Remove certificate file](#) 18

Push rules:

[Modify](#) 19

Pull rules:

[Modify](#) 20

[Submit](#)

1. **Base URL** The base-url to the external server you want to sync with.
Example: <https://foo.sig.mil.be>
2. **Instance Name** A name that will make it clear to your users what this instance is. For example: Organisation A's instance
3. **Internal instance** This checkbox will only show up if the set 'local organisation', see 5, is the same as the owning organisation of the instance the remote server is being configured on. If this flag is set, the distribution of pushed data will not be automatically downgraded. Please refer to the [syncing scenarios with communities distribution](#) section for a table overview of the differences.
4. **Remote Sync Organisation Type** MISP has several organisation "pools", one for local and one for known external organisations. When adding a [synchronisation](#) connection, you need to define the host organisation of the remote instance. Select which pool you wish to pick the organisation from using this drop-down. You also have the option of adding a new external organisation directly from this interface.
5. **Local/Known remote Organisation** Choose the organisation from the selected pool that defines the host organisation on the remote side. Make sure that the remote instance is actually run by the organisation you select as this is used in an integral part of the sharing mechanism. Do not select your own organisation for this setting.
6. **Authkey** You can find the authentication key on your profile on the external server. If advanced auth keys is enabled you might have to create an auth key manually. This can be done on your profile view as well.
7. **Push** Allow the upload of events and their attributes. Only Events that match the given [push](#) rules (see 19) will be pushed to the server. Sightings and relevant galaxy clusters will not be pushed unless 'Push Sightings' and 'Push Galaxy Clusters' are enabled as well.
8. **Pull** Allow the download of events and their attributes from the server. Only data matching the given [pull](#) rules (see 20) will be pulled. Relevant galaxy clusters will not be pulled in unless the 'Pull Galaxy Clusters' checkbox is ticked as well.
9. **Push sightings** If checked, sightings will be pushed out as well on [push](#).
10. **Caching Enabled** Allow caching of the remote server. Once cached, caching related functionalities such as server overlap analysis can be done.
11. **Push Galaxy Clusters** If checked, relevant galaxy clusters will be pushed out as well on [push](#).
12. **Pull Galaxy Clusters** If checked, relevant galaxy clusters will be pulled in as well on [push](#). This also enables you to do a [pull](#) for galaxy clusters only if [pull](#), see 8, is checked as well.
13. **Unpublish Event** Unpublish the synced event. This only works on [push](#).
14. **Publish Without Email** Publish the event without sending out an email.

15. **Self Signed** Check this if you would like to allow a connection despite the other instance using a self-signed certificate (not recommended).
16. **Skip proxy (if applicable)** Do not connect to this server using the configured proxy (if any proxy host is set in the MISP configuration).
17. **Server certificate file** You can upload a certificate file if the instance you are trying to connect to has its own signing authority. (*.pem)
18. **Client certificate file** Set a client certificate to use when connecting to this server.
19. **Push rules** Allows you to set filtering rules for data to be pushed out (tag based and organisation based). Please see [rules](#) for more info.
20. **Pull rules** Allows you to set filtering rules for data to be pulled in (tag based and organisation based). Please see [rules](#) for more info.

Test connection

The connection test can be used to test the connection to the remote server and will give a feedback about local and remote version of MISP.

Servers

« previous next »

ID	Name	Prio	Connection test
2	JEROEN_PUBLIC	⬆️⬆️	Run

ID	Name	Prio	Connection test
2	JEROEN_PUBLIC	⬆️⬆️	Local version: 2.4.140 Remote version: 2.4.140 Status: OK Compatibility: Compatible POST test: Received sent package

Rules

Rules are used to limit sharing when synchronising events and attributes. In the example below, data tagged with tlp:red or owned by organisation Setec Astronomy will not be pushed out to this server. Please note any other filtering set up on the instance will still apply as well (blocklists for example).

The screenshot displays the 'Set push rules' configuration window. It is divided into two main sections: 'Tags' and 'Organisations', each with 'Allowed' and 'Blocked' lists. The 'Tags' section shows 'Allowed Tags (OR)' as an empty list, 'Available Tags' including 'event-block-rule-test', 'tlp:amber', 'tlp:ex:chr', 'tlp:green', and 'tlp:white', and 'Blocked Tags (AND NOT)' containing 'tlp:red'. The 'Organisations' section shows 'Allowed Orgs (OR)' as an empty list, 'Available Organisations' including 'CSI', 'JEROEN_LOCAL', 'RECEIVINGORG-LOCA', 'RECEIVINGORG-LOCA', and 'JEROEN_4EYES', and 'Blocked Orgs (AND NOT)' containing 'Setec Astronomy'. The interface includes 'Update' and 'Cancel' buttons at the bottom.

Section	Category	Item
Tags	Allowed Tags (OR)	
	Available Tags	event-block-rule-test, tlp:amber, tlp:ex:chr, tlp:green, tlp:white
	Blocked Tags (AND NOT)	tlp:red
Organisations	Allowed Orgs (OR)	
	Available Organisations	CSI, JEROEN_LOCAL, RECEIVINGORG-LOCA, RECEIVINGORG-LOCA, JEROEN_4EYES
	Blocked Orgs (AND NOT)	Setec Astronomy

Troubleshooting

If you have issues connecting to a remote servers try to do the following things:

- manually try to do an [API](#) request, to ensure that your [API](#) key is valid
- try to connect with your user account to the remote server and check your [roles](#) on the remote server
- perform a package capture and analyse the traffic
- if you have a SSL connection issue to a remote server with a certificate signed by a CA that is not included in OS, make sure the whole certificate path is included in the path.

Sharing and distribution

The following section describes how distribution mechanisms of events and attributes work.

Distribution settings

The below five distribution settings are available for events and attributes. Descriptions of those settings can be found [here](#).

- Your organisation only
- This [community](#) only
- Connected communities
- All communities
- Sharing group

Events that are not published are only distributed/shared to the local organisations on the same MISP server/instance (within the limit of the distribution model). Only events that are **published** will be shared with remote organisations on other MISP servers via [push/pull](#) mechanisms. More details on [publishing](#) events [here](#).

Visibility of data - events objects and attributes

Assuming that none of the ancestors of the object of attribute are too restrictive, you can view an event/object/attribute on an instance if:

- You are a [site admin](#)
- Your organisation is owner of the event
- Neither of the above apply and one of the below statements is true:
 - The distribution of the event/object/attribute is 'This [community](#) only', 'Connected communities' or 'All communities'
 - Your organisation belongs to the sharing group of the event/object/attribute or the sharing group has the 'all orgs' flag set for the instance

Note:

- As of MISP version 2.4.140: When pulling in data you can only see due to the 'all orgs' flag being set in the sharing group, your organisation will be added to the sharing group when creating the data locally.

Community

A [community](#) is composed of the local organisations on a MISP server and the remote organisations connected by the sync users. For more information on the concept of [community](#), refer to an [article on MISP information sharing following ISO/IEC 27010](#), explaining the concept of [community](#).

Specifically, communities are not reversible. Taking the example of [the above figure](#), illustrating the [synchronisation](#) between two MISP servers, OrgB.ServerB is part of the MISP ServerA [community](#) but OrgB.ServerA is not part of MISP ServerB [community](#).

Sharing-groups

There is an article about [sharing groups](#) in [here](#)

Distribution mechanisms

The distribution level of an event is automatically decreased as it is synchronised with other MISP instances, when it was originally set to:

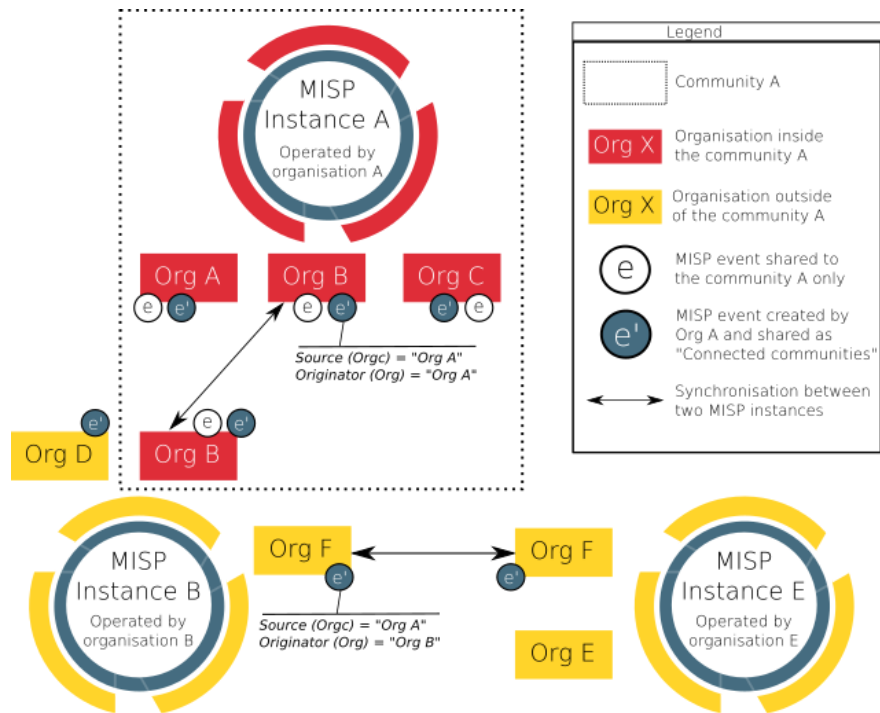
- [Community](#) only (to organisation only)
- Connected [community](#) (to [community](#) only)

It is not decreased when it was originally set to:

- Organisation only
- All communities
- Sharing group

[!] This rule does not apply if "Internal instance" has been checked when creating the server.

As an example, the figure below illustrates two events **e** and **e'** created by OrgA and respectively shared as "This [community](#) only" and "Connected communities" and how they propagate in an illustrative MISP set of instances synchronised with each others.



General syncing rules

- The owner organisation of the event on instance B is set to the organisation of the [sync user](#).
- The creator user is the authkey user when pushing
- The creator user is the user triggering the [pull](#) when pulling. This user can be different than the authkey user.
- Rule of thumb: if the user configured to [pull](#) from instance A to B can see the event on instance A, the event will be synced.

Syncing scenarios with communities distribution

Internal instance flag not set

The below scenarios are if "Internal instance" has not been checked when creating the server. This is the usual scenario.

Push from instance A to instance B - usual scenario

Which organisation the remote [sync user](#) belongs to has no impact on which events are pushed.

Instance A	Instance B
Your organisation only	Event/object/attribute not pushed
This community only	Event/object/attribute not pushed
Connected communities	Event/object/attribute distribution decreased to 'This community only' on B
All communities	Event/object/attribute distribution stays 'all communities'

Pulling from instance A to instance B - usual scenario

Rule of thumb: if the user configured to [pull](#) from instance A can see the event on instance A, the event will be synced.

Instance A	Instance B
Your organisation only	Event/object/attribute pulled in only if the sync user is member of the event's owner organisation on A. Event distribution stays 'Your organisation only' on instance B
This community only	Event/object/attribute distribution decreased to 'Your organisation only' on B
Connected communities	Event/object/attribute distribution decreased to 'This community only' on B
All communities	Event/object/attribute distribution stays all communities on B

Internal instance flag set

The below scenarios are if "Internal instance" has been checked when creating the server. This is the *not* the usual scenario and *potentially dangerous*. The internal instance flag can be used when both instances have the same hosting organisation.

Push from instance A to instance B - internal flag set scenario

Instance A	Instance B
Your organisation only	Event/object/attribute not pushed if triggering push of already locally (on instance A) published event. Event/object/attribute synced on publication of an event, even if the organisation publishing is not the host organisation of the instance
This community only	Event/object/attribute distribution stays 'This community only' on B
Connected communities	Event/object/attribute distribution stays 'Connected communities' on B
All communities	Event/object/attribute distribution stays 'All communities on B'

Pulling from instance A to instance B - internal flag set scenario

Rule of thumb: if the user configured to [pull](#) from instance A can see the event on instance A, the event will be synced.

Instance A	Instance B
Your organisation only	Event/object/attribute pulled in only if the sync user is member of the event's owner organisation. Event distribution stays 'Your organisation only' on B
This community only	Event/object/attribute distribution decreased to 'Your organisation only' on B
Connected communities	Event/object/attribute distribution decreased to 'This community only' on B
All communities	Event/object/attribute distribution stays 'All communities' on B

Collaboration

Proposals

[Proposals](#) can be used to propose new attribute values that can be reviewed by the event owner.

Forums / Threats

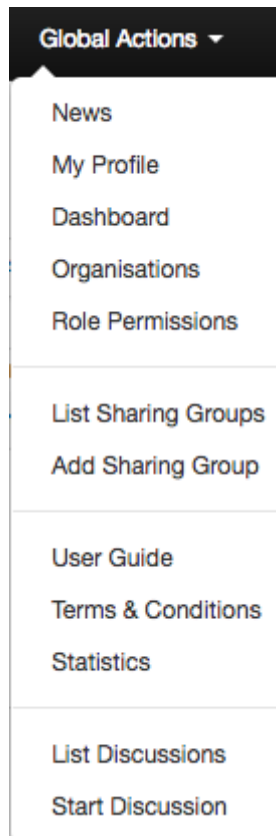
Forums can be used to discuss non event related topics.

Discussions can be accessed on the top "Global Actions - List Discussions"

Discussions will and can not be shared with other servers

and via URL:

```
https://<misp url>/threads/index
```



Create a new Topic

To create a new topic

`https://<misp url>/posts/add`

[List Threads](#)
[New Thread](#)

Add Post

Thread Subject

[Quote](#) [Event](#) [Thread](#) [Link](#) [Code](#)

I would like to talk about foo bar because...

Submit

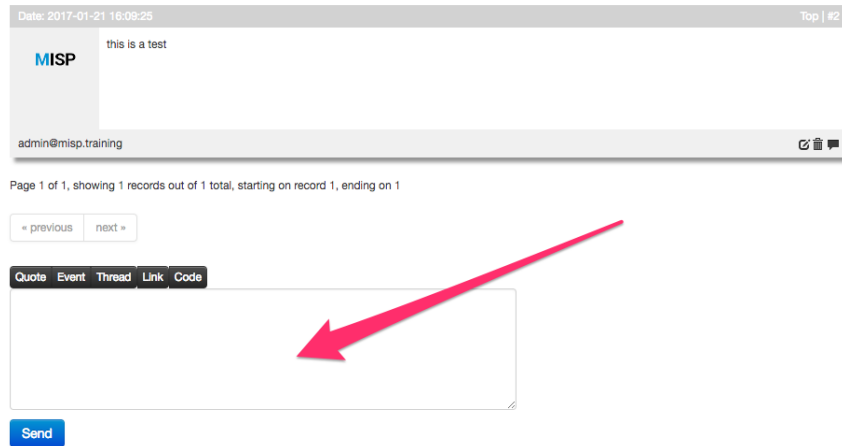
Comment a topic

A topic can be commented by any user

```
https://<misp url>/threads/view/<topic id>
```

Comments to events

In MISP ongoing events can be commented by every user to ask free text question to events. **Comments to events will not be shared with other servers**



The screenshot displays the MISP web interface for commenting on an event. At the top, a header bar shows the date '2017-01-21 16:09:25' and a 'Top | #2' link. Below this, the MISP logo is visible next to the text 'this is a test'. The user 'admin@misp.training' is logged in, as indicated by the text at the bottom of the header. A pagination bar shows 'Page 1 of 1, showing 1 records out of 1 total, starting on record 1, ending on 1'. Below the pagination bar are two buttons: '« previous' and 'next »'. A row of tabs includes 'Quote', 'Event', 'Thread', 'Link', and 'Code'. The 'Event' tab is selected. Below the tabs is a large text input area for the comment. A red arrow points to this input area. At the bottom left of the input area is a blue 'Send' button.

Contact a reporter

This feature can be used to contact the person or the organisation that the person belongs to that has created the event.

All E-Mails can be enforced to be encrypted

Contact organization reporting event 4

You are about to contact the organization that reported event 4.

Feel free to add a custom message that will be sent to the reporting organization.

Your email address and details about the event will be added automatically to the message.

Message

Hello,

we have seen several of the indicators mentioned in this event in our network, do you have any more information on it?

☒ Submit only to the person that
created the event

Submit

Receive alerts

It is possible to get alerts via encrypted mail in the following cases:

- published events by other user of the [MISP instance](#)
- events pushed to the [MISP instance](#)
- events pulled by the [MISP instance](#)

These E-Mail alerts are an opt-in feature

Edit My Profile

Email	Password	Confirm Password
<input type="text" value="admin@misp.training"/>	<input type="password"/>	<input type="password"/>
Organisation	Role	Nids Sid
<input type="text"/>	<input type="text" value="admin"/>	<input type="text" value="4000000"/>


GPG key

[Fetch GPG key](#)

☐ Receive alerts when events are published

☐ Receive alerts from "contact reporter" requests

[Submit](#)



Recommendation

The following section will describe what is the best practice how many MISP instances that showed to be good for orgs. Of course depending on your specific requirements an architecture could be more spread or simplified.

The architecture is divided into several systems / stages beginning with:

MISP Staging System

This systems purpose is to be linked to all available external MISP systems that you have access to. It will download all events and do enrichment between these events.

MISP SECOps System

This system is the main system used by human analysts. It will it is not linked to any external [MISP instance](#) other then the Staging System.

To publish events to the [community](#) assign the right tags to match your [push Rules](#) and **publish the event**

Last modified: Sun Feb 28 2021 09:22:59 GMT+0100 (Central European Standard Time)

External Connectors

The **MISP to Microsoft Graph Security Script** enables you to connect your custom threat [indicators](#) or [Indicators of Compromise \(IoCs\)](#) and make these available in the following Microsoft products.

Azure Sentinel

[Azure Sentinel](#)

Microsoft Defender ATP

[Microsoft Defender ATP](#)

MISP to Microsoft Graph Security Script

The script provides clients with MISP instances to migrate threat [indicators](#) to the [Microsoft Graph Security API](#).

For more information on Microsoft Graph Security [API](#) visit [Microsoft Graph Security API](#).

For more information on Microsoft Graph visit [Microsoft Graph](#).

Prerequisites

Before installing the sample:

- Install Python 3.x version from <https://www.python.org/>.
- To register your application for access to Microsoft Graph, you'll need either a [Microsoft account](#) or an [Office 365 for business account](#). If you don't have one of these, you can create a Microsoft account for free at outlook.com.

Getting Started

After the prerequisites are installed or met, perform the following steps to use these scripts:

1. Download or clone this repository.
2. Go to directory `security-api-solutions/Samples/MISP`
3. Install dependencies. In the command line, run `pip3 install requests requests-futures pymisp`

4. To run script, go to the root directory of misp-graph-script and enter

```
PYTHONHASHSEED=0 python3 script.py
```

 in the command line.

App Registration

To configure the sample, you'll need to register a new application in the Microsoft [Application Registration Portal](#). Follow these steps to register a new application:

1. Sign in to the [Application Registration Portal](#) using either your personal or work or school account.
2. Choose **New registration**.
3. Enter an application name, and choose **Register**.
4. Next you'll see the overview page for your app. Copy and save the **Application Id** field. You will need it later to complete the configuration process.
5. Under **Certificates & secrets**, choose **New client secret** and add a quick description. A new secret will be displayed in the **Value** column. Copy this password. You will need it later to complete the configuration process and it will not be shown again.
6. Under **API permissions**, choose **Add a permission > Microsoft Graph**.
7. Under **Application Permissions**, add the permissions/scopes required for the sample. This sample requires **ThreatIndicators.ReadWrite.OwnedBy**.

Note: See the [Microsoft Graph permissions reference](#) for more information about Graph's permission model.

8. Modify the RequestManager.py file to comment out line 121-124. (This allows the script to run without failing due to line 123 being divided by `avg_speed` incase it starts as `0` .
9. Modify the script.py to add in `config.misp_verifycert` at line 13. Ensure it looks like below.

```
misp = PyMISP(config.misp_domain, config.misp_key, config.misp_verifycert)
```

10. Modify config.py file to add in `misp_verifycert = False` anywhere in the file.

As the final step in configuring the script, modify the config.py file in the root folder of your cloned repo.

Update tenant, client_id, and client_secret in config.py

```
graph_auth = {
    'tenant': '<tenant id>',
    'client_id': '<client id>',
    'client_secret': '<client secret>',
}
```


Once changes are complete, save the config file.

Configurations

Target Product

```
targetProduct = "Azure Sentinel" or targetProduct = "Microsoft Defender ATP"
```

Misp Event Filter

Filters can be set in the config.py file under the "misp_event_filters" property

Below is a list of parameters that can be passed to the filter (source:

<https://pymisp.readthedocs.io/modules.html>):

- values – values to search for
- not_values – values not to search for
- type_attribute – Type of attribute
- category – Category to search
- org – Org reporting the event
- tags – Tags to search for
- not_tags – Tags not to search for
- date_from – First date (Format: '2019-01-01')
- date_to – Last date (Format: '2019-01-01')
- last – Last published events (for example 5d or 12h or 30m)
- eventid – Event ID
- withAttachments – return events with or without the attachments
- uuid – search by uuid
- publish_timestamp – the publish timestamp (Note: Uses UNIX timestamp. Format: '1551811160')
- published – return only published events (Format: True or False)

A list or a specific value can be passed to the above parameters. If a list is passed to the parameter, the filtered events are the result of the union of provided list.

This field needs to be a list that contains multiple filters. The filtered events are the result of the intersection of provided filters.

First Example of How This Field can be Configured

```
misp_event_filters = [
    {
        "type_attribute": 'mutex'
    },
    {
        "type_attribute": 'filename|md5'
    },
]
```

An event meets this filtering criteria if the event has an attribute with attribute type of 'mutex' AND the event has an attribute with attribute type of 'filename|md5'.

Second Example of How This Field can be Configured

```
misp_event_filters = [
  {
    "type_attribute": ['mutex', 'filename|md5']
  }
]
```

An event meets this filtering criteria if the event has an attribute with attribute type of 'mutex' OR the event has an attribute with attribute type of 'filename|md5'.

Third Example of How This Field can be Configured

```
misp_event_filters = [
  {
    "values": 'http://www.test.com'
  }
]
```

An event meets this filtering criteria if the event has an attribute with attribute value of '<http://www.test.com>'.

Fourth Example of How This Field can be Configured

```
misp_event_filters = []
```

This gets all events.

Action

Possible **action** values are: `alert` , `allow` , `block` .

```
action = "alert" (This is default).
```

Passive Only

```
passiveOnly = False (This is default).
```

Days to Expire

This property is used to specify the amount of days the records will expire in Microsoft Graph Security [API](#). The default value for days to expire is 30.

```
days_to_expire = 5
```

Misp Key

The Misp Auth Key is required to fetch data from your [Misp instance](#). Configure a [sync user](#).

```
misp_key = '<misp key>'
```

Verify Cert

This gives you the option to choose if python should validate the certificate of the [misp instance](#). (This allows ease within testing environments)

```
misp_verifycert = False
```

IT IS RECOMENDED TO USE A VALID SSL CERT IN PRODUCTION AND CHANGE THIS TO TRUE

Instructions on Reading TilIndicators That Have Been Pushed

In the command line, run `python3 script.py -r`

Instructions on Seeing All Requests That Resulted in Errors

1. In the command line, run `cd logs` to go to the logs folder.
2.
 - o To print all the requests that resulted in errors to the console, simply run `cat *_error_*` in the command line.
 - o To aggregate all the requests that resulted in errors to a file, run `cat *_error_* > <filename>.txt` in the command line.

Script Output

As the script runs, it prints out the request body sent to the Microsoft Graph Security [API](#) and the response from the Microsoft Graph Security [API](#).

Every request is logged as a json file under the directory "logs". The name of the json file is the datetime of when the request is completed.

Schedule with CRONTAB

Below is a CRONTAB entry example of running the script every Sunday at 2am

```
0 2 Sun /home/mark/misp-graph-script/python3 script.sh
```

This README.md has been adapted from the README.md found in the [Microsoft Graph Security API MISP sample](#). For most recent changes, visit [Microsoft Graph Security API MISP sample](#). Provide your feedback on this sample by [filing a GitHub request](#).

Last modified: Sun Feb 28 2021 09:22:59 GMT+0100 (Central European Standard Time)

MISP modules

[MISP modules](#) are autonomous modules that can be used for expansion and other services in MISP. The modules are written in Python 3 following a simple [API](#) interface. The objective is to ease the extensions of MISP functionalities without modifying core components. The [API](#) is available via a simple REST [API](#) which is independent from MISP installation or configuration.

[MISP modules](#) support is included in MISP starting from version 2.4.28.

[More](#)

[MISP modules GitHub Repo](#)

Installation

[Install guide on Ubuntu](#)

[Install guide RHEL/CentOS](#)

Last modified: Sun Feb 28 2021 09:22:59 GMT+0100 (Central European Standard Time)

- [MISP ZeroMQ](#)
 - [MISP ZeroMQ configuration](#)
 - [MISP ZeroMQ debugging and testing](#)
 - [Testing with sub.py tool](#)
 - [Notification Schemas](#)
 - [misp_json](#) - events published
 - [misp_json_attribute](#) - attribute updated or created
 - [misp_json_sighting](#) - sighting added to an attribute or an event
 - [misp_json_user](#) - user updates or creation
 - [misp_json_organisation](#) - organisation updates or creation
 - [misp_json_self](#) - keep-alive messages sent every minute
 - [Tips for Building a Subscriber](#)

MISP ZeroMQ

MISP includes a flexible publish-subscribe model to allow real-time integration of MISP activities (event publication, attribute creation or removal, sighting). The MISP ZeroMQ plugin operates at global level in MISP which means standard distribution rules don't apply and every activity will be published within the ZeroMQ pub-sub channels.

MISP ZeroMQ functionality can be used for various models of integration or to extend MISP functionalities:

- real-time search of [indicators](#) into a SIEM
- automatic expansion
- dashboard activities
- logging mechanisms
- continuous indexing
- custom software or scripting

The following notification topic channels exist and can be included in the MISP ZeroMQ pub-sub:

- `misp_json` - events published
- `misp_json_attribute` - attribute updated or created
- `misp_json_sighting` - sighting added to an attribute or an event
- `misp_json_user` - user updates or creation
- `misp_json_organisation` - organisation updates or creation
- `misp_json_self` - keep-alive messages sent every minute

MISP ZeroMQ configuration

To enable MISP ZeroMQ, the feature must be enabled in the Plugin setting tab.

Prior to enabling it, make sure that you have pyzmq installed by running

```
sudo pip install pyzmq
sudo pip install redis
```

If you have problems and the plugin does not start, the logfile may be helpful.

```
sudo cat /var/www/MISP/app/tmp/logs/mispzmq.error.log
```

Server Settings & Maintenance

Overview	MISP settings (M)	Import settings (I)	Export settings (E)	Search settings (S)	Plugin settings (P)	Log settings	Manage files	Advanced
Filter the table(s) below								
Import								
Export								
Colors								
Signings								
MSP								
Index								
DevOps								
Optional	Plugin-DevOps_enable	True	Enables or disables the publish feature of DEVOPS. Make sure that you install the requirements for the plugin to work. Refer to the installation instructions for more information.					Value not set.
Optional	Plugin-DevOps_host	127.0.0.1	The host that the publish feature will use.					Value not set.
Optional	Plugin-DevOps_port	8000	The port that the publish feature will use.					Value not set.
Optional	Plugin-DevOps_username		The username that client needs to use to connect to DevOps.					Value not set.
Optional	Plugin-DevOps_password		The password that client needs to use to connect to DevOps.					Value not set.
Optional	Plugin-DevOps_redis_host	localhost	Location of the Redis db used by DEVOPS and the Python-PUB scripts to push data to be published.					Value not set.
Optional	Plugin-DevOps_redis_port	6379	The port that Redis is listening on.					Value not set.
Optional	Plugin-DevOps_redis_password		The password, if any, for Redis.					Value not set.
Optional	Plugin-DevOps_redis_database	1	The database to be used for pushing messages for the publish functionality.					Value not set.
Optional	Plugin-DevOps_redis_channels	misp:	The channels to be used for pushing messages for the publish functionality.					Value not set.
Optional	Plugin-DevOps_redis_compression	None	Enables this setting to include the base64 encoded payloads of malware samples/statements in the output.					Value not set.
Optional	Plugin-DevOps_redis_notifications_enable	None	Enables or disables the publishing of any event notifications/statements.					Value not set.
Optional	Plugin-DevOps_redis_notifications_enable	None	Enables or disables the publishing of any object notifications/statements.					Value not set.
Optional	Plugin-DevOps_redis_notifications_enable	None	Enables or disables the publishing of any attribute notifications/statements.					Value not set.
Optional	Plugin-DevOps_redis_notifications_enable	None	Enables or disables the publishing of any tag notifications/statements as well as tags being attached to / detached from various MISP elements.					Value not set.
Optional	Plugin-DevOps_redis_notifications_enable	None	Enables or disables the publishing of new signposts to the DMZ publish feed.					Value not set.
Optional	Plugin-DevOps_redis_notifications_enable	None	Enables or disables the publishing of new modified users to the DMZ publish feed.					Value not set.
Optional	Plugin-DevOps_redis_notifications_enable	None	Enables or disables the publishing of new modified organizations to the DMZ publish feed.					Value not set.
Optional	Plugin-DevOps_redis_notifications_enable	None	Enables or disables the publishing of log entries to the DMZ publish feed. Keep in mind, this can get pretty verbose depending on your logging settings.					Value not set.

Each notification channel can be enabled (from event publication to sightings), the MISP [site admin](#) can decide which types of messages to publish.

By default, the ZMQ pub-sub channel is available to localhost only on TCP port 50000. The binding of the pub-sub channel can be updated in the configuration interface as shown above

MISP ZeroMQ debugging and testing

In the diagnostic section, ZeroMQ service can be started and stopped. There is a status check that can be run to give information about the number of events processed by the service.

ZeroMQ

This tool tests whether the ZeroMQ extension is installed and functional.

ZeroMQ settings....OK

Start / Restart

Stop

Status

Testing with sub.py tool

A simple command line tool is included with MISP to connect to the MISP ZeroMQ channel and get the notifications:

```
python3 sub.py --help
usage: sub.py [-h] [-s] [-p PORT] [-r HOST] [-o ONLY] [-t SLEEP]

Generic ZMQ client to gather events, attributes and sighting updates from a
MISP instance

optional arguments:
  -h, --help            show this help message and exit
  -s, --stats           print regular statistics on stderr
  -p PORT, --port PORT  set TCP port of the MISP ZMQ (default: 50000)
  -r HOST, --host HOST  set host of the MISP ZMQ (default: 127.0.0.1)
  -o ONLY, --only ONLY  set filter (misp_json, misp_json_attribute or
                        misp_json_sighting) to limit the output a specific
                        type (default: no filter)
  -t SLEEP, --sleep SLEEP
                        sleep time (default: 2)
```

The `sub.py` will output the JSON objects for the subscribed topic, by default, all the topic channels are dumped:


```

misp@cpeb:/var/www/MISP/tools/misp-zmq$ python3 -u sub.py | jq .
....
{
  "uptime": 50,
  "status": "And when you're dead I will be still alive."
}
{
  "uptime": 60,
  "status": "And believe me I am still alive."
}
{
  "uptime": 70,
  "status": "I'm doing science and I'm still alive."
}
{
  "uptime": 80,
  "status": "I feel FANTASTIC and I'm still alive."
}
{
  "uptime": 90,
  "status": "While you're dying I'll be still alive."
}
{
  "Sighting": {
    "uuid": "592d9588-fda0-490f-bf6e-4e56950d210f",
    "source": "",
    "type": "0",
    "date_sighting": 1496159624,
    "org_id": "2",
    "event_id": "8102",
    "attribute_id": "1044812"
  }
}
{
  "Attribute": {
    "id": "1044802",
    "value2": "",
    "value1": "1.2.3.4",
    "uuid": "592d8494-7120-4760-b5e2-4858950d210f",
    "batch_import": "0",
    "comment": "",
    "value": "1.2.3.4",
    "type": "ip-dst",
    "to_ids": 0,
    "timestamp": 1496155284,
    "distribution": "5",
    "sharing_group_id": 0,
    "deleted": "0",
    "disable_correlation": "0",
    "event_id": "8100",
    "category": "Network activity"
  }
}
....

```

Notification Schemas

Each notification channel uses a slightly different JSON schema. Consult this section to identify which MISP components exist in a channel:

misp_json - events published

When an event is published to ZMQ (which is different from being published in MISP) the ZMQ notification will contain the [MISP event](#) data along with all its component children. These components include:

- A list of attributes
- A list of objects, which contain their own lists of attributes
- A list of related events - added when attributes in separate events correlate
- Any galaxies that this event belongs to
- A list of tags that apply to the event

Example:

```

{
  "Event": {
    "id": "625",
    "orgc_id": "2",
    "org_id": "1",
    "date": "2017-05-24",
    "threat_level_id": "3",
    "info": "M2M - Fwd: IMG_3428.pdf",
    "published": false,
    "uuid": "59259036-fcd0-4749-8a6c-4d88950d210f",
    "attribute_count": "7",
    "analysis": "1",
    "timestamp": "1505755565",
    "distribution": "3",
    "proposal_email_lock": false,
    "locked": false,
    "publish_timestamp": "1505416766",
    "sharing_group_id": "0",
    "disable_correlation": false,
    "Org": {"id": "1", "name": "MISP", "uuid": "56ef3277-1ad4-42f6-b90b-046"},
    "Orgc": {"id": "2", "name": "CIRCL", "uuid": "55f6ea5e-2c60-40e5-964f-4"},
    "Attribute": [
      {
        "id": "157835",
        "type": "attachment",
        "category": "Artifacts dropped",
        "to_ids": false,
        "uuid": "59259037-1014-4669-96b1-46af950d210f",
        "event_id": "625",
        "distribution": "5",
        "timestamp": "1495633975",
        "comment": "IMG_3428.pdf",
        "sharing_group_id": "0",
        "deleted": false,
        "disable_correlation": false,
        "object_id": "0",
        "object_relation": null,
        "value": "tmpzuni0skf",
        "ShadowAttribute": []
      }
    ],
    "ShadowAttribute": [],
    "RelatedEvent": [],
    "Galaxy": [],
    "Object": [
      {
        "id": "1",
        "name": "http-request",
        "meta-category": "network",
        "description": "A single HTTP request header",
        "template_uuid": "b4a8d163-8110-4239-bfcf-e08f3a9fdf7b",
        "template_version": "1",
        "event_id": "625",
        "uuid": "59c0016c-0984-4779-9688-05b8c0a83832",
        "timestamp": "1505755500",
        "distribution": "5",
        "sharing_group_id": "0",
        "comment": "",
        "deleted": false,
        "ObjectReference": [],
        "Attribute": [
          {
            "id": "164371",
            "type": "http-method",
            "category": "Network activity",

```

```

        "to_ids": false,
        "uuid": "59c0016c-a744-440d-ad92-05b8c0a83832",
        "event_id": "625",
        "distribution": "5",
        "timestamp": "1505760143",
        "comment": "",
        "sharing_group_id": "0",
        "deleted": false,
        "disable_correlation": false,
        "object_id": "1",
        "object_relation": "method",
        "value": "POST",
        "ShadowAttribute": []
    },
    {
        "id": "164372",
        "type": "uri",
        "category": "Network activity",
        "to_ids": true,
        "uuid": "59c0016c-fac0-4055-9f3d-05b8c0a83832",
        "event_id": "625",
        "distribution": "5",
        "timestamp": "1505755500",
        "comment": "",
        "sharing_group_id": "0",
        "deleted": false,
        "disable_correlation": false,
        "object_id": "1",
        "object_relation": "uri",
        "value": "\\test.php",
        "ShadowAttribute": []
    }
]
}
],
"Tag": [{"id": "2", "name": "tlp:white", "colour": "#ffffff", "exportat
}
}

```

misp_json_attribute - attribute updated or created

The attributes appear to have the most diversity depending on the action applied to them.

When an attribute gets created, the attribute gets sent out via ZMQ. The parent event id is included in the attribute JSON, but there is no extra event metadata like there is when an attribute is deleted or modified.

Create Example:

```
{
  "Attribute": {
    "to_ids": "1",
    "timestamp": 1505235275,
    "distribution": "5",
    "deleted": "0",
    "disable_correlation": "0",
    "event_id": "625",
    "category": "Network activity",
    "type": "domain",
    "value": "microsoft.net",
    "comment": "",
    "batch_import": "0",
    "uuid": "59b8114b-1c80-4149-be3a-03e9c0a83832",
    "sharing_group_id": 0,
    "value1": "microsoft.net",
    "value2": "",
    "id": "164363"
  }
}
```

Edited attribute notifications send metadata about their parent events and information about the attribute's sharing group, attribute-level tags, and sightings data. It's important to note that only the new value of the edited attribute is sent along the ZMQ channel. In order to see the difference between the new and old values, you'd need to have a copy of the old attribute value stored somewhere. If you do, you can use the attribute's `uuid` key (which never changes) to correlate the new and old values.

Edit Example:

```
// microsoft.net --> microsoft.com
{
  "Attribute": {
    "id": "164363",
    "event_id": "625",
    "category": "Network activity",
    "type": "domain",
    "value1": "microsoft.com",
    "value2": "",
    "to_ids": "1",
    "uuid": "59b8114b-1c80-4149-be3a-03e9c0a83832",
    "timestamp": 1505235283,
    "distribution": "5",
    "sharing_group_id": 0,
    "comment": "",
    "deleted": false,
    "disable_correlation": false,
    "value": "microsoft.com",
    "batch_import": "0"
  },
  "Event": {
    "id": "625",
    "org_id": "1",
    "date": "2017-05-24",
    "info": "M2M - Fwd: IMG_3428.pdf",
    "user_id": "1",
    "uuid": "59259036-fcd0-4749-8a6c-4d88950d210f",
    "published": false,
    "analysis": "1",
    "attribute_count": "5",
    "orgc_id": "2",
    "timestamp": "1505235275",
    "distribution": "3",
    "sharing_group_id": "0",
    "proposal_email_lock": false,
    "locked": false,
    "threat_level_id": "3",
    "publish_timestamp": "1505233367",
    "disable_correlation": false
  },
  "SharingGroup": {
    "id": null,
    "name": null,
    "releasability": null,
    "description": null,
    "uuid": null,
    "organisation_uuid": null,
    "org_id": null,
    "sync_user_id": null,
    "active": null,
    "created": null,
    "modified": null,
    "local": null,
    "roaming": null
  },
  "AttributeTag": [],
  "Sighting": []
},
```

When an attribute gets deleted, the `deleted` key gets set to `1`, and the attribute's event metadata gets sent alongside it.

Delete Example:

```
{
  "Attribute": {
    "id": "164362",
    "event_id": "625",
    "category": "Network activity",
    "type": "domain",
    "value1": "microsoft.com",
    "value2": "",
    "to_ids": true,
    "uuid": "59b81121-f4b4-4ed3-aa43-03eac0a83832",
    "timestamp": 1505235262,
    "distribution": "5",
    "sharing_group_id": 0,
    "comment": "",
    "deleted": 1,
    "disable_correlation": false,
    "value": "microsoft.net"
  },
  "Event": {
    "id": "625",
    "org_id": "1",
    "date": "2017-05-24",
    "info": "M2M - Fwd: IMG_3428.pdf",
    "user_id": "1",
    "uuid": "59259036-fcd0-4749-8a6c-4d88950d210f",
    "published": false,
    "analysis": "1",
    "attribute_count": "5",
    "orgc_id": "2",
    "timestamp": "1505235233",
    "distribution": "3",
    "sharing_group_id": "0",
    "proposal_email_lock": false,
    "locked": false,
    "threat_level_id": "3",
    "publish_timestamp": "1505233367",
    "disable_correlation": false
  }
}
```

misp_json_sighting - sighting added to an attribute or an event

The message sent for sightings is fairly simple, with the type of sighting (0 = Addition, 1 = False Positive), the date (in seconds-since-epoch format), the id of the attribute it applies to and the id of the attribute's parent event.

Addition Example:

```
{
  "Sighting": {
    "type": "0",
    "attribute_id": "164373",
    "event_id": "625",
    "org_id": "1",
    "date_sighting": 1505767537,
    "source": "",
    "uuid": "59c03071-f480-4311-a710-03edc0a83832",
    "id": "1"
  }
}
```

False Positive Example:

```
{
  "Sighting": {
    "type": "1",
    "attribute_id": "164373",
    "event_id": "625",
    "org_id": "1",
    "date_sighting": 1505767543,
    "source": "",
    "uuid": "59c03077-d560-4a8b-b841-05b8c0a83832",
    "id": "2"
  }
}
```

misp_json_user - user updates or creation

An update is sent through ZMQ when users log in. There are actually two messages for this - both being fairly sparse. The `current_login` message contains who logged in and at what time (in seconds-since-epoch format) the login happened. The `last_login` message contains who just logged in, what time the previous login occurred (`last_login`) and the time the record was modified, which should be the same as `current_login` time.

Login Example:

```
{
  "User": {
    "id": "1",
    "last_login": "1000046766",
    "date_modified": 1000060160
  }
}
{
  "User": {
    "id": "1",
    "current_login": 1000060160,
    "date_modified": 1000060160
  }
}
```

When a user gets created, all of the information about the user (id, email, base64 encoded GnuPG key, role, etc.) gets sent to ZMQ. If this information is modified, the same JSON will be sent along the ZMQ channel, with updated values. For example, if the below user is disabled, the same JSON will be sent, but the `disabled` key will be set to `"1"`

User Creation and User Edit Example:


```
{
  "User": {
    "server_id": 0,
    "autoalert": "1",
    "invited_by": "1",
    "nids_sid": 5976699,
    "termsaccepted": 0,
    "role_id": "3",
    "change_pw": 1,
    "contactalert": "1",
    "disabled": "0",
    "current_login": "0",
    "last_login": "0",
    "force_logout": "0",
    "email": "user@testemail.com",
    "enable_password": "0",
    "org_id": "1",
    "authkey": "__<redacted>__",
    "gpgkey": "__<redacted>__",
    "notify": "1",
    "date_created": 1000000000,
    "date_modified": 1000000000,
    "newsread": 0,
    "certif_public": "",
    "id": "4"
  }
}
```

misp_json_organisation - organisation updates or creation

Org notifications are sent when Orgs are updated and created, but not when they are deleted. They are generally the same, with the additional fields `created_by` and `date_created` being present when an Org is created.

Creation Example:

```
{
  "Organisation": {
    "created_by": "1",
    "local": "1",
    "name": "test",
    "uuid": "59c0367d-fe8c-42a4-9db2-03ecc0a83832",
    "description": "Test",
    "nationality": "Not specified",
    "sector": "",
    "type": "",
    "contacts": "",
    "logo": {
      "name": "",
      "type": "",
      "tmp_name": "",
      "error": 4,
      "size": 0
    },
    "date_created": "2017-09-18 23:11:28",
    "date_modified": "2017-09-18 23:11:28",
    "id": "10"
  }
}
```

Edit Example:

```
{
  "Organisation": {
    "local": "1",
    "name": "test",
    "uuid": "59c0367d-fe8c-42a4-9db2-03ecc0a83832",
    "description": "Alternate Test",
    "nationality": "Not specified",
    "sector": "",
    "type": "",
    "contacts": "",
    "logo": {
      "name": "",
      "type": "",
      "tmp_name": "",
      "error": 4,
      "size": 0
    },
    "id": "10",
    "date_modified": "2017-09-18 23:11:37"
  }
}
```

misp_json_self - keep-alive messages sent every minute

Only really useful to ensure the ZMQ server is running. And for a bit of humor

```
{
  "status": "I'm doing science and I'm still alive.",
  "uptime": 9170
}
```

Tips for Building a Subscriber

1. `misp_json_attribute` notifications are sent when attributes are created, deleted, and edited
 - Check the `deleted` key to identify if an attribute has been created or deleted
 - If an attribute has been edited, the new value will be sent out via ZMQ, but the `uuid` key will remain the same. Use this to determine if an attribute has existed before or not
2. Some compound attribute types have component types that don't exist outside of them
 - For example, MISP doesn't have a single `ip` attribute type except in the `domain|ip` type
 - If you're going to split up and resubmit these attributes, you may have to modify these component types so MISP will recognize them (e.g. `domain|ip` -> `domain`, `ip-dst`)

Last modified: Thu Mar 04 2021 14:48:45 GMT+0100 (Central European Standard Time)

- [Keyboard shortcuts in MISP](#)

Keyboard shortcuts in MISP

MISP has keyboard shortcuts managed using JSON files. To see the list of shortcuts for a given page, press the small black triangle at the bottom right of the page. **Demo:**

The screenshot displays the MISP interface for viewing an event. The top navigation bar includes links for Home, Event Actions, Galaxies, Input Filters, Global Actions, Sync Actions, Administration, and Audit. The left sidebar contains a 'View Event' section with links like 'View Correlation Graph', 'View Event History', 'Edit Event', 'Delete Event', 'Add Attribute', 'Add Object', 'Add Attachment', 'Populate from...', 'Merge attributes from...', 'Publish Event', 'Publish (no email)', 'Contact Reporter', and 'Download as...'. Below this is a 'List Events' section with a link to 'Add Event'.

The main content area is titled 'Un event' and shows event details:

- Event ID: 1
- Uuid: 5a74bf1a-c898-4d6a-bf61-34fc704ab76f
- Org: CCIRC-EMILIO
- Owner org: CCIRC-EMILIO
- Contributors: test@test.com
- Email: test@test.com
- Tags: untag x 3e tag x
- Date: 2018-02-02
- Threat Level: High
- Analysis: Initial
- Distribution: This community only
- Info: Un event
- Published: No (highlighted in red)
- #Attributes: 0
- Sightings: 0 (0) - restricted to own organisation only.

Below the details is a 'Galaxies' section with an 'Add new cluster' button. At the bottom, there is a table with columns: Date, Org, Category, Type, Value, Tags, Comment, Correlate, and Related Events. A red warning message states: 'Attribute warning: This event doesn't contain any attribute. It's strongly advised to populate the event with attributes (indicators, obser...'. The bottom status bar indicates 'Could not locate the PGP/GPG public key.' and 'Powered by MISP 2.4.87'.

Q: Is it possible to customize the shortcuts in the GUI once they are there?

A: Not at the moment.

Q: How do I add keyboard shortcuts to my [MISP instance](#)? A:

1. Add a JSON file in `app/webroot/shortcuts` named after the page from which it will be included (for example `event_view.json`).
2. Set your shortcuts using this format:

```
1  {
2      "shortcuts": [
3          {
4              "key": "t",
5              "description": "Open the tag selection modal",
6              "action": "$('#addTagButton').click()"
7          },
8          {
9              "key": "f",
10             "description": "Open the freetext import modal",
11             "action": "$('#freetext-button').click()"
12          },
13          {
14              "key": "a",
15              "description": "Add an attribute",
16              "action": "console.log($('#liaddAttribute').children()[0].click())"
17          }
18      ]
19  }
```

(`action` field is JS code)

3. Include the keyboard shortcut config in the `.ctp` file you wish it to be used in using an `input type="hidden"` tag like this:

```
371 |   });  
372 | });  
373 | </script>  
374 | <input type="hidden" value="/shortcuts/event_view.json" class="keyboardShortcutsConfig" />
```

4. Test your shortcuts.

Last modified: Sun Feb 28 2021 09:22:59 GMT+0100 (Central European Standard Time)

MISP and Internationalization (i18n)

Requirements

Please read the following [CakePHP documentation about i18n & l10n](#).

Add one .md per translation effort

Please add a file à la: ja_JP.md (Japanese_Japan) or it_CH.md (Italian_Switzerland), in which you briefly describe what the current status of your translation effort is and what has been translated and which parts might be gotchas. This would also be a good place to quickly explain what your language is about, like whether most technical terms are a translation from the original, an adaptation from the English word or perhaps you just mostly use English terms.

Style

Please follow whatever is the purest and most intelligible form of written language in the native tongue being translated.

Formatting

It is important to use correct formatting. This is wrong:

```
<p><?php echo __('Are you sure you want to delete Proposal #') . $id . ' ' ?></p>
```

You want to have ultimate flexibility and that line should look more like this:

```
<p><?php echo __('Are you sure you want to delete Proposal #{ $id }?');?></p>
```

In the above example we use an alternative notation of the format string in PHP. Using the above, the generated po-template file ([default.pot](#)) will have the name of the to-be-translated variable in the "msgid" part of the file. Which is easier to read than a non descriptive %s and allows the translator to have context on how the phrase is used in MISP.

In case you have HTML-Tags, move them out of the sentence, out of the php code if possible:

```
<p><?php echo __('<h1>Are you sure you want to:<br />Delete Proposal #s?', $id
```

```
<p><h1><?php echo __('Are you sure you want to:%sDelete Proposal #{id}?', '<b
```

Issues

Some times it might be impossible to translate some phrases. Or you notice a certain bad formatting, or segmentation of sentences. In that case, please either open an [Issue on Github](#)

Quirks

Lines like this:

```
echo $this->Form->button('Submit', array('class' => 'btn btn-primary'));$
```

Should be prepared as such:

```
echo $this->Form->button(__('Submit'), array('class' => 'btn btn-primary'));
```

Or another case:

```
echo $this->Form->input('sharing_group_id', array(
    'options' => array($sharingGroups),
    'label' => 'Sharing Group',
));
```

To:

```
echo $this->Form->input('sharing_group_id', array(
    'options' => array($sharingGroups),
    'label' => __('Sharing Group'),
));
```

Let us know!

Are you planning to do a translation or localization? Please open a ticket on the [issue system](#). This will allow us and others to track what is being worked on. You can keep it very light, as all the details should be in your markdown in misp-book.

Reach out to the community

Want to chat with other MISP contributors? Make sure to join our [MISP Gitter channel](#).

Last modified: Wed May 05 2021 11:17:55 GMT+0200 (Central European Summer Time)

- Frequently Asked Questions
 - General questions
 - Where can I get support?
 - What are the hardware requirements?
 - How to monitor MISP?
 - Specific questions
 - Can I configure MISP encrypted notification emails to contain more information in the subject?
 - How can I restart the workers?
 - How can I redirect HTTP to HTTPS?
 - When I try to access my new installation, I am redirected to localhost:8443 and get an error.
 - How can I define the default sharing level?
 - How can I add an organisation logo and/or footer logo?
 - All workers are starting correctly except `schdlr`. How can I fix this?
 - How can I import data directly from PDF reports?
 - I am having trouble updating beyond version 2.4.50 (stuck loading any page beyond the login), what can I do?
 - I have many failed jobs when doing email notification. What should I do?
 - Upgrading from MISP 2.4.65 to MISP 2.4.66 - Unable to merge due to the Composer file.
 - I have issues with pushing events
 - I have many users or API accesses, what's the best PHP session handler?
 - Is there TAXII support?
 - Wipe MISP data - Remove all data
 - Constantly acknowledging my self-signed certificate drives me nuts
 - How can I change the theme?
 - How can I deal with a MISP instance that has pulled in feeds over and over into new events, generating hundreds of GBs of junk correlations, rendering the instance unusable?
 - I have a long list of events that I want to delete via the API, do I really have to loop through each and issue a delete to `/events/delete`?
 - I can no longer log in. How do I reset the admin password?
 - How do I set the baseurl from the command line?
 - Usage questions
 - How can I see all the deleted events in a MISP instance?
 - Permission issues
 - RHEL/CentOS
 - Redis Connection problems
 - RHEL/CentOS SELinux debug
 - Clearing the audit logs
 - When to update MISP?
 - How to switch from tagged releases and back?

- Update MISP fails
 - What can go wrong if I update MISP?
 - error: pathspec 'app/composer.json' did not match any file(s) known to git
 - MISP modules "Connection refused"
- Uninstalling MISP
- Updating PyMISP to incorporate newer versions of the MISP object templates
- How to disable freetext/custom/user-created tags and only allow certain tags
- How to enable the csv import module?
- Why do I see 'The request has been black-holed' when I submit forms?
- Importing large feeds creates PHP Fatal error
- I deleted the admin user by mistake
- config.php is not writeable
- How to debug misp-dashboard
- How to update object templates?
- What to do if my REST client is throwing SSL errors when trying to query my MISP instance?
- What to do if my REST client cannot reach the host, despite me being able to issue requests using Curl / Postman / etc.?
- How would one set up a sharing group with a remote org, where we only share a mutual community instance (i.e. we both have sync users on that instance). On our local instance, they exist as a remote org (from events that have synced from their instance via our shared community instance).
- Is it possible to propose objects to an event?
- How to use the enforceWarninglist parameter in REST search?
- Column not found issue
 - Symptoms
- WatchList Customization
 - How to create a customized WatchList.
- How to upgrade PHP on RHEL/CentOS?
 - Example: Upgrade from PHP 7.2 to 7.3 on CentOS 7
 - Enable repository
 - Install packages
 - Install required PEAR-modules
 - PHP configuration
 - Switch to PHP 7.3
 - Disable/enable services
- How to add a galaxy to an event via PyMISP
- Updating PHP from 7.2 to 7.4.5 on Ubuntu 18.04
 - Installation
 - Verification of php 7.2 to 7.4
 - What are the required steps after a MISP installation to have a properly running instance?

Frequently Asked Questions

The following page hosts some frequently asked questions as noticed in our [issues](#) and [gitter](#) channels.

General questions

Where can I get support?

If you have feature requests or you found a bug you can open a ticket on [MISP's GitHub repository issue](#) tracker.

If you want to discuss something related to MISP or want help from the MISP [community](#), join the appropriate MISP Gitter channel:

- [MISP Developer Room](#) Dev discussions
- [MISP Support Room](#) OMGoo! My MISP doesn't work discussions
- [MISP Sharing Room](#) Threat Intelligence Sharing discussions
- [misp-cloud Room](#) Using MISP in the clouds discussions

What are the hardware requirements?

From a hardware perspective, MISP's requirements are quite humble, a web server with 2+ cores and 8-16 GB of memory should be plenty, though more is always better of course. A lot of it depends on the data set and the number of users you are dealing with.

We recommend a standard LAMP stack on top of Ubuntu >18.04 LTS. For details on the exact dependencies please refer to the [installation guide](#) as well as the [requirements for the MISP modules](#).

During a [Hackathon](#) a small tool called [MISP-Sizer](#) was conceived. It will give you a **very rough** idea on what requirements are if you have a bigger installation. [source-code is here](#)

How to monitor MISP?

There are many ways to monitor MISP via the MISP [API](#) or relying on external tools. The following documentation is available for different monitoring tools:

- Using [Cacti](#), a blog post with the [instruction](#) is available.
 - Using [Munin](#), [misp-monitor](#) for instructions.
 - Using [Nagios](#), [Monitoring MISP with Nagios](#)
 - Using [OpenNMS](#), a blog post with the [instructions](#) is available.
 - [Live monitoring of MISP usage](#) via the httpd logs.
-

Specific questions

Can I configure MISP encrypted notification emails to contain more information in the subject?

The setting 'MISP.extended_alert_subject' allows you to have an extended subject. /\ Beware if you're using encryption: the subject will not be encrypted. Be aware that you might leak some sensitive information this way. Below is an example how the two subject types look like. First with the option disabled, then with the option enabled.

```
Event 7 - Low - TLP Amber
Event 8 - OSINT - Dissecting XXX... - Low - TLP Amber
```

(Source: [Getting started with MISP](#))

How can I restart the workers?

The workers can be restarted from the web interface:

```
administration -> server settings -> workers -> restart all
```

You can also follow the manual process below.

If you are on Ubuntu / Debian based systems:

```
sudo su -l www-data -s /bin/bash -c "bash /var/www/MISP/app/Console/worker/sta
```

If you are on RHEL / Fedora based systems:

```
su -s /bin/bash apache -c 'bash /var/www/MISP/app/Console/worker/start.sh'
```

How can I redirect HTTP to HTTPS?

```

<VirtualHost *:80>
    ServerAdmin misp@misp.misp
    ServerName misp.misp.misp
    ServerAlias misp-int.misp.misp

    Redirect permanent / https://misp.misp.misp

    LogLevel warn
    ErrorLog /var/log/apache2/misp.local_error.log
    CustomLog /var/log/apache2/misp.local_access.log combined
    ServerSignature Off
</VirtualHost>

<VirtualHost *:443>
    ServerAdmin misp@misp.misp
    ServerName misp.misp.misp
    ServerAlias misp-int.misp.misp

    DocumentRoot /var/www/MISP/app/webroot
    <Directory /var/www/MISP/app/webroot>
        Options -Indexes
        AllowOverride all
        Order allow,deny
        allow from all
    </Directory>

    SSLEngine On
    SSLCertificateFile /etc/ssl/misp.misp.misp/misp.crt
    SSLCertificateKeyFile /etc/ssl/misp.misp.misp/misp.key
    SSLCertificateChainFile /etc/ssl/misp.misp.misp/mispCA.crt

    LogLevel warn
    ErrorLog /var/log/apache2/misp.local_error.log
    CustomLog /var/log/apache2/misp.local_access.log combined
    ServerSignature Off
</VirtualHost>

```

Source: [Getting started with MISP](#)

When I try to access my new installation, I am redirected to localhost:8443 and get an error.

By default, MISP runs on a local instance and is setup for local access upon installation. This allows you to setup security and customizations before making it available elsewhere. If you would like to access the [MISP instance](#) from a remote host (including another VM host/client), assign an IP to the MISP host and point your browser accordingly. Please refer to [how to set the baseurl from command line](#). Once the update is done, you should then be able to access the instance using the set IP/DNS name.

How can I define the default sharing level?

MISP allows you to define the group of people with whom you want to share your threat data. If you do not set it to your preferred default then it's likely that at one given moment you'll make an error and share your intel with the wrong group. Defining the sharing level is done with the setting `default_event_distribution` in the configuration file. There are three levels:

```

0 : Your organisation only (default)
1 : This community only
2 : Connected communities
3 : All communities

```

You can set a similar configuration setting for the attributes. The setting `default_attribute_distribution` has the same values as `default_event_distribution`. Additionally it has the value `event` which allows the attribute to get the setting from the event to which it belongs.

Source: [Getting started with MISP](#)

How can I add an organisation logo and/or footer logo?

MISP can be made more appealing to the eye by adding some graphics.

As Org.- or Site-admin navigate to *Administration* -> *List organisations* and edit the corresponding organization. Withing this editor you will be able to update the logo.

Other ways to achieve this, would be:

Set your organisation logo by adding an image (.png) that has the same name as your organisation in the directory `/var/www/MISP/app/webroot/img/orgs/`.

Yet another way of doing this is by logging into your [MISP instance](#) with Admin rights, navigate to *Administration* -> *Server Settings*, tab -> *Manage files*.

You can add a footer logo. Add an image to the directory `/var/www/MISP/app/webroot/img/custom/` and define the footer logo in the config file (`config.php`) or in *Adminitration* -> *Server Settings...* -> *MISP settings* (search for: "footer_logo") point to the location on-disk of the image.

Partial source: [Getting started with MISP](#)

All workers are starting correctly except *schdlr* . How can I fix this?

This can happen if the [FQDN](#) of the server hosting the instance has changed. A way to fix this is to flush temporary data stored in redis. This can be done by logging in redis, for example when logging in with `redis-cli`, and issuing a *flushall* command.

How can I import data directly from PDF reports?

/!\ This section needs review, verification and eventual amendments to make sure it works.

You can use a generic script called [IOC parser](#) (https://github.com/armbues/ioc_parser) or use a script published by Palo Alto to convert [IOC parser](#) output to a [MISP event](#) (<https://github.com/PaloAltoNetworks->

[BD/report_to_misp/](#)). You have also the option to select all the text and paste it in the free-text import form.

Another option is the new [OCR import module](#) that can be used via the import modules. You will need to install the OCR software tesseract.

I am having trouble updating beyond version 2.4.50 (stuck loading any page beyond the login), what can I do?

!! This applies to an earlier version of MISP, do not randomly try this fix on valuable data. By all means try it on a test-machine and report back if your problem was solved by this.

This is most likely due to the fact that MISP did not clean up expired sessions prior to version 2.4.51 automatically and relied on a site-admin occasionally cleaning it up using the button found on the diagnostics page. Once you upgrade to 2.4.51, MISP will try to cull the table with each page load by a site-admin, which in some cases if the table has grown to extreme sizes it will get stuck on. To resolve the issue, log into mysql:

```
mysql -u [misp-db-user-name] -p [misp-db-name];
```

and execute the following commands:

```
DROP cake_sessions; CREATE TABLE IF NOT EXISTS cake_sessions ( id
varchar(255) COLLATE utf8_bin NOT NULL DEFAULT "", data text COLLATE
utf8_bin NOT NULL, expires int(11) NOT NULL, PRIMARY KEY ( id ), INDEX
expires ( expires ) ) ENGINE=InnoDB DEFAULT CHARSET=utf8
COLLATE=utf8_bin;
```

After this everything should work and the session table will be trimmed each time a site-admin loads a page.

I have many failed jobs when doing email notification. What should I do?

This is most probably due to some encryption failing for some users. We strongly advise to review the current PGP keys and to ensure that they keys are not expired or perhaps not supported anymore (weak keys). The keys can be reviewed at the following location in MISP:

```
https://<YOUR MISP URL>/users/verifyGPG
```

Upgrading from MISP 2.4.65 to MISP 2.4.66 - Unable to merge due to the Composer file.

In MISP 2.4.66, Composer is included by default to avoid the risk of downloading a rogue PHP Composer version (if the composer repository is compromised or MiTM are performed) via the download and php execution. But when upgrading (via a [git pull](#)), the git merge process might complain about the composer phar file still being there. You can safely remove that file and `git pull origin 2.4` again.

I have issues with pushing events

- What does the 'Connection test' for the specific server report? (*Sync Actions - > List Servers*)
- Is the event you assume to [push/pull](#) ready to be published?
- Is the distribution level set not too restrictive?
- Have you enabled [push](#) in the servers config you want to [push](#) to?
- Do you have any limitations to the [push](#) rules e.g. limited to a certain TLP Level tag or other?
- What is written in your job log?

<https://jobs/index>

Have a look at: `/var/www/MISP/app/tmp/logs` and `/var/log/apache2/misp` (or the relevant apache log folder of the instance in cause)

I have many users or API accesses, what's the best PHP session handler?

We strongly recommend production-level MISP installations to rely on PHP session in Redis. As Redis is already part of a standard MISP setup, we recommend to enable the redis session handling.

To configure the redis session handling in PHP, edit :

```
session.save_handler = redis
session.save_path = "tcp://127.0.0.1:6379"
```

Is there TAXII support?

A TAXII 1 implementation can be found at <https://github.com/MISP/MISP-Taxii-Server> . This is mostly a TAXII server hooked up to MISP, meant to receive STIX files to its in box and uploading them to MISP. There is also an experimental feature to [push](#) MISP events to the TAXII server when they're published - that's in `scripts/push_published_to_taxii.py` . It seems to work, but may occasionally re-upload duplicate events to MISP.

TAXII 2 is provided in the future once the specification, which is at time of writing in draft, reaches a stable form.

Wipe MISP data - Remove all data

If you need to start from scratch with your MISP database and remove all data you can use the `misp-wipe` script provided in the `tools/` folder.

Constantly acknowledging my self-signed certificate drives me nuts

You want to add it in 2 places: Your browser(s) and your OS.

The following steps can be performed on the CLI to install the Certificate:

```
sudo mkdir -m 0755 /usr/local/share/ca-certificates/MISP
sudo cp /etc/ssl/private/misp.local.crt /usr/local/share/ca-certificates/MISP
sudo chmod 0644 /usr/local/share/ca-certificates/MISP/misp.local.crt
sudo update-ca-certificates
```

For the Chrome Browser:

1. Visit: "Advanced Settings" -> `chrome://settings/?search=Manage+certificates`
2. Scroll down to: Manage Certificates (click)
3. Select: "Authorities"
4. Click: "Import"
5. Browse to your .crt file and import it.
6. On the next screen tick: "Trust this certificate for identifying websites"
7. Done, enjoy the new gained quality of life

Note: Chrome might expect a [Subject Alternative Name](#) make sure you created your certificate with '-extension san'.

To allow insecure localhost connections enable this option: `chrome://flags/#allow-insecure-localhost`

Sources: [CLI](#) and [Chrome/Chrome insecure localhost](#)

[For the Firefox Browser](#)

How can I change the theme?

MISP uses [bootstrap.css](#) the specific CSS file can be found on a typical MISP install at `/var/www/MISP/app/webroot/css/bootstrap.css`.

You can customize this for your own needs. There are also pre-made bootstrap themes which you can use as-is or build upon.

Before making any changes, confirm the version of bootstrap currently used by running `head -5 /var/www/MISP/app/webroot/css/bootstrap.css`. You can find themes on sites like [Bootswatch](#).

To replace the current theme with a theme you found on bootswatch, run: `sudo -u www-data wget https://bootswatch.com/2/readable/bootstrap.css -O /var/www/MISP/app/webroot/css/bootstrap.css`, replacing the URL as needed.

Some bootswatch themes applied on MISP:

- <https://i.imgur.com/usONTLk.png>
- <https://i.imgur.com/5XMjB7o.png>
- <https://i.imgur.com/5gc57VU.png>
- <https://i.imgur.com/4AJCPgf.png>
- <https://i.imgur.com/JuMGm8U.png>
- <https://i.imgur.com/v1Wu6xW.png>

How can I deal with a MISP instance that has pulled in feeds over and over into new events, generating hundreds of GBs of junk correlations, rendering the instance unusable?

Step 1: ensure that all your CSV/freetext source_format feeds are using the fixed event setting. If you want to make sure this is the case, you can run this SQL query instead of doing it manually:

```
UPDATE feeds SET fixed_event = 1 WHERE source_format="csv" OR source_format="f
```

Step 2: purge all of your correlations (this will make the next steps much faster), for which you have two methods at your disposal:

- either go to your administration -> server settings -> MISP tab and set `MISP.completely_disable_correlation` to `true`
- via MYSQL run `TRUNCATE correlations;`

Step 3: purge all of your feed data that have been pulled into multiple events. The easiest way of doing this: check which feeds are enabled (ignore misp source format feeds, they are not causing issues) and note down the IDs. Afterwards, use the CLI cleanup tool to remove all the feed events:

```
/var/www/MISP/app/Console/cake Admin purgeFeedEvents [user_id] [feed_id]
```

Execute this for each feed that you had enabled, replacing `user_id` with your admin user's ID and `feed_id` with the individual feed IDs on your list.

Step 4: recorelate your data, depending on which method you've used in *Step 2* you have two options:

- either go to your *Administration* -> *Server Settings...* -> *MISP...* tab and set `MISP.completely_disable_correlation` to `false`
- recorelate your current data-set via the recorelate attributes tool on `/pages/display/administration`

I have a long list of events that I want to delete via the API, do I really have to loop through each and issue a delete to `/events/delete`?

No, the delete action also accepts a list of IDs when it comes to bulk event deletions.

Simply POST your ID list to `/events/delete` in the following format:

```
{
  "id": [1,3,5,7,9]
}
```

I can no longer log in. How do I reset the admin password?

You can reset the password via the console. See [Issue #1160](#)

```
/var/www/MISP/app/Console/cake Password [email] [password]
```

How do I set the baseurl from the command line?

You can change the baseurl via the console.

```
sudo -u www-data /var/www/MISP/app/Console/cake Baseurl [baseurl]
```

You can confirm the baseurl is updated correctly by checking the config.php file

```
grep baseurl /var/www/MISP/app/Config/config.php
```

Usage questions

How can I see all the deleted events in a MISP instance?

You can use the logging system for this, to see all deleted events, simply go to *Audit -> Search Logs* and use the following parameters:

```
model: Event
action: delete
```

This will list all event deletions. To find out more about what a particular deleted event was, simply grab the ID from the above search results and search for:

```
model: Event
action: add
model_id: <Event ID retrieved from the listing of all event deletions>
```

To do the same via the [API](#), first search for the deletions:

```
POST request:
url: https://url.of.your.misp/logs/index
headers:
  Authorization: <your_api_key>
  Accept: application/json
  Content-type: application/json
Body:
{
  "model": "Event",
  "action": "delete"
}
```

Then find the individual event's metadata that was deleted

```

POST request:
url: https://url.of.your.misp/logs/index
headers:
  Authorization: <your_api_key>
  Accept: application/json
  Content-type: application/json
Body:
{
  "model": "Event",
  "action": "add",
  "model_id": "<Event ID retrieved from the query before>"
}

```

Permission issues

If you have any permission issues, please [set the permissions](#) to something sane first.

RHEL/CentOS

There are a plethora of issues that might arise when using SELinux when it comes to permissions. First, please familiarize yourself with [the basics](#) of SELinux. RedHat has a comprehensive [SELINUX USER'S AND ADMINISTRATOR'S GUIDE](#).

For file system permissions, refer to the [install guide](#) first.

Another way to see what SELinux might not be happy about is to use **ausearch**. This assumes Audit is enabled.

```

# Just php-fpm
sudo ausearch -c 'php-fpm' --message AVC
# All messages
sudo ausearch --message AVC

```

Redis Connection problems

If you have the following in **error.log**

```

2019-05-08 10:16:05 Error: [RedisException] Permission denied
Request URL: /events/view/1
Stack Trace:
#0 /var/www/MISP/app/Model/AppModel.php(1776): Redis->connect('127.0.0.1', 6379)
#1 /var/www/MISP/app/Model/Feed.php(329): AppModel->setupRedis()
#2 /var/www/MISP/app/Model/Event.php(2073): Feed->attachFeedCorrelations(Array,
#3 /var/www/MISP/app/Controller/EventsController.php(1547): Event->fetchEvent(/
#4 [internal function]: EventsController->view('1')
#5 /var/www/MISP/app/Lib/cakephp/lib/Cake/Controller/Controller.php(499): Refl
#6 /var/www/MISP/app/Lib/cakephp/lib/Cake/Routing/Dispatcher.php(193): Control
#7 /var/www/MISP/app/Lib/cakephp/lib/Cake/Routing/Dispatcher.php(167): Dispatch
#8 /var/www/MISP/app/webroot/index.php(92): Dispatcher->dispatch(Object(CakeRec
#9 {main}

```

This means that apache/php-fpm cannot connect over the network (localhost included).

Fix:

```
sudo setsebool -P httpd_can_network_connect on
# Perhaps a reload is not needed, but good practice wants us to test it anyways
sudo systemctl restart rh-php72-php-fpm.service
sudo systemctl restart httpd.service
```

RHEL/CentOS SELinux debug

More often than not there might be issues with SELinux when not configured correctly. The below will give you pointers where to look and how to figure out what is wrong.

You can investigate SELinux issues without any tools by opening the audit log it generates. This log is found at `/var/log/audit/audit.log`. However, unless you know exactly what to look for and have a lot of free time, you're going to find it difficult making sense of the log.

Install some handy tools:

```
# Note: This will pull in some X tools, you have been warned
sudo yum install setroubleshoot setools
```

We now have a tool called `sealert` that analyzes the audit log used by SELinux. `Sealert` will scan the log file and will then generate a report containing all discovered SELinux issues. In this overview of what went wrong you will see suggestions on how to fix them after the issue detected.

To run `sealert` from the command-line, we need to point it to the SELinux audit log.

```
sudo sealert -a /var/log/audit/audit.log
```

Clearing the audit logs

It is not recommended to clear the audit logs as they might contain information needed in the future for troubleshooting or security investigations. However, if that is not the case, just empty the audit log:

```
# > /var/log/audit/audit.log
```

[Partial source](#)

[StackExchange](#)

[Gentoo Wiki](#)

When to update MISP?

One question might be how often to update MISP. You can update MISP as often as you like. If you see the following:

MISP version

Every version of MISP includes a json file with the current version. This is checked against the latest tag on github, if there is a version mismatch the tool will warn you about it. Make sure that you update MISP regularly.

Currently installed version... v2.4.97 (4462a72206a9cce39559c1facee90efdec2a308d)

Latest available version... v2.4.97 (6e9b6fb80382346f338aa94f37b52d326b7cc551)

Status... OK

Current branch... 2.4

Update MISP

This means that the main repository has an update available.

If you want to play it safer or want to integrate it in your Weekly/Bi-Monthly update routine you can track our [Changelog](#) a more up to date version is available [here](#)

Further on we do regular tagged releases. (Approximately once per month.) The releases happen either if a milestone has been hit for a certain feature/improvement/fix or for any security related matters.

Thus you have the choice of either tracking 2.4 which is on a rolling release schedule, or track the tagged releases.

How to switch from tagged releases and back?

This can be achieved with the following git commands:

```
$ cd /var/www/MISP # aka. $PATH_TO_MISP
$ sudo -H -u www-data git checkout tags/$(git describe --tags `git rev-list --tags --max-count=1`)

## OS Upgrades

In theory all should "just work"(tm), but in practice the following dependencies are required:

* php/pear
* python
* apache
* init scheme/scripts
* mariadb/mysql
* redis
* git

### PHP

This is probably the most likely one that might get you into trouble.
The following happened on a Debian Testing lately. During the upgrade php got updated.
The fix was to remove any *libapache2-mod-php7.2* packages and make sure that the correct version is installed.
Then double check if all the php dependencies are installed, refer to the installation instructions.

The same for pear, where we mostly use 2 (bundled) packages: Console Command Line Tool and PEAR.
If you upgrade from a very old and out of date version of MISP this might raise some issues.

php.ini might also become problematic if you just erase the recommended default configuration.

### Python3

If you use python2 for MISP, please read the install docs about MISP being Python2.
Currently Python3.6 is minimum. It is known working on 3.7 with some minor differences.
The biggest issue is certainly with PyMISP doing unexpected things when python is upgraded.
Using a virtualenv, whilst not always ideal for all setups, will at least make it easier to manage.

### Apache

Mostly config issues might be a show stopper. And major version updates where some config changes are required.

### init/systemd

MISP launches a couple of things on boot. Changing what handles boot behaviour might be problematic.

### MariaDB/MySQL/redis

Similar to apache, most importantly always take good care that the DB engine is properly updated.
From minor to major updates, rarely things might need to be adapted.

### git

Currently (as of v2.4.108) the git-cli command is used in MISP core. In very rare cases you might need to use the git command.
Included here more as an FYI than anything else.

## Hardening

### How do I harden my MISP instance?

You can check the [hardening section](https://misp.github.io/MISP/generic/hardening/) for more information.

## Maintenance mode

### Is there a MISP maintenance mode?

Yes, you want to flip your instances "Live-mode".
This wants to be done on the CLI if you experience issues:
```



```

$ bash
$PATH_TO_MISP/app/Console/cake "MISP.live" 0

```

Other related MISP Settings

Optional `MISP.maintenance_message` Great things are happening! MISP is undergoing maintenance, but will return shortly. You can contact the administration at \$email or call CIRCL. The message that users will see if the instance is not live.

Critical `MISP.live` true Unless set to true, the instance will only be accessible by site-admins.

Update MISP fails

If your [MISP instance](#) is outdated, meaning ONLY the core, not the modules or dashboard or python modules, you will see the following.

MISP version

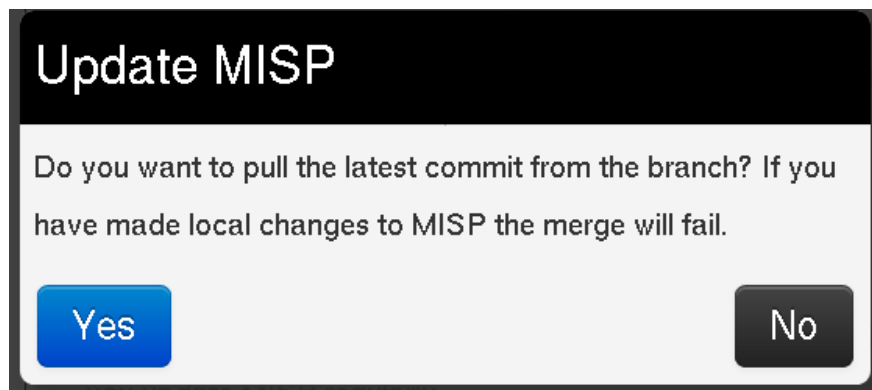
Every version of MISP includes a json file with the current version. This is checked against the latest tag on github, if there is a version mismatch the tool will warn you about it. Make sure that you update MISP regularly.

```

Currently installed version... v2.4.96 (f3850747da103ca616a7dbaab955df373db272f7)
Latest available version... v2.4.97 (ce3c78cd7db60812d0147ced992a7650509d31da)
Status... Outdated version
Current branch... 2.4
Update MISP

```

Once you click on update MISP you will be asked confirmation.



If you are not on a branch, the UI will tell you this, the update will fail.

Currently installed version.. v2.4.96 (bbc8a8bf4dce4d64fb676a3a76bb4c6be091e890)

Latest available version.. v2.4.97 (ce3c78cd7db60812d0147ced992a7650509d31da)

Status **Outdated version**

Current branch.. **You are not on a branch, Update MISP will fail**

```
git checkout app/composer.json 2>&1

error: pathspec 'app/composer.json' did not match any file(s) known to git

git pull origin 2>&1

error: pathspec 'app/composer.json' did not match any file(s) known to git
You are not currently on a branch.
Please specify which branch you want to merge with.
See git-pull(1) for details.

    git pull <remote> <branch>

=====

git submodule update --init --recursive 2>&1
```

Update MISP

If you cannot write the **.git** files and directory as the user running the web server (and thus PHP), the update will fail. The following diagnostic check will let you know if you can update or not.

Writeable Files

```
/var/www/MISP-priv/app/Config/config.php...OK
```

```
/var/www/MISP-priv/.git/ORIG_HEAD...File is not writeable
```

In case you get a file not found on **.git/ORIG_HEAD**, this means that you have never updated your MISP OR you have installed git from an archive file (like .zip/.tar.gz or similar) Try to click update MISP and see what happens.

Writeable Files

/var/www/MISP/app/Config/config.php...OK

/var/www/MISP/.git/ORIG_HEAD...File not found

What can go wrong if I update MISP?

In theory nothing. We put great effort into protecting the integrity of the data stored in your [MISP instance](#). DB upgrades happen upon login or on reload once you have update the repository. You cannot "break" anything by clicking **Update MISP** worse case it will complain about something and you will certainly find the answer on this page.

IF not, please open an [issue](#) on GitHub or come to our [gitter](#) chat to see if the [community](#) can help.

error: pathspec 'app/composer.json' did not match any file(s) known to git

This is **not** an error and can be ignore. Nothing will be impacted by this.

Currently installed version... **v2.4.96 (f3850747da103ca616a7dbaab955df373db272f7)**

Latest available version... **v2.4.97 (ce3c78cd7db60812d0147ced992a7650509d31da)**

Status... **Outdated version**

Current branch... 2.4

```
git checkout app/composer.json 2>&1

error: pathspec 'app/composer.json' did not match any file(s) known to git

git pull origin 2.4 2>&1

error: pathspec 'app/composer.json' did not match any file(s) known to git
From https://github.com/MISP/MISP
 * branch                2.4          -> FETCH_HEAD
    f3850747d..ce3c78cd7  2.4          -> origin/2.4
Updating f3850747d..ce3c78cd7
Fast-forward
 VERSION.json                | 2 +-
 app/Controller/AppController.php | 2 +-
 app/Controller/Component/ACLComponent.php | 1 +
 app/Controller/Component/RestResponseComponent.php | 16 ++-
 app/Controller/EventsController.php | 2 +-
 app/Controller/SightingsController.php | 36 ++++++
 app/Lib/Export/CsvExport.php | 28 +++++
 app/Lib/Export/JsonExport.php | 9 +-

```

MISP modules "Connection refused"

Module System

This tool tests the various module systems and whether they are reachable based on the module settings.

Enrichment module system. **Connection refused**

Import module system. **Connection refused**

Export module system. **Connection refused**

Cortex module system. **System not enabled**

If you get have a **Connection refused state** on your modules one of the following might be true.

- You have no [misp-modules](#) not installed
- They are installed but not running
- Something completely different

If they are not installed, check out this section of the [INSTALL guide](#) of [misp-modules](#).

In case they are not running, try this on the console:

```
sudo -u www-data /var/www/MISP/venv/bin/misp-modules -l 127.0.0.1 -s &
```

OR if you were foolish enough to not install in a Python virtualenv:

```
sudo -u www-data misp-modules -l 127.0.0.1 -s &
```

[warning] Running misp-modules like this will certainly kill it once you quit the session. Make sure it is in your **/etc/rc.local** or some ther init script that gets run on boot.

Uninstalling MISP

There is no official procedure to uninstalling a [MISP instance](#).

If you want to re-use a machine where MISP was installed, wipe the machine and do a fresh install. Consider the data in your [MISP instance](#) as potentially confidential and if you synchronized with other instances, be respectful and wipe it clean.

Updating PyMISP to incorporate newer versions of the MISP object templates

In some cases, for instance if a newer version of a MISP object is present on the server but not yet on PyMISP, you want to reflect the current state in your PyMISP installation.

In order to do so, perform the following steps. It fetches the latest object templates and installs PyMISP again:

```
git clone https://github.com/MISP/PyMISP.git
cd PyMISP/pymisp/data
git submodule update --init
cd misp-objects
git pull origin master
cd ../../../../
sudo pip3 install -I .
```


How to disable freetext/custom/user-created tags and only allow certain tags

Remove the "tag editor" from the permissions that you grant to users. Set all tags that you do not want to "hidden". There is a server setting to treat all incoming tags as hidden by default: `MISP.incoming_tags_disabled_by_default`

Important Make sure that you don't remove "tag editor" from sync users, or you'll be stripping tags from synchronized data.

How to enable the csv import module?

First you have to enable the import services: double-click on "false" in the very first line and change it to "true".

In Server Settings & Maintenance -> Plugin Settings -> Import -> set "Plugin.Import_csvimport_enabled" to true. Afterwards you'll find the csvimport from within the newly created event: "Populate from..."

Don't use from the main site ("Import from...").

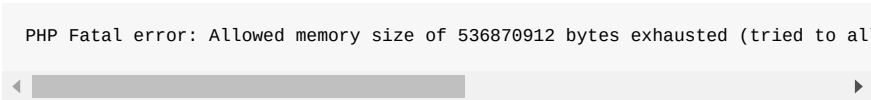
Why do I see 'The request has been black-holed' when I submit forms?

That's a security measure for form tampering protection.

All forms have a timeout (~15min) and all of them can only be submitted once. If you use your browser's "back" button and resubmit the form MISP will consider it as a potential attempt at form tampering.

Importing large feeds creates PHP Fatal error

When importing a large feed like the CIRCL feed, the job reaches 99% and then fails. The log file records:



```
PHP Fatal error: Allowed memory size of 536870912 bytes exhausted (tried to allocate 1048576 bytes) in /var/www/misp/lib/MISP/Model/Event.php on line 100
```

In this case you will need to increase the `memory_limit` option in `php.ini` file

I deleted the admin user by mistake

Now, I only have [Org Admin](#).

You have several options:

1. Delete the [org admin](#). MISP automatically creates a new default site-admin user if no users are found in the db (mysql: truncate users;)
2. Upgrade a user to a site-admin, such as an [org admin](#) user:

```
SELECT id, email from users;
```

Note down the ID you want to upgrade. Let's say this is 2 for the example's sake.

```
SELECT id, name from roles;
```

Note down the role ID you want to upgrade. Let's say this is 1 for the example's sake.

```
UPDATE users set role_id = 1 where id = 2;
```

config.php is not writeable

```
Warning: app/Config/config.php is not writeable. This means that any setting ch
```

According to the install guide, make sure to:

```
chown -R apache:apache /var/www/MISP
find /var/www/MISP -type d -exec chmod g=rx {} \;
chmod -R g+r,o= /var/www/MISP
```

If it still doesn't work, make sure SELinux is not enabled or modify the rule set:

```
chcon -t httpd_sys_rw_content_t /var/www/MISP/app/files
chcon -t httpd_sys_rw_content_t /var/www/MISP/app/files/terms
chcon -t httpd_sys_rw_content_t /var/www/MISP/app/files/scripts/tmp
chcon -t httpd_sys_rw_content_t /var/www/MISP/app/Plugin/CakeResque/tmp
chcon -R -t httpd_sys_rw_content_t /var/www/MISP/app/tmp
chcon -R -t httpd_sys_rw_content_t /var/www/MISP/app/webroot/img/orgs
chcon -R -t httpd_sys_rw_content_t /var/www/MISP/app/webroot/img/custom
```

How to debug misp-dashboard

This is the full chain from MISP to the live dashboard and some tips to find out which link is faulty.

1. MISP Ensure that ZMQ is installed and enabled with the correct settings
2. MISP ZMQ You can use MISP/tools/misp-zmq/sub.py which will subscribe to the ZMQ and print the data

3. ZMQ_subscriber You can change the logging level from logging.INFO to logging.DEBUG and look in the logs for the string Pushed: * Or add a print statement in the put_in_redis_list function
4. ZMQ_dispatcher Look in the logs for the string Handling *
5. Server (Flask) and Browser (live Dashboard) Open the Web developer Network tab in your browser and look for the url /_logs with Content-Type: text/event-stream;

How to update object templates?

`git submodule update` in your MISP directory (or via the diagnostic page) and just click "Update Objects" in List Object Templates.

What to do if my REST client is throwing SSL errors when trying to query my MISP instance?

The REST client will use the framework's certificate store to validate the contacted host. If your root CA / self-signed certificate is not known by the certificate store, the request will fail. You can skip the SSL validation altogether using the "Skip SSL validation" checkbox.

What to do if my REST client cannot reach the host, despite me being able to issue requests using Curl / Postman / etc.?

The REST client issues instructions to your MISP server to contact a remote host (most commonly itself). Always consider how your MISP server can address itself when using the REST client, by default it will prepend the requested relative path in the URL field with the instance's baseurl.

If your MISP cannot reach itself via the baseurl the request will fail. You can use the "Use full path - disclose my API key" checkbox along with the full URL in the URL field to instruct MISP to use another path than what it would construct using the baseurl.

How would one set up a sharing group with a remote org, where we only share a mutual community instance (i.e. we both have sync users on that instance). On our local instance, they exist as a remote

org (from events that have synced from their instance via our shared community instance).

It is not possible to do that. Keep in mind that if you are both on a mutual [community](#) instance, someone is in charge of that instance that will have database and admin level access. They would be able to inspect the data you exchange on their [community](#) instance with one another, so MISP will block any attempt to share with them.

If you really want to go through the [community](#) instance to exchange with them, you explicitly have to include the host organisation of the [community](#) instance (they would get access if they wanted to anyway, this way we can ensure that you are clear about that):

- You are org a on instance A.
- Your partner that you want to share with is org b on instance B.
- You have no way of directly reaching org b, but you both have access to instance C, which is run by org c (the sharing instance)
- In order to reach org b, you have two options for [sharing groups](#), depending on whether you want to be able to [push](#) to them or want to rely on them pulling data from the [community](#) instance:

```
SG Option 1 (push all the way to B)
orgs: a, b, c
instances: A, B, C
```

```
SG Option 2 (b has to pull from C):
orgs: a, b, c
instances: A, C
```

Is it possible to propose objects to an event?

This is not possible yet. What you can do at the moment: Create a new event and extend it with the other (foreign) event.

How to use the enforceWarninglist parameter in REST search?

If you would like to export IoCs, for example into a suricata rule and exclude all values matching your warning lists, you can use the following:

```
{
  "returnFormat": "suricata",
  "published": 0,
  "enforceWarninglist": 1
}
```

Keep in mind that unpublished events need the `"published": 0` parameter in order to be exported.

Column not found issue

When a user attempts to add an object to an event and the following error is received (Level 1 debug enabled):

```
SQLSTATE[42S22]: Column not found: 1054 Unknown column 'Event.org_id' in 'where clause'
```

One potential resolution is to upgrade MISP to 2.4.107.

Symptoms

Users with the site-admin role are able to add objects to events without any error. This error was encountered when a user belonged to every role **except** site-admin.

WatchList Customization

How to create a customized WatchList.

WatchLists are stored within folder under `/var/www/MISP/app/files/warninglists/lists` Every folder contains a `list.json` file. Create a new folder and copy and modify an existing list (or create a new one from scratch). Ensure the "name" value within the file is unique. Increment the version number when the file is changed.

Within the MISP GUI, go to WarningLists and "Update WarningLists".

The new WarningList will now show up. In case of errors, check the permissions on the `list.json` and it's folder.

To modify the list or to add entries to it, go back to the file via the CLI, modify the file and reload it via the GUI ("Update WarningLists").

How to upgrade PHP on RHEL/CentOS?

To our knowledge, there is no way to "upgrade" PHP. You'll need to install the new PHP version like you're doing a fresh install. You may try copying your old

`php.ini` to your new PHP config directory which may work. We would recommend redoing the config though.

Example: Upgrade from PHP 7.2 to 7.3 on CentOS 7

Enable repository

```
$ sudo yum install -y http://rpms.remirepo.net/enterprise/remi-release-7.rpm
$ sudo yum-config-manager --enable remi-php73
```

Install packages

```
$ sudo yum install -y php73-php php73-php-cli php73-php-fpm php73-php-devel php73-php-gd
```

Confirm GPG key if required:

```
Retrieving key from file:///etc/pki/rpm-gpg/RPM-GPG-KEY-remi
Importing GPG key 0x00F97F56:
  Userid      : "Remi Collet <RPMS@FamilleCollet.com>"
  Fingerprint: 1ee0 4cce 88a4 ae4a a29a 5df5 004e 6f47 00f9 7f56
  Package     : remi-release-7.6-2.el7.remi.noarch (installed)
  From        : /etc/pki/rpm-gpg/RPM-GPG-KEY-remi
  Is this ok [y/N]: y
```

Install required PEAR-modules

```
$ sudo php73-pear channel-update pear.php.net
Updating channel "pear.php.net"
Update of Channel "pear.php.net" succeeded
$ sudo php73-pear install /var/www/MISP/INSTALL/dependencies/Console_CommandLine
install ok: channel://pear.php.net/Console_CommandLine-1.2.2
$ sudo php73-pear install /var/www/MISP/INSTALL/dependencies/Crypt_GPG/package
install ok: channel://pear.php.net/Crypt_GPG-1.6.3
```

PHP configuration

Edit `/etc/opt/remi/php73/php.ini` :

```
date.timezone = "Europe/Berlin"
max_execution_time = 300
memory_limit = 512M
upload_max_filesize = 50M
post_max_size = 50M
```

Switch to PHP 7.3

```
$ sudo systemctl stop rh-php70-php-fpm
$ sudo systemctl start php73-php-fpm
# check if everything's fine
$ sudo systemctl status php73-php-fpm
```

Now check if the MISP web UI is accessible and if the diagnostics page shows any errors.

The diagnostics page will show "PHP CLI Version (>7.2 recommended): Unknown (Issues determining version)". That's a [known issue](#).

Disable/enable services

```
$ sudo systemctl disable rh-php70-php-fpm
Removed symlink /etc/systemd/system/multi-user.target.wants/rh-php70-php-fpm.service
$ sudo systemctl enable php73-php-fpm
Created symlink from /etc/systemd/system/multi-user.target.wants/php73-php-fpm.service to /usr/lib/systemd/system/php73-php-fpm.service
```

How to add a galaxy to an event via PyMISP

A galaxy can be assigned like a tag. You can use the add tag function and copy the full connector-tag. Example `misp-galaxy:ransomware="Locky"`, which can be found in `/galaxy_clusters/view/`

Updating PHP from 7.2 to 7.4.5 on Ubuntu 18.04

Installation

1. Disable and Uninstall Currently Installed SSDEEP

```
sudo phpdismod ssdeep
sudo pecl uninstall ssdeep
sudo apt purge ssdeep
sudo rm -rf /etc/php/7.2/mods-available/ssdeep.ini
```

2. Install PHP 7.4.5

```
sudo apt install software-properties-common -y
sudo add-apt-repository ppa:ondrej/php -y
sudo apt update
sudo apt install -y \
    libapache2-mod-php7.4 \
    php7.4 \
    php7.4-cli \
    php7.4-dev \
    php7.4-json \
    php7.4-xml \
    php7.4-mysql \
    php7.4-opcache \
    php7.4-readline \
    php7.4-mbstring \
    php-redis \
    php-gnupg \
    php-gd
sudo apt update
sudo apt upgrade -y
```

3. Install SSDEEP

```
cd /usr/local/src
sudo rm -rf ssdeep-2.14.1.tar.gz ssdeep-2.14.1
sudo wget https://github.com/ssdeep-project/ssdeep/releases/download/release-2.14.1/ssdeep-2.14.1.tar.gz
sudo tar xzvf ssdeep-2.14.1.tar.gz
cd ssdeep-2.14.1
sudo ./configure --datadir=/usr --prefix=/usr --localstatedir=/var --sysconfdir=/etc
sudo make
sudo make install
```

4. Test SSDEEP

```
ssdeep -h
```

5. Install ssdeep_php

```
sudo pecl channel-update pecl.php.net
sudo pecl install ssdeep
```

6. Enable SSDEEP in both 7.2 and 7.4 (**as root** `sudo su`)

```
echo 'extension=ssdeep.so' > /etc/php/7.2/mods-available/ssdeep.ini
echo 'extension=ssdeep.so' > /etc/php/7.4/mods-available/ssdeep.ini
```

7. Enable SSDEEP PHP Mod

```
sudo phpenmod ssdeep
```

8. Set PHP 7.4.5 to default PHP

```
sudo a2dismod php7.2
sudo a2enmod php7.4
sudo update-alternatives --set php /usr/bin/php7.4
```

9. [Optional] Set better values for defaults

```
sudo sed -i "s/max_execution_time = 30/max_execution_time = 300/" /etc/php/7.2/mods-available/ssdeep.ini
sudo sed -i "s/memory_limit = 128M/memory_limit = 2048M/" /etc/php/7.4/apac
sudo sed -i "s/upload_max_filesize = 2M/upload_max_filesize = 500M/" /etc/
sudo sed -i "s/post_max_size = 8M/post_max_size = 500M/" /etc/php/7.4/apac
sudo sed -i "s/max_execution_time = 30/max_execution_time = 300/" /etc/php/7.4/apac
sudo sed -i "s/upload_max_filesize = 2M/upload_max_filesize = 500M/" /etc/
sudo sed -i "s/post_max_size = 8M/post_max_size = 5000M/" /etc/php/7.4/cli
```

10. Restart Apache to implement changes

```
sudo sudo systemctl restart apache2
```

Verification of php 7.2 to 7.4

1. Administration > Server Settings & Maintenance

2. Diagnostics

3. Scroll down to the **PHP Settings** section and verify

What are the required steps after a MISP installation to have a properly running instance?

- First login with the installation credentials and change the password immediatly (especially if your instance is publicly accessible)
- Set the `base_url` to the hostname of your machine (apache virtualhost name)
- Create a new organisation which will be the host organisation running the [MISP instance](#)
- Set the new organisation in `MISP.host_org_id` to replace the default one
- Set messages like `MISP.footermidleft` and alike to a proper message to help your users
- Create a new user as `admin` role with the new organisation
- Log with the new user, if successful, remove the default user used during the installation such as `admin@admin.test`
- Select and enable required taxonomies for your sharing [community](#)
- Select and enable the external feeds (as caching only if you don't want full events but you can get the full feeds too)
- Select and enable the warning-list (if you don't know what to enable, select all)
- Add the remote MISP instances where you have access to (either caching only or full [pull](#) if you want the complete events)

Last modified: Sun Feb 28 2021 09:22:59 GMT+0100 (Central European Standard Time)

Developer FAQ

Main Developer Resources

The main developer resources can be found on GitHub in the [MISP Wiki](#).

The following pages are worth inspecting closer in case you want to actively develop for MISP:

- [The real FAQ](#)
- [Contributor Overview](#)
- [Some objectives of MISP](#)
- [Various deployment tools](#)
- [MISP Code of Conduct](#)
- [UI coloring scheme](#)
- [Notes on MISP and STIX 2](#)
- [Commit Messages Best Practices](#)
- [Internationalization \(i18n\)](#)

Our [gitter channel](#) is a welcome place to ask other [community](#) developers in case you are stuck.

Last modified: Sun Feb 28 2021 23:24:20 GMT+0100 (Central European Standard Time)

- [Best Practices](#)
 - [Tagging](#)
 - [Tagging at event level versus tagging at attribute level](#)
 - [Minimal subset of tags to use for each event](#)
 - [Traffic Light Protocol](#)
 - [Confidence](#)
 - [Origin](#)
 - [Permissible Actions Protocol](#)
 - [Setting distribution](#)
 - [Use objects instead of combined attributes](#)
 - [Use proposals when possible to request author to make changes to an event](#)

Best Practices

The following page hosts some best practices for the usage of the MISP platform. For generic threat intelligence practices, please refer to [MISP project - best practices in threat intelligence](#).

Tagging


Tagging at event level versus tagging at attribute level

You can add tags to an entire event. For a more fine-grained specification tags can also be placed at attribute level. This allows the user to put a more detailed and selective view on each attribute. If a tag applies to all or most attributes in the event, the best practice is to only include a specific tag for the attributes when they are an exception from the tag set at event level. In the below screenshot you see an example of the best practice, the tlp:white tag is only set at the event level.

Good practice tagging event

Event ID	1279
UUID	2efcd218-4c8a-4943-a040-fcd93aa2949a
Creator org	Setec Astronomy
Owner org	Setec Astronomy
Creator user	admin@admin.test
Tags	ip.white
Date	2021-02-28
Threat Level	High
Analysis	Initial
Distribution	This community only
Info	Good practice tagging event
Published	No
Attributes	4 (0 Objects)
First recorded change	2021-02-28 16:08:57
Last change	2021-02-28 16:09:14
Modification map	
Signings	0 (0) - restricted to own organisation only

Related Events

 OSINT - Babuk Ransomware
2021-01-05 4








[+Pivots](#) [+Galaxy](#) [+Event graph](#) [+Event timeline](#) [+Correlation graph](#) [+ATT&CK matrix](#) [+Event reports](#) [+Attributes](#) [+Discussion](#)

1279: Good p...

Galaxies

[v previous](#) [next v](#) [view all](#)

<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>Scope toggle</div><div>Deleted</div><div>LC Decay score</div><div>SigningsDB</div><div>Context</div><div>Related Tags</div><div>Filtering tool</div></div> <th>Date ?</th> <th>Org</th> <th>Category</th> <th>Type</th> <th>Value</th> <th>Tags</th> <th>Galaxies</th> <th>Comment</th> <th>Correlate</th> <th>Related Events</th> <th>Feed title</th>	Date ?	Org	Category	Type	Value	Tags	Galaxies	Comment	Correlate	Related Events	Feed title
<input type="checkbox"/>	2021-02-28		External analysis	link	https://twitter.com/Rekkent_SCI/status/1345566395726242373	 	 		<input checked="" type="checkbox"/>	1209	
<input type="checkbox"/>	2021-02-28		External analysis	link	http://shuangdong.com/reverse/20engineering/2021/01/03/BabukRansomware/	 	 		<input checked="" type="checkbox"/>	1209	
<input type="checkbox"/>	2021-02-28		Payload delivery	shu256	8203c2f0dec33ae960a5247a7d7b8b35e55c38939807c85db4b5c9205495f a9	 	 		<input checked="" type="checkbox"/>	1209	
<input type="checkbox"/>	2021-02-28		Payload delivery	md5	e10713a4a9635767dc0544609bec977	 	 		<input checked="" type="checkbox"/>	1209	

[v previous](#) [next v](#) [view all](#)

In the next screenshot you see a bad practice example. The tlp:white tag is added to both the event and all the attributes.

Bad practice tagging event

Event ID	1279
UUID	2efc8216-4dca-4463-a040-fc9d3ba548bc
Creator org	Secter-Absconomy
Owner org	Secter-Absconomy
Creator user	admin@admin.test
Tags	tlp:white
Date	2021-02-28
Threat Level	High
Analysis	Initial
Distribution	This community only
Info	Bad practice tagging event
Published	No
Attributes	4 (0 Objects)
First recorded change	2021-02-28 16:07:08
Last change	2021-02-28 16:08:22
Modification map	
Sightings	0 (0) - restricted to own organisation only

[Photos](#) [Galaxy](#) [Event graph](#) [Event timeline](#) [Correlation graph](#) [ATT&CK matrix](#) [Event reports](#) [Attributes](#) [Discussion](#)

1279: Bad pr...

Galaxies

[Previous](#) [Next](#) [View all](#)

	Date	Org	Category	Type	Value	Tags	Galaxies	Comment	Correlate	Related Events	Feed hits
<input type="checkbox"/>	2021-02-28		Payload delivery	msb	e10713a4a59b35767a054a608be977	tlp:white			<input checked="" type="checkbox"/>	1209	
<input type="checkbox"/>	2021-02-28		Payload delivery	sha256	8203c200e0c3bae860a3247a7d7b635e5c38939607c05dbdbdc920495f	tlp:white			<input checked="" type="checkbox"/>	1209	
<input type="checkbox"/>	2021-02-28		External analysis	link	http://chuangdong.com/reverse%20engineering/2021/01/03/BabukRansomware/	tlp:white			<input checked="" type="checkbox"/>	1209	
<input type="checkbox"/>	2021-02-28		External analysis	link	https://twitter.com/Ak4ard_SOLO/status/13456689395726242373	tlp:white			<input checked="" type="checkbox"/>	1209	

[Previous](#) [Next](#) [View all](#)

Minimal subset of tags to use for each event

Traffic Light Protocol

TLP-Tags: TLP utilizes a simple four color schema for indicating how intelligence can be shared.

Confidence

Confidence-Tags/Vetting State: There are huge differences in the quality of data, whether it was vetted upon sharing. As this means that the author was confident that the shared data is or at least was a good indicator of compromise.

Origin

Origin-Tags: Describes where the information came from, whether it was in an automated fashion or in a manual investigation. This should give an impression how value this intelligence is, as manual investigation should supersede any automatic generation of data.

Permissible Actions Protocol

PAP-Tags: An even more advanced approach of data classification is using the Permissible Actions Protocol. It indicates how the received data can be used to search for compromises within the individual company or constituency.

Setting distribution

Similar to [tagging](#), inheritance should be used wherever possible. This is especially important when using [sharing groups](#) due to limit the impact of sharing group usage on performance. Note that for distribution, the event or object distribution of the attribute should be the same or less restrictive than the attribute distribution. Below are two good practice examples, the first using [community](#) distribution and the second using [sharing groups](#). Note that a combination of the two can be used as well.

Good practice distribution event

Event ID1279

UUID2ef08218-4c0a-4f43-a040-1c0e93aa949a

Creator orgSetec Astronomy

Owner orgSetec Astronomy

Creator useradmin@admin.test

Tags

Date2021-02-28

Threat LevelHigh

AnalysisInitial

DistributionThis community only

InfoGood practice distribution event

PublishedNo

#Attributes5 (0 Objects)

First recorded change2021-02-28 16:06:57

Last change2021-02-28 16:32:34

Modification map

Sightings0 (0) - restricted to own organisation only

Related Events

OSINT - Babuk Ransomware2021-01-054

PhotosGalaxyEvent graphEvent timelineCorrelation graphATT&CK matrixEvent reportsAttributesDiscussion

1279: Good p...

Galaxies

< previousnext >View all

Scope toggleDeletedDecay scoreSighting OGCContextRelated TagsFiltering tool

Enter value h

Date	Org	Category	Type	Value	Tags	Galaxies	Comment	Correlate	Related Events	Feed hits	IDS	Distribution
2021-02-28	Other	comment	Warninglist should be renamed to prevent-oppie-list		Up:red							Organisation
2021-02-28	External analysis	link	https://twitter.com/Arkibird_SOLO/status/134550839725242373						1209			Inherit
2021-02-28	External analysis	link	http://chuongdong.com/reverse%20engineering/2021/01/03/BabukRanso...means/						1209			Inherit
2021-02-28	Payload delivery	sha256	8203a2f0ce0d3ae900cb3247a7c7b635e55c38038007c855bdb5c6220495f						1209			Inherit

























482

Related Events

OSINT - Bobuk Ransomware
2021-01-05 4

✖ 1279: Good p...

« previous	next »	view all
----------------------------	------------------------	--------------------------

[Close] [X] [Search] [Add] [Edit] [Delete] [Duplicate] [Link] [Copy] [Paste] [Print] [Share] [More]													Enter value
ID	Date	Org	Category	Type	Value	Tags	Database	Comment	Complete	Related Events	Feed hits	ID's	Distribution
	2021-02-28		Object name: employee** Reference: 0										
<input type="checkbox"/>	2021-02-28		Targeting data	email-addr@161:	admin@admin.test target email	 	 		<input checked="" type="checkbox"/>			<input type="checkbox"/>	Inherit
<input type="checkbox"/>	2021-02-28		External analysis	link	https://twitter.com/Abdoul_S/status/134556639572524273	 	 		<input checked="" type="checkbox"/>		1209	<input type="checkbox"/>	Inherit
<input type="checkbox"/>	2021-02-28		External analysis	link	http://richungdong.com/research/02engineering/2021/01/03/8abaRandom.html	 	 		<input checked="" type="checkbox"/>		1209	<input type="checkbox"/>	Inherit
<input type="checkbox"/>	2021-02-28		Payload delivery	sha256	8203c2f50ec3d4ee60a3247c7b7835e5c3939607f6d6bdc5dc02459f8b	 	 		<input checked="" type="checkbox"/>		1209	<input type="checkbox"/>	Inherit
<input type="checkbox"/>	2021-02-28		Payload delivery	md5	e10713a8e8836781e0d546058e9b77	 	 		<input checked="" type="checkbox"/>		1209	<input type="checkbox"/>	Inherit
<input type="checkbox"/>	2021-02-28		Other	comment	Warninglist should be removed to prevent opaque list	 	 		<input checked="" type="checkbox"/>			<input type="checkbox"/>	Subnet_sharing_group
<div>« previous</div> <div>next »</div> <div>view all</div>													

In the next to screenshots, you can see the equivalent bad practice examples.

Bad practice distribution event example

Event ID 1279

L&ID JwKd0T9f-Akku-4H2J u6d0 f6e93ae8fHu [🔍]

Creator org [Sales Automation](#)

Owner org [Sales Automation](#)

Creator user admin@admin.test

Tags top white [👤] [📅] [🔗]

Date 2021-02-28

Threat Level 🔴 High

Analysis Initial

Distribution This community only [👤] [📅] [🔗]

Info Best practice distribution event example

Publisher No

Attachments 0 (1) Clients

First recorded change 2021-02-28 17:41:58

Last change 2021-02-28 17:42:51

Modification map [📍]

Highings 0 (0) restricted to own organisation only [🔒]

🔍 1279f test pr...

Galleries

[👤] [📅] [🔗]

< previous next > view all

🏠 Home → 🌐 Galaxy → 📅 Event graph → ⚙️ Event timeline → 📊 Correlation graph → 📈 ATT&M matrix → 📢 Event reports → 📎 Attachments → 🗄️ Discussion

												Enter via	
🏠 Home 🌐 Galaxy 📅 Event graph ⚙️ Event timeline 📊 Correlation graph 📈 ATT&M matrix 📢 Event reports 📎 Attachments 🗄️ Discussion													
☐	Date	Org	Category	Type	Value	Type	Galaxies	Comment	Correlate	Related Events	Feed title	👤	Distribution
<input type="checkbox"/>	2021-02-28		Payment delivery	nvd	c10713a4a8035767a0c54805bed377	[👤] [📅] [🔗]			<input checked="" type="checkbox"/>	1209		<input type="checkbox"/>	Community
<input type="checkbox"/>	2021-02-28		Payment delivery	stu256	(B03c2f0edcc3bae980cb3247a7eb7db35c6c53939607f05dbdcbb0c205495f a0)	[👤] [📅] [🔗]			<input checked="" type="checkbox"/>	1209		<input type="checkbox"/>	Community
<input type="checkbox"/>	2021-02-28		Other	comment	Warning! link should be renamed to prevent ospide fail	[👤] [📅] [🔗]			<input checked="" type="checkbox"/>			<input type="checkbox"/>	Organisation
<input type="checkbox"/>	2021-02-28		External analysis	link	http://chuangbang.com/research/Songheevoting20210163/Babuk-Ramadan-wani	[👤] [📅] [🔗]			<input checked="" type="checkbox"/>	1209		<input type="checkbox"/>	Community
<input type="checkbox"/>	2021-02-28		External analysis	link	https://twitter.com/fvksbfm_SQLGvnuhuq/1345689365720242373	[👤] [📅] [🔗]			<input checked="" type="checkbox"/>	1209		<input type="checkbox"/>	Community
2021-02-28 Object name: employee -- Subcategory: 0 Community													
<input type="checkbox"/>	2021-02-28		Targeting data	email-addr#989:	admin@admin.test target email	[👤] [📅] [🔗]			<input checked="" type="checkbox"/>			<input type="checkbox"/>	Community

Bad practice distribution event example - sharing group case

Event ID

1279

UUID

2ef02216-Acta-4163-a040-f4ed3a3a1b16 

Creator org

[Setec Automation](#)

Owner org

[Setec Automation](#)

Creator user

admin@admin.local

Tags


[tpc white](#)




Date

2021-02-28

Threat Level

 High

Analysts

Initial

Distribution

[big_sharing_group](#)



Info

Bad practice distribution event example - sharing group case

Published

No

Attributes

6 (1 Object)

First recorded change

2021-02-28 17:54:55

Last change

2021-02-28 18:01:16

Modification map






Signings


restricted to own organisation only


Related Events

OSINT - Babuk Ransomware
2021-01-05 4

[-Pivots](#) [-Galaxy](#) [+Event graph](#) [+Event timeline](#) [+Correlation graph](#) [+ATT&CK matrix](#) [+Event reports](#) [-Attributes](#) [-Discussion](#)

✖ 1270: Bad pr...

Galaxies

[« previous](#)
[next »](#)
[view all](#)

													Enter value
+	Info	Org	Type	Value	Tags	Galleries	Comment	Correlate	Related Events	Feed hits	📄	Distribution	
2021-02-28			Payload delivery	m5d e10713acba983c6763cfcd5f4609be5b77					1209			Big_sharing_group	
2021-02-28			Payload delivery	shwz56d 8205270dcdec3ae960a3247af7cb35ce5fc38939607f5dbdcb5e9204695ab					1209			Big_sharing_group	
2021-02-28			External analysis	link http://chugangbing.com/inverse%20gaining/20210103/BabaRandom.html					1209			Big_sharing_group	
2021-02-28			External analysis	link https://twitter.com/Arkadev_SOJ/Gist/uw134656989752543273					1209			Big_sharing_group	
2021-02-28			Object name: employee** References: C-0									Big_sharing_group	
2021-02-28			Targeting data	email-address: admin@admin.local target email								Big_sharing_group	
2021-02-28			Other	comment Warninglist should be renamed to prevent coexist-list								Subst_sharing_gmp	

« previous	next »	view all
----------------------------	------------------------	--------------------------

Use objects instead of combined attributes

Some attributes like filename|sha512 and ip-dst|port now have equivalent objects such as file and ip-port. Using the object equivalent of attributes is recommended. It gives flexibility to add more context later and groups all the relevant attributes related to one concept, for example a file, together.

Use proposals when possible to request author to make changes to an event

If possible, use [proposals](#) when you want to inform the original analyst/author (e.g. a security vendor or a CSIRT) about a specific mistake or error which needs to be corrected. The advantages of using the proposal system include the lack of a need to create a new event as well as the process itself being very simple and fast.

Last modified: Wed May 05 2021 11:17:55 GMT+0200 (Central European Summer Time)

MISP User Stories

User story	Example workflow
As a lead threat intelligence analyst, I want to lead a team focused on hunting down threats so that I can prevent attacks against ICT infrastructures and organizations	<ul style="list-style-type: none"> • Monitor what teams are up to in real-time using the Live Dashboard
As a threat analyst, I want to research, analyze and reverse engineer malware so that I can know how to counter it	<ul style="list-style-type: none"> • Attach and download files and malware samples from events • Search for hashes/IPs/domains/URLs from malware events, or add malware samples hashes to an event • Analyse observables and malware collected during an incident (e.g. domain name, IP addresses etc.) by checking whether observables are IoCs or false positives using 'correlation graph' and 'expansion modules'. • Enrich malware events by querying data sources external to MISP using modules • Perform dynamic malware analysis correlations • Submit events with malware samples to analysis tools (e.g VirusTotal, VMRay) for further analysis, and then extend MISP with malware analysis results
As a lead threat intelligence analyst, I want to convert threat data into actionable threat intelligence so that I can improve security posture.	<ul style="list-style-type: none"> • Import data from external sources • Add feeds • Contextualise events and attributes using tags, taxonomies and galaxies
As a threat analyst, I want to exchange threat information with third parties so that we can gain shared situational awareness	<ul style="list-style-type: none"> • Setup different models of distribution on MISP instance • Sync events and attributes between instances • Use filtering functionalities to meet an organisation's sharing policy • Share information, pentest information, malware samples, vulnerabilities internally and externally • Use feature/achievements widget adding gamification to the information sharing

User story	Example workflow
As a threat analyst, I want to monitor threats and access live data so that I can manage threats before they cause major damage	<ul style="list-style-type: none"> • Import lists of indicators and check if the IOCs are present in feeds. • Monitor statistics and sightings using widgets • Show live data and stats from one or more MISP instances via the Dashboard • Process information in real-time when it's updated, created, or published by instances by integrating with ZMQ • Use sightings to notify an instance about activities related to an indicator
As a threat analyst, I want to aggregate and compare indicators from various sources so that I can connect the dots between various threats	<ul style="list-style-type: none"> • Join communities and subscribe to the feeds • Add events and assign events to specific feeds • Correlate indicators using MISP's automated correlation engine • Use the overlap feed analysis available in MISP • Link events and attributes using the correlation graph • Analyse and gain more information on attributes using modules • Link events with malware, threat actors etc using galaxies (e.g ATT&CK)
As a threat analyst, I want to have a structured database of threat data that I can use to perform lookups/queries when investigating new threats	<ul style="list-style-type: none"> • Store information in a structured format using STIX • Import unstructured reports using the free-text import tool • Use MISP as a centralized hub for security and fraud threat intel. Centralize threat intel by aggregating indicators from OSINT and commercial feeds • Remove false positives and duplicates • Score indicators based on Sightings and other metrics • Import/integrate feeds or threat intelligence from third parties • Generate, select, exchange, and collect intelligence using feeds • Select and import events • Look for correlations between events using the correlation graph • Build filtered subsets of the data repository for feed creation. • Preview and correlate feed data directly for evaluation

User story	Example workflow
<p>As a threat analyst, I want to contextualize and enrich raw threat data so that I can produce actionable intelligence</p>	<ul style="list-style-type: none"> • Understand attacker TTPs by using taxonomies to link events • Categorize risks and incidents using galaxies and taxonomies • Quickly classify information using tags collections • Contextualise sightings with information on the source • Enrich IDSes export with tags to fit your NIDS deployment • Decay attributes and score indicators using sightings (reported by IDSes) • Describe and visualise complex scenarios using MISP's richer data structure • Allow advanced combination of attributes using MISP objects
<p>As a threat analyst, I want to investigate threats so that I can protect computer systems from attacks</p>	<ul style="list-style-type: none"> • Find relevant data for investigations from MISP communities. Preview new MISP events and alerts from multiple sources such as email reports, CTI providers, and SIEMs • Query a MISP instance for events that include a given IOC. Browse through other MISP events, attributes, objects, tags, and galaxies • Create events, add IoCs (attributes), and contextualise (using tags) • Pivot an event into its attributes, objects, tags, galaxies, and/or related Events • Explore further details from Galaxies and related Events • Categorize available related information within the ATT&CK framework. • Query tools (e.g Cytomic Orion API) to check if certain MISP indicators have been observed, and the import sighting details to add them to MISP events • Prioritize threats using Sightings collected from users, scripts and IDSes. • Decay/expire indicators using sightings reported by users, scripts and IDSes • Launch lookups from MISP against SIEMs as part of an investigation • Correlate network forensic flows from several tools

User story	Example workflow
<p>As a SOC team, we want to ingest, analyse, store and make connections between threat data so as to discover potential threats</p>	<ul style="list-style-type: none"> • See connections between events using the correlations graph • Import CVEs and vulnerabilities (e.g from MetaSploit) and contextualise them • Contextualise CVEs using events gotten from articles/reports • Convert CVE information into a feed • Pull shared CVE feeds • Combine collected data with your MISP data set for correlation • Share correlated info to the team using the export function or API search • View current threats and activity, historical, geolocalized information using MISP Dashboard
<p>As a junior SOC analyst, I want to enrich alerts so that I can "punch above my weight" and make connections that would have otherwise required more experience</p>	<ul style="list-style-type: none"> • Create events, add/import observables • Use Cortex and its analyzers to gain insight • Leverage tags, sightings, and previously-seen observables to feed your threat intelligence • Export IOCs to MISP instances after investigations are complete • Integrate MISP with Maltego to generate visualisations of data • Integrate MISP with Elastic to access threat data without the complexities of the MISP interface. • Push attributes from MISP to Elastic and have a representation with graphs, an alternative to using MISP Dashboard. • Create taxonomies using the taxonomy editor. • Contextualise data using taxonomies, clusters and galaxies

User story	Example workflow
As a SOC analyst, I want to customize risk feeds to ignore or downgrade alerts that do not match organization/ industry-specific criteria, so that I can focus on relevant alerts	<ul style="list-style-type: none"> • Filter incidents based on taxonomies (e.g the veris country taxonomy to indicate countries affected by an incident) • Normalise external input and feeds in MISP (e.g. feed importer). • Compare feeds before import to find similarities and false positives. • Evaluate the quality of the information before importing it (warning-list lookups at feed evaluation)
As a SOC analyst, I want to share real-time information pertaining to new or existing cases/observables to team members so that we can collaborate on investigations simultaneously	<ul style="list-style-type: none"> • Control threat sharing using 'distribution settings': sharing group, community-only, connected communities, all communities. • Share sensitive and confidential events using the 'sharing group' functionality • Measure the impact of an incident using taxonomies based on NISD/OESS impact criteria • Export and share sightings in ATT&CK sightings format to give insights on TTPs and frequency of usage
As a SOC analyst, I want to rule out false positives so that I can focus on significant threats	<ul style="list-style-type: none"> • Weed out false positives using warning lists • Crowd source data validation from community • Filter indicators based on specific criteria • Receive information on false positives using collaborative tools (proposals, sightings)

User story	Example workflow
As a threat analyst, I want to remove false positives, filter and prioritize alerts so that I can focus on what really matters to my organization	<ul style="list-style-type: none"> • Evaluate the quality and freshness of indicators using decaying models • Enforce warninglists to exclude events with certain attributes • Enable warninglists to alert for certain issues • Classify information (add/remove tags) based on their score or visibility via sightings • Use tags to set events or attributes for further processing by external tools (e.g. VirusTotal auto-expansion using Viper) • Notify an instance about activities related to an indicator via Sighting • Limit NIDS exports and improve rules using Sightings • Filter indicators based on specific criteria • Filter out relevant data when feeding protective tools
As a security analyst, I want to unravel the inner workings of a malicious file, phishing email or domain so that I can prevent attacks	<ul style="list-style-type: none"> • Integrate MISP with a Security Incident Response Platform (e.g TheHive) • Import indicators from MISP into the SIRP for further analysis
As a security analyst, I want to create blacklists/whitelists (e.g of domains) so that I can protect customers from malicious activity	<ul style="list-style-type: none"> • Import threat data into MISP from synced servers and label using taxonomies • Enable warning lists, and exclude attributes that exist on the warning lists • Create lists with preferred attributes and export the list in an easy accessible format as CSV
As a security analyst, I need a real-time overview of threat information so that I can quickly glance at important metrics	<ul style="list-style-type: none"> • Integrate ZMQ to access a dashboard showing live data and stats • Monitor ongoing trends based on interests using the EventStream widget • Monitor activity in real-time on MISP dashboard by subscribing to ZMQ feeds • View immediate contributions made by organisations from MISP's live dashboard • Find threats within your constituency using MISP Geolocalisation Dashboard • Get geospatial threat information from specific regions using the Geolocalisation Dashboard

User story	Example workflow
As a security analyst, I want to automate repetitive tasks related to data normalization, importation, aggregation and enrichment so that I can have more time to put into threat analysis efforts	<ul style="list-style-type: none"> • Automate tasks using PyMISP • Use PyMISP for Scripted processing of events and attributes
As a security analyst, I want to collaborate with other analysts within and out of my organization's sector so that we can support one another	<ul style="list-style-type: none"> • Build or join communities to exchange specific data structures • Share real-time analysis of an incident • Propose modifications to someone else's analysis using Proposals
As a security analyst, I want to triage and prioritize alerts so as to avoid alert fatigue	<ul style="list-style-type: none"> • Evaluate the quality and freshness of indicators using decaying models • Weed out false positives using warning lists • Enable warning lists to alert for critical issues • Filter indicators based on specific criteria • Score indicators based on user sightings, including negative sightings and expiration sightings. • Classify information (add/remove tags) based on their score or visibility via sightings
As an incident responder, I want to get an up-to-date picture of the threat landscape so that I can prepare for threats in advance	<ul style="list-style-type: none"> • Describe the impact of threat using taxonomies (e.g using the veris timeline taxonomy to indicate the duration of the incident) • Classify data to gain insight into the threat landscape. • Classify data so IDSes can alert on a rule • Integrate ZMQ to have a dashboard showing live data and statistics. • Integrate ZMQ to process information in real-time when it's updated, created, or gathered in MISP.
As an incident responder, I want to identify and respond to incidents so that I can reduce the impact and severity of an attack	<ul style="list-style-type: none"> • Report false or true positives using the sighting mechanism, based on an incident investigation • Decay indicators to guarantee the quality of the indicators

User story	Example workflow
<p>As an incident responder, I want to receive early warnings and alerts about threats/incidents so that I can retaliate before they cause any harm</p>	<ul style="list-style-type: none"> • Receive correlated threat intel from sharing groups and communities • Monitor MISP feeds for alerts • Preview new events and alerts from multiple sources • Automate import/export of IoCs to/from protective or detection tools like IDSeS and IPSeS • Dispatch notifications when certain events are created or modified using the alert feature • Create filter rules based on personalised uses. Restrict alert messaged by tags, publishing organisation or other metrics
<p>As an incident responder, I want to store information identified during an incident investigation so that I can perform lookups/queries against the historical database during future incidents</p>	<ul style="list-style-type: none"> • Use a MISP instance as a database of events representing incidents. Store incident response data internally in a structured manner on MISP • Represent indicators using attributes. Attributes such as network indicators (e.g. IP address) or system indicators (e.g. a string in memory) • Combine OSINT and your own intelligence • Create events made up of indicators (attributes) and then leverage these as a threat data feed • Modify events representing incidents to enable monitoring over time • Add object types to describe incidents • Monitor indicators for relevancy using Sightings • Ensure information quality and freshness by expiring indicators depending on their personalised objectives • Pull events from indicator lists to perform lookups against SIEMs • Use indicators to check logs and verify if you're affected by a threat • Correlate indicators with actual incidents to get more information • Integrate MISP with IR tools (e.g TheHive) to (1) analyse observables during an incident, (2) import and (3) export events from MISP to TheHive and vice-versa • Perform large-scale bulk data/traffic analysis and correlation against your MISP database using SightingsDB

User story	Example workflow
<p>As an incident responder, I want to export and feed data between security tools so that I can enhance their functionalities</p>	<ul style="list-style-type: none"> • Export data from MISP to feed protective/detective tools and early warning systems. Export formats support IDSes / IPSes (e.g. Suricata, Bro, Snort), SIEMs (eg CEF), Host scanners (e.g. OpenIOC, STIX, CSV, yara), analysis tools (e.g. Maltego), DNS policies (e.g. RPZ) • Feed MISP using automatic tools (e.g. Sandbox Analysis, low-value information needing correlation, Analyst workbench) • Pull events from feeds or indicator lists to perform lookups against SIEMs • Subscribe to ZMQ pub-sub to get published events for use in lookup processes • Match attributes against SIEMs using the lookup expansion module • Import activities from a SIEM (e.g. Splunk lookup validation or false-positive feedback), NIDS or honeypot devices • Post Sightings from IDSes, IPSes, SIEMs back to MISP • Use sightings to improve NIDS rule-sets • Generate IDS and NIDS rules automatically or manually using IoCs • Feed data to honeypots to generate blocklists and DNS RPZ zones • Consume correlated results in SIEMs using the API • Search indicators in real-time into a SIEM using MISP ZMQ • Submit large sets of IoCs from MISP into SIEMs using PyMISP • Import indicators into MISP from other tools (SIEMs, IDSes) and be notified when those indicators appear again
<p>As a CSIRT, we want to exchange and discuss information related to incidents and associated risks so that we can collaboratively respond to incidents</p>	<ul style="list-style-type: none"> • Build communities to exchange specific data structures • Discuss non-event related topics in Forums • Add comments to events (which may represent an incident) • Contact a reporter (e.g. another CSIRT) via email (encrypted, anonymously or not) to discuss commercially-sensitive information related to an incident

User story	Example workflow
As a CSIRT, we want to interact with threat data in various ways during the threat investigation and incident response process	<ul style="list-style-type: none"> • View events, indicators and feeds • Search and filter the data set • Classify, contextualize and correlate data • Download the viewed data in various formats • Interact with MISP data using other tools in the MISP ecosystem (e.g MISP Workbench, Viper, MISPEgo)
As a CSIRT, we want to coordinate with team members and other organisations so that we can avoid duplication of work	<ul style="list-style-type: none"> • Create and manage sharing groups between sectors • Join existing communities or sharing groups • Create and exchange events and indicators • Propose changes to existing analysis or reports • Enhance an analysis with additional information using Extended Events • Report sightings as false-positive or true-positive (e.g. a partner/analyst has seen a similar indicator) • Contribute to threat intel feeds and analyse overlapping data
As a CSIRT, we want to share incident information and discuss risks with other team members so that we can collaboratively perform incident analysis	<ul style="list-style-type: none"> • Create, modify, delete and exchange events and indicators • Modify distribution settings to exchange individual incidents and ensure confidentiality • Use taxonomies and galaxies to classify data before exchange (e.g Indicate the confidentiality of incidents using the NATO classification, indicate the risk of an incident using the threat-level taxonomy) • Edit, visualize, and share reports using Event Report • Incorporate reports from information sources using the Event Report module • Share indicators derived during incident response • Correlate and enrich data derived during incidents • Coordinate with affected parties during incident response using MISP's collaborative tools (proposals, sightings, emails)

User story	Example workflow
As a fraud analyst, I want to investigate financial threats so that I can help financial institutions and consumers prevent financial fraud	<ul style="list-style-type: none"> • Join communities and receive shared IOCs • Subscribe to feeds and get IOCs in an easily accessible format • Access lists and public feeds of malicious domains (e.g phishing sites) and threats • Use indicators to check logs and verify if you're affected by a threat • Gather information related to a phishing site and create events • Integrate MISP with Maltego to visualise the full ATT&CK framework
As a fraud analyst, I want to blend updated threat intel with anti-fraud tools so that I can prevent fraud in real-time	<ul style="list-style-type: none"> • Feed data from MISP to fraud prevention tools • Report sightings to MISP from fraud prevention tools
As a fraud analyst, I want to collaborate with analysts from other institutions so that we can gain shared situational awareness	<ul style="list-style-type: none"> • Implement a MISP instance, and join relevant communities • Publish fraud perpetrators for others to see • Exchange events containing fraud information (e.g a bank account number) • Use shared fraud data to feed firewalls and blocklists • Warn of false positives by alerting for invalid financial indicators • Give more credibility to indicators by reacting to event attributes (Sightings) • Get feedback from the community on the quality of indicators (Sightings)
As a customs and border control agent, I want to facilitate the flow of legal immigration and goods while preventing the illegal trafficking of people and contraband so that I can ensure homeland security	<ul style="list-style-type: none"> • Create or join sharing groups and communities • Share information (e.g travel documents / biometric information) between border control agencies using MISP • Categorize data using predefined types such PNR (passenger name records) • Share information / involve experts for the identification of smuggled goods • Perform anonymised lookups against exported data sets information (e.g. offline border control check)

User story	Example workflow
As a law enforcement officer, I want to investigate digital crimes and threats so that I can apprehend criminals	<ul style="list-style-type: none"> • Access information sharing communities • Get indicators and actionable information from CSIRTs/CERTs networks or researchers • Exchange information with other officers via sharing communities • Exchange and store incident information on MISP, enabling the system to act as a forensic tool over time
As a law enforcement officer, I want to collect and verify evidence of digital crimes so that I can bootstrap my DFIR cases	<ul style="list-style-type: none"> • Collect indicators from shared events • Propose changes to existing analysis or reports • Enhance existing events with additional pieces of evidence using Extended Events • Exchange analysis and reports of digital forensic evidence • Correlate indicators corresponding to forensic pieces of evidence • Import Mactime timelines to describe forensic activities on an analysed file system • Describe forensic analysis cases using objects templates • Create, modify and visualise the timeline of events • Share analysis and reports of digital forensic evidence • Report sightings such as false-positive or true-positive (e.g. a partner/analyst has seen a similar indicator)

User story	Example workflow
As a cybersecurity consultant, I want to provide structured threat intelligence to cross-sector partners with diverse requirements so that I can secure their infrastructure	<ul style="list-style-type: none"> • Implement an instance and join relevant communities • Integrate MISP with an organisation's existing solutions using the API • Exchange events containing indicators • Setup distribution levels to ensure confidentiality during threat sharing • Sync between untrusted and trusted networks using Feed support • Notify the community about activities related to an indicator using Sightings • Score indicators based on user sightings, including negative sightings and expiration sightings • Propose updates to an event owner or indicate a sighting • Share attacker techniques via integration with ATT&CK • Set an attribute for detection tools using the IDS flag
As a cybersecurity specialist, I want to anonymously publish threat intel so that I can protect the identity of people who don't want to be associated with the information	<ul style="list-style-type: none"> • Pseudo-anonymously publish data using Event Delegation
As a cybersecurity specialist, I want to investigate threats so that I can remediate and prevent cyber attacks	<ul style="list-style-type: none"> • Query an instance for events that include a given IOC • Explore more details from Galaxies and related events • Categorize related information within the MITRE ATT&CK framework
As a security analyst, I want to access threat data so that I can use it to support my research	<ul style="list-style-type: none"> • Contextualise indicators (attributes) using categories, taxonomies and galaxies • Reinforce an analysis using correlation features (e.g. do other analysts have the same hypothesis?) • Confirm a specific aspect using correlation features (e.g. are the sinkhole IP addresses used for one campaign?) • Verify if a threat is new or unknown in your community using correlation features

User story	Example workflow
As a security analyst, I want to access updated threat data so that I can build protection in real time	<ul style="list-style-type: none"> • Monitor feeds for recent indicators • Monitor activity in real-time on MISP dashboard by subscribing to ZMQ feeds • Process information in real-time when it's updated, created or gathered using ZMQ
As a risk analyst, I want to identify and predict risks to my organization so that I can improve the organization's security posture and situational awareness	<ul style="list-style-type: none"> • Use a MISP instance as a database of events representing threats • Classify risks using taxonomies and galaxies • Generate statistics from your MISP instance to deduce from incidents the current operational status, risk posture, and threats to the cyber environment • Monitor trends and adversary TTPs using MISP-dashboard and built-in statistics
As a risk analyst, I want to present risk data to stakeholders in various formats (depending on their technical ability), so that I can justify the need for risk-mitigating strategies	<ul style="list-style-type: none"> • Show trends within the sector/geographical region using MISP dashboard and built-in statistics • Turn MISP data into explorable graphs or timelines representing their activity or events • Export data from MISP in various formats • Share reports along with actionable data using Events Report
As a disinformation researcher, I want to identify indicators associated with a specific operation or campaign so that I can help track and mitigate threats	<ul style="list-style-type: none"> • Monitor MISP feeds for indicators • Find relationships between indicators using correlation

User story	Example workflow
<p>As a disinformation researcher and journalist, I want to investigate information campaigns so that I can report whether there is or isn't disinformation or misinformation</p>	<ul style="list-style-type: none"> • Compare external feeds information with already-available information • Analyze the connections between incident objects • Map data with AMITT (embedded in MISP) to understand threat actor capabilities • Generate events that can be shared directly, via email or MISP • Add object types (e.g for common social media platforms), relationship types (to make the graphs that users can traverse in MISP richer) and taxonomies (e.g DFRLab's Dichotomies of Disinformation, and a NATO-led tactical variant) to describe indicators and events • Generate and share information operations data in MISP JSON or STIX format for easy sharing • Classify events with AMITT techniques using the inline AMITT Navigator • Describe attack patterns using AMITT for the attack patterns • Track disinformation techniques using the AMITT galaxy • Integrate MISP with TheHive for case tracking • Describe additional disinformation cases using object templates
<p>As a disinformation researcher, I want to connect with other researchers and responders so that we can collaboratively verify if an article/video/image contains disinformation and verify that a source (publisher, domain, etc) doesn't distribute disinformation</p>	<ul style="list-style-type: none"> • Join a disinformation community • Notify the community about activities related to an indicator • Score indicators based on users sighting • Corroborate a finding using correlation features (e.g. is this the same campaign?)

User story	Example workflow
As a disinformation researcher, I want to collaborate with other researchers and responders so that we can collectively stop disinformation campaigns	<ul style="list-style-type: none"> • Browse and Join disinformation communities (e.g CogSec Collab MISP) • Contextualise data using tags, taxonomies and galaxies • Describe information campaigns indicators and events using taxonomies (e.g DFRLab Dichotomies of Disinformation) • Find relationships between indicators using correlation • Describe misinformation tactics/techniques using the AM!TT framework (galaxy) • Include relevant techniques found in a report or sighting in misinformation event data using AM!TT Navigator
As a data scientist, I want to automate tasks related to data collection, curation, analysis, and visualization so that I can reduce security analysts' workloads	<ul style="list-style-type: none"> • Collect, add, update, search events/attributes/tags using PyMISP • Study malware samples using PyMISP • Write scripts to import (from other tools such as VirusTotal) additional attributes or IOC data (such as hashes) to build up knowledge on an event • Automatically handle indicators in third-party tools using PyMISP • Integrate MISP with existing infrastructure using PyMISP • Automate the dissemination of threat intelligence and threat data using the API • Generate exports to be ingested into other platforms • Create a range of filtered subsets of the dataset for various protective measures • Write scripts to disable the IDS flag based on the number of false-positive reported sightings, in order to prevent using false-positive indicators for detection or correlation actions • Generate data statistics and send reports via email, attached as CSV files using the API • Feed processed data into IDSes and 3rd party visualization using PyMISP • Build custom widgets to visualise/track data via the Dashboard • Extend MISP with Python scripts using MISP modules • Auto-discover new modules with their features using the API

User story	Example workflow
As a data scientist, I want to collect and analyze data from various sources so that I can prioritize and predict risk	<ul style="list-style-type: none">• Aggregate indicators and sightings of all attributes/objects, useful for detecting particular security events or threats• Use PyMISP for Scripted processing of events and attributes• Collect data from open data portals using the API• Publish open data and create data sets• Investigate file hashes, malicious website URLs, IP Addresses and domain names using shared indicators• Aggregate data sets for security research and threat analysis• Analyse and select threat feeds for incorporation into other tools to hunt known indicators• Indicate if an attribute should be used for detection or correlation actions using the IDS flag• Download data in various formats for ingestion in other tools, and for training ML models

Last modified: Sun Mar 28 2021 11:44:26 GMT+0200 (Central European Summer Time)

MISP user personas

These personas are fictitious but are concrete representations of the people using MISP. We can use these personas to keep in mind who we are working for, what are their needs, and what MISP should do for them. These personas come from [OSINT](#) on current MISP users (Gitter chats, GitHub issues, LinkedIn) and other sources of information about cybersecurity.

Primary personas

Farrah and Adam represent the users that are the most important to us.

Farrah

The Threat Hunter

Farrah works as a threat intelligence for a security service provider in Malaysia that offers a range of cybersecurity solutions. He leads a threat intelligence team made up of experienced intelligence analysts who are former military/government employees and contractors.

Farrah uses MISP to analyze malware, gather information about specific adversary groups, and discover emerging threats. He also uses MISP for data normalization (consolidating data across different source formats), de-duplication (removal of duplicate information), and enrichment (removal of false positives, scoring of [indicators](#), and the addition of context).

"In order to effectively address threats, you must maintain a team focused on monitoring, generating and triaging alerts"

Role

Lead Threat Intelligence Analyst

His primary goals are to:

- Hunt down threats, analyze malware, manage vulnerabilities and prevent attacks against ICT infrastructures, organizations, or people.
- Improve security posture through the aggregation, correlation, and analysis of threat data from multiple sources
- Investigate and understand adversarial capabilities, infrastructure & TTPs.
- Turn threat data from various sources into actionable threat intelligence.

He uses MISP to:

- Dispatch notifications containing IoCs to various parties via `mail_to_misp`.

- Monitor feeds for [indicators](#) and correlate attributes and analyze malware (check ransom notes, look for any [indicators](#), check the origin, etc).
- Store attack info in a structured format and allow for automated use of the database for various purposes using the [API](#).
- Prioritize [indicators](#) using sighting reports and purge false positives using warning lists.
- Classify and contextualize data using taxonomies and galaxies, and keep track of the advancement of an analysis using tags.
- View and visualize events and activities using MISP-dashboard or Maltego.
- Automatically import, aggregate, compare, contextualize, query, and cross-reference data using PyMISP
- Import, export and enrich data using [MISP modules](#)
- Aggregate, curate, and validate [indicators](#) from various feeds, then feed the data into detection and analysis tools like [NIDs](#), IDS, and SIEMs
- Query vulnerability scan results in MISP, automatically create/classify events on matching results, then create blocklists by excluding attributes that exist on warning lists.
- Collaborate with others in a sharing [community](#) using [Proposals](#) (send and receive feedback), Extended Events (add additional information to other's analytics), and Event Reports (supply resolution steps and recommendations).
- Share and receive reports of a specific threat, false positives, or post-mortem analysis of an incident from [sharing groups](#).

His objectives are to:

- Join relevant sharing communities, produce and publish [indicators](#) and share information across sectors to avoid hybrid threats.
- Use IoCs from feeds to identify vulnerabilities, compromised assets, data leaks and to verify the results of a malware scan.
- Triage threat intel, prioritize vulnerabilities, and customize risk feeds to ignore or downgrade irrelevant alerts in order to avoid alert fatigue.
- Generate and share alerts to provide critical information to internal teams and external peers.
- Share information about relevant vulnerabilities, coordinate with security vendors to get notifications, and [community](#) sharing of pentest results with other analysts.
- Research the evolution of high-risk malware families, validate malware signatures and domain reputations.
- Use [indicators](#) to query security logs/systems and databases, identify compromised systems, and add/modify signatures (used by firewalls, intrusion detection systems, etc), and block or alert on activity matching the [indicators](#).
- Correlate shared [indicators](#) from feeds with those captured by other security and network tools to produce intelligence placed in the context of wider threat landscapes.
- Integrate with existing security solutions so as to centralize security in one place. Leverage integrations to alert on information leaks (AIL 2), hunt down threats (McAfee OpenDXL), share attacker's techniques (ATT&CK), query

and prioritize [indicators](#) (MVISION EDR), speed up investigations (Cytomic Orion), and enhance the power of threat data (Carbon Black).

Adam

The Remediator

Adam is part of the Computer Security Incident Response Team (CSIRT) at a Belgian cybersecurity consulting firm. His responsibilities involve incident response, incident coordination, threat intelligence, and vulnerability management. He monitors potential threats, investigates attacks, and works with other security personnel to reduce the impact and severity of an attack.

Adam uses MISP to monitor incidents, provide early warnings/alerts about incidents, respond to incidents and provide incident analysis and situational awareness.

"A breach alone is not a disaster, but mishandling it is. The goal is to handle the situation in a way that limits damage and reduces recovery and time costs"

Role

Incident Response

His primary goals are to:

- Uncover the effects of attacks, determine how to clean up its impact, and inform a response to an existing incident to mitigate its extent or impacts.
- Develop and maintain strong processes for the most common incidents and threats, and create actionable results and remediation plans for internal stakeholders to proactively improve the security posture and maturity.
- Accelerate incident investigations, management, and prioritization by looking for information on the who/what/why/when/how of an incident.
- Determine the scope of incidents and limit the potential damage.

He uses MISP to:

- Store incidents as a database of events, describe incidents through event classification (using taxonomies and galaxies) and use the [API](#) to deduce from all incidents the current operational status, risk posture, and threats to the cyber environment.
- Join [sharing groups](#) and communities to share incident information with others and discuss information related to risks associated with incidents via Forums, comments to events, and contact a reporter.
- Analyze observables/malware collected during an incident, determining whether they are IoCs or false positives using the correlation graph and expansion modules.
- Alert and send emails when events are created in the system or major changes occur in the events, serving as part of an early warning system.
- [Pull](#) events via the [API](#) or export IOCs in formats for easy ingestion into other tools (such as SIEMs and IDS) and carrying out investigations by launching

lookups against databases.

- Collaborate and get feedback from team members and affected parties during incident response using [Proposals](#).
- Dismiss false positives (using warning lists) and enable alert prioritization.
- Aggregate and compare information from internal and external feeds to identify genuine threats.
- Perform large-scale data/traffic analysis and correlation through lookups against SightingDB.
- Share, receive, store and forward incidents and information identified during an incident investigation, enabling the MISP system to act as a forensic tool over time.
- Correlate and reference network forensic flows from different tools or network equipment
- Speed up incident response via integration with TheHive.

His objectives are to:

- Share information and get critical alerts and relevant actionable information in the event of a crisis situation.
- Support forensic analysts and collaborate with law enforcement.
- Improve incident response functionality and increase coverage and detection through integrations with tools like SIEMs.
- Use threat data to validate alarms/events and decide which to escalate to the rest of the incident response team for remediation.
- Aggregate information from various sources and correlating in order to understand how this data fits together in the broad threat landscape.
- Get insights (e.g using data feeds) into attacks, thereby helping incident response teams understand the nature, intent, and timing of specific attacks.
- Prioritize incidents based on risk and impact to the organization and filter out false alerts.

Secondary personas

Tina, Henry, Jacob, and Sarah represent other users that are also important to us.

Tina

The Fraud Catcher

Tina works as a fraud analyst at a National bank in Canada. She is responsible for investigating any forgery or theft within customers' accounts and transactions on behalf of the bank.

Tina uses MISP to find and share financial [indicators](#) in order to detect financial frauds.

"Fighting fraud with threat intelligence is all about alerting"

Role

Fraud analyst

Her primary goals are to:

- Identify and trace fraudulent activity.
- Create models for analyzing and determining financial fraud in order to protect consumers and stakeholders.
- Assess and analyze the attack surface, conduct threat modeling, and deliver actionable intelligence with a focus on current and emerging cyber-attacks against financial sector assets.

She uses MISP to:

- Map legacy and internal systems/models using [MISP objects](#).
- Find IoCs, malware, vulnerabilities, financial threat, fraud information and share data between other banks and financial institutions using [sharing groups](#).
- Create, modify and visualize the timeline of events, use MISP Dashboard to provide real-time information showing current threats and activity.
- Minimize false positives during the fraud vetting process using warning lists and sightings.
- Detect fraud using threat intel such as real-time notifications for stolen credit cards and phishing URLs from [MISP feeds](#).
- Prevent fraud by integrating MISP with a network of crawlers, honeypots, and other techniques that can cross-reference [indicators](#) against feeds, enabling the bank to intercept cards before they are sold on the black market and therefore reduce this risk of fraud.
- Monitor feeds for specific [indicators](#) (e.g. email header content, attachments, embedded URLs) related to phishing and fraud attacks.
- Block wire transfers to money mule accounts by integrating MISP warning lists and sightings with blocking systems.
- Aggregate sightings of attributes/objects so as to detect particular security events or threats.

Her objectives are to:

- Investigate financial [indicators](#) and handle false positives in order to detect and alert for certain potentially invalid data points.
- Aggregate, correlate, and analyze financial [indicators](#) from multiple feeds to discover any fraudulent activity.
- Blend threat intel from MISP with anti-fraud tools to identify and prevent fraud in real-time.
- Use threat intel to produce awareness reports informing the institution of threats in the financial sector, and then develop proactive defense strategies against fraud activity.
- Engage with sharing communities that allow individual enterprises to receive and share data so they can protect themselves before they are compromised.

Henry

The Enforcer

Henry is a law enforcement officer living in Florida, USA. He works with the Digital Forensics and Incident Response (DFIR) team. He is responsible for investigating digital security incidents, identifying digital assets targeted during attacks, and documenting all findings.

He uses MISP to support or bootstrap his DFIR cases.

"I worry about what I don't know, not what I know"

Role

Law Enforcement Officer

His primary goals are to:

- Find, gather and analyze digital evidence for criminal investigations.
- Carry out data breach and malware investigations.

He uses MISP to:

- Propose changes to existing analyses or reports.
- Correlate (1-to-1 value matches, fuzzy hashing, CIDR block matching) evidence against external/local attributes.
- Correlate and reference network forensic flows from different tools or network equipment using the [community-id](#) feature.
- Export data in various formats to feed into and lookup in other security tools.
- Join [sharing groups](#) and collaborate with other investigators.
- Receive, gather, analyze and share intelligence on digital crimes.
- Report digital evidence (in STIX) in a structured way for forensic use.
- Collect evidence for forensic analysis from feeds, using shared [indicators](#) to carry out cybercriminal behavior investigations, attribution, and identifying the link to organized crime activities.
- Exchange, store and forward incidents/information identified during an incident investigation, enabling the MISP system to act as a forensic tool over time.

His objectives are to:

- Share [indicators](#), analyses, and reports of forensic evidence among other law enforcement officers within and out of his team.
- Collaborate with CSIRT/CERTs and security researchers in the investigation of cyberattacks.
- Correlate data identified in a recent incident with data from previous investigations or external feeds.
- Bridge their use-cases with MISP's information-sharing mechanism.

Jacob

The Veteran

Jacob is a cybersecurity consultant for organizations looking to secure their infrastructure. He has founded a cybersecurity agency that provides threat intel and security consulting services to small and medium-sized businesses.

Jacob uses MISP to investigate threats and find IOCs. He works with many clients and typically wants to integrate MISP into existing client solutions.

"There's a difference between threat data and threat intelligence"

Role

Cyber Security consultant

His primary goals are to:

- Produce intelligence that will be embedded into organizational workflows and would serve decision-makers.
- Scope and implement custom security solutions across a variety of client software, architectures, and tools.
- Detect, contain, and remediate cybersecurity incidents, manually or programmatically.

He uses MISP to:

- Create, collaborate, automate and share threat intel using flexible [sharing groups](#), automatic correlation, free-text import helper, event distribution, and [proposals](#).
- Allow users to notify a [MISP instance](#) about activities (gotten from SIEMs, [NIDS](#), honeypot devices, etc) related to an indicator using sightings.
- Monitor feeds delivered through a REST [API](#) and correlate IOCs with firewall and other logs to identify potential threats in the organization.
- [Push/pull](#) events between local and client MISP instances in order to exchange intel internally and externally.
- Import, export, and enrich data using modules, automate such tasks using PyMISP.
- Create sub-communities and MISP object templates to allow rapid sharing of information using specific data models with existing communities.
- Validate data and flag false positives using warning lists and sightings.
- View live data/statistics and process information in real-time through integration with ZMQ to access MISP-dashboard.
- Pseudo-anonymously publish data using the MISP delegation system.
- Contextualize shared information within MISP instances and communities (using taxonomies and tags), and attach more complex structures to data (using MITRE ATT&CK and other galaxies)

His objectives are to:

- Run a Cyber Threat Intel platform using MISP integrated with existing client solutions (such as Active Directory, Splunk ES, ThreatConnect, Recorded Future, and CrowdStrike).

- Gather unstructured data from various sources and connect the dots to provide context on IoCs and TTPs of threat actors.
- Identify incoming threats, triage and prioritize alerts as they emerge.
- Feed SIEMs from MISP and feed MISP from other sources (SIEMs included).
- Share incidents and IOCs for detection (checking if IoCs are present in client infrastructure), blocking (using attributes to block, sinkhole, or divert the traffic), and intelligence (gathering information about campaigns and attacks) purposes.

Jay

The Inquisitor

Jay is a risk analyst for a large technology company in the USA. He is responsible for identifying and predicting risks, as well as forecasting the cost of certain attacks to the organization.

Jay uses MISP data to learn about the broad threat landscape and analyze the likelihood of certain risks, so as to gain situational awareness.

"The more certain you can be about the probability of a specific exploit impacting your environment, the easier it is to manage risk"

Role

Risk analyst

His primary goals are to:

- Improve the organization's security posture, situational awareness, and resilience.
- Forecast evolving threats before they materialize, provide detailed insights into which vulnerabilities pose the greatest risk, and plan accordingly to avoid them.
- Assess business and technical risks, identify the right strategies and technologies to mitigate the risks, communicate the nature of the risks to top management and justify investments in defensive measures.

He uses MISP to:

- Monitor trends and adversary TTPs within the company's sector/geographical region, share and track information emerging on a particular topic from the MISP dashboard in order to gain situational awareness.
- Monitor IoCs from various technical feeds and add additional context to internal sources of data using the automatic correlation engine.
- Access risk scores using correlation and sightings.
- Present data using different export formats, event reports, and the MISP dashboard timeline.

His objectives are to:

- Use shared [indicators](#) to perform a risk assessment, identify key information/assets and illustrate the intent/capability of actors to target these assets through impact assessments.
- Score threats according to the organization's specific needs and prepare processes in advance based on threat data gathered from feeds
- Present data to stakeholders in various formats – articles, timelines, graphs, raw data – depending on their technical knowledge.
- Gain shared situational awareness through information sharing and collaboration with other experts in the same sector.

Sarah

The Fact Checker

Sarah is a disinformation researcher and journalist working for a large American newspaper. She works with security researchers around the world to investigate cybercrimes and report disinformation. In the past, she has written about national security and geopolitics. She is used to making decisions on what should or shouldn't be published or shared.

Sarah uses MISP to collaborate with security researchers and investigate disinformation as it happens.

"Decisions as to what is or isn't published or shared go far beyond what is technically interesting"

Role

Disinformation researcher and journalist

Her primary goals are to:

- Conduct research and write intelligence reports about up-and-coming emerging threats and recent breaches.
- Investigate and report disinformation as it happens.
- Convert technical data into articles and reports that non-technical people can understand.

She uses MISP to:

- Write/read event reports, create misinformation events using relevant techniques found in a report or sighting.
- Join [sharing groups](#) and communities (e.g [Cogsec Collab](#)) that connect misinformation researchers and responders, share incident data with organizations focusing on response and counter-campaigns.
- Integrate with the AM!TT Framework (as a galaxy) in order to describe misinformation tactics/techniques, break an incident into techniques that can be analyzed/countered, and check for disinformation through mapping.
- Monitor feeds, investigate disinformation using shared [indicators](#) in feeds, generate structured intelligence using the automated correlation engine, and decide if there are any falsehoods in data.

- Enrich threat data by adding object types, new relationship types (to make the graphs that users can traverse in MISP richer), and taxonomies to cover things like types of threat actors.
- Classify events, [indicators](#), and threats using taxonomies (such as the Admiralty Scale taxonomy), which ranks the reliability of a source and the credibility of the information.

Her objectives are to:

- Distill essential information from a large piece of data, making it clear to the reader what really matters.
- Integrate MISP with TheHive for enhanced disinformation investigation and reporting.
- Verify that an article (or image, video, etc) doesn't contain disinformation and verify that a source (publisher, domain, etc) doesn't distribute disinformation.
- Extend MISP for disinformation, adding object types for incidents and narratives, and using [AMITT](#) for attack patterns.

Other personas

Malcolm represents users that we care about but aren't so important to us.

Malcolm

The Data Expert

Malcolm is a data scientist for a telecom operator in the USA. He assists the Security Operations Center with tasks related to anomaly detection, exploratory data analysis, data visualization, modeling, and optimization of security solutions.

Malcolm uses data from MISP alongside natural language processing, predictive modeling, and other data science techniques to assess, prioritize, and even predict risk. He can process threat data to help with alert prioritization and data-driven decision making.

"It is a mistake to theorize before one has data. Insensibly, one begins to twist facts to suit theories, instead of theories to suit facts"

Role

Data Scientist

His primary goals are to:

- Develop tools to help businesses detect threats so they can develop solid plans of action and better protect themselves.
- Make predictions, perform data analysis, and detect patterns in data.
- Support the threat analysis team with the development of new and innovative ways of extracting insight from large sets of structured and unstructured data.
- Translate complex data into relevant insights and visualize information.

He uses MISP to:

- Collect IoCs and sift through data from feeds to derive useful insights and connect dots between actors from various sources.
- Join [sharing groups](#) to collaborate with threat analysts and reduce analysts' workload by taking on many tasks related to data collection and correlation.
- Automatically aggregate, parse, de-duplicate, and manage [indicators](#) using the [API](#).
- Visualize events in real-time by setting up MISP-dashboard.
- Export large threat data sets that can be used to train ML models

His objectives are to:

- Combine data from MISP and other security sources to find patterns/relationships in data, develop models, assess, prioritize, and predict risk using data science and AI techniques.
- Produce informative visualizations and knowledge graphs based on large data sets.
- Eliminate manual tasks by writing scripts that automatically aggregate, parse, de-duplicate, and manage [indicators](#) in MISP.
- Classify risks in order to save analysts time sorting through false positives and deciding what to prioritize.

Last modified: Sun Feb 28 2021 09:22:59 GMT+0100 (Central European Standard Time)

Summary

- [Appendix A: External Authentication](#)

```
* [The external authentication mechanism described](#the-external-authenti
* [Setting up the external authentication mechanism](#setting-up-the-exte
* [User management](#user-management)
* [Logging](#logging)
```

- [Appendix B: ACL descriptors](#)

```
* [Querying the ACL system](#querying-the-acl-system)
* [Getting a list of URLs accessible to a role](#getting-a-list-of-urls-ac
* [Getting a list of all accessible controllers and actions in MISP](#gett
* [Viewing a list of yet unmapped functions](#viewing-a-list-of-yet-unmapp
```

- [Appendix C: Official MISP developments](#)
- [Appendix D: Third-party development](#)
- [Appendix E: Other Threat Intel Ressources](#)
- [Appendix F: LDAP Authentication](#)

```
* [Installation and configuration](#installation-and-configuration)
* [Debugging](#debugging)
* [Migrating existing user to LDAP](#migrating-existing-user-to-ldap)
* [Caveats](#caveats)
```

Appendix A: External Authentication

The external authentication mechanism described

The external authentication allows a user or an external tool to authenticate with MISP using an arbitrary value passed along in a custom header. This authentication method overrides the regular authentication mechanisms and is customisable by a site-admin.

It is possible to create a mixed mode MISP setup where certain users can go through the normal authentication mechanism and other users are required to use the external authentication method.

Setting up the external authentication mechanism

To change the authentication settings, navigate to Administration - Server settings - Plugin settings

The settings associated with the external authentication can be found by pressing the CustomAuth button as depicted below:

ZeroMQ			
CustomAuth			
Priority	Setting	Value	Description
Optional	Plugin.CustomAuth_enable	true	Enable this func authenticate wit
Optional	Plugin.CustomAuth_header	radac_auth_header	Set the header header.
Optional	Plugin.CustomAuth_required	false	If this setting is Alternatively yc users will be re
Optional	Plugin.CustomAuth_only_allow_source		If you are using url as a valid pc
Optional	Plugin.CustomAuth_name	Radac	The name of the creation page a
Optional	Plugin.CustomAuth_disable_logout	true	Disable the log
Optional	Plugin.CustomAuth_custom_password_reset	https://my/custom/pw/reset	Provide your cu reset their pass
Optional	Plugin.CustomAuth_custom_logout	https://my/custom/logout	Provide a custo system you use

To change a setting simply double click on the value to edit the field. Use the guidance provided by the setting tool to configure the external authentication. The accessible settings are as follows:

- **enable:** Enable or disable external authentication (off by default)
- **header:** The header which MISP will use to identify users
- **required:** Enabling this setting will force all users to use the external authentication. Leave this disabled allows administrators to assign external authentication or regular authentication users.
- **only_allow_source:** Setting a url / IP address here will only allow requests that originated from the given address
- **name:** The name to be used for the authentication mechanism. This is reflected in the user creation / edit views, the logs and the error messages on failed logins.
- **disable_logout:** Disable the default logout button. Using an external authentication mechanism that authenticates via the header with each requests makes the logout button obsolete.
- **custom_password_reset:** If your authentication system has a url that a user can access to reset his/her password, please specify the full url for it here. This will then be reused in the UI.
- **custom_password_logout:** If your authentication system has a url that a user can access to logout, please specify the full url for it here. This will then be reused in the UI.

User management

Using a new setting, user self management can be disabled for all users that are not administrators via the `MISP.disableUserSelfManagement` setting, found in the MISP settings tab. Enabling this setting removes the ability of users to change their user settings and reset their authentication keys. All other functionality remains unchanged.

Email

☐ External authentication user

☒ Set password

Organisation

Role

Authkey

Nids Sid

Sync user for

GPG key

Fetch GPG key

☐ Receive alerts when events are published

☐ Receive alerts from "contact reporter" requests

☐ Disable this user account

Submit

To create an external authenticated user, simply tick the External authentication user checkbox, after which an external auth key field will appear. This will be used to identify the users via the passed along header.

Logging

For a description of the logging facilities provided by this plugin, please refer to the "Logging of failed authentication attempts" section of the Administration section.

Appendix B: ACL descriptors

Querying the ACL system

MISP allows site admins to query the ACL system for various types of data. This can be interesting when tuning for example WAF access to MISP. All applicable queries can be requested via /servers/queryACL

Getting a list of URLs accessible to a role

```
https://<misp url>/servers/queryACL/printRoleAccess/<role id>
```

The above URL will return a JSON with all accessible URLs for the given role ID. If no Role ID is provided, a JSON containing all [roles](#) and their access lists will be returned.

Example:

```

{
  "3": {
    "name": "User",
    "urls": [
      "/*restSearch",
      "/attributes/add",
      "/attributes/add_attachment",
      "/attributes/add_threatconnect",
      "/attributes/addTag",
      "/attributes/attributeReplace",
      "/attributes/attributeStatistics",
      "/attributes/bro",
      "/attributes/delete",
      "/attributes/deleteSelected",
      "/attributes/describeTypes",
      "/attributes/download",
      "/attributes/downloadAttachment",
      "/attributes/downloadSample",
      "/attributes/edit",
      "/attributes/editField",
      "/attributes/editSelected",
      "/attributes/exportSearch",
      "/attributes/fetchEditForm",
      "/attributes/fetchViewValue",
      "/attributes/getMassEditForm",
      "/attributes/hoverEnrichment",
      "/attributes/index",
      "/attributes/removeTag",
      "/attributes/restore",
      "/attributes/restSearch",
      "/attributes/returnAttributes",
      "/attributes/rpz",
      "/attributes/search",
      "/attributes/searchAlternate",
      "/attributes/toggleCorrelation",
      "/attributes/text",
      "/attributes/toggleToIDS",
      "/attributes/updateAttributeValues",
      "/attributes/view",
      "/attributes/viewPicture",
      "/authKeys/add",
      "/authKeys/delete",
      "/authKeys/edit",
      "/authKeys/index",
      "/authKeys/view",
      "/auth_keys/add",
      "/auth_keys/delete",
      "/auth_keys/edit",
      "/auth_keys/index",
      "/auth_keys/view",
      "/dashboards/getForm",
      "/dashboards/index",
      "/dashboards/updateSettings",
      "/dashboards/getEmptyWidget",
      "/dashboards/renderWidget",
      "/dashboards/listTemplates",
      "/dashboards/saveTemplate",
      "/dashboards/export",
      "/dashboards/import",
      "/dashboards/deleteTemplate",
      "/decayingModel/export",
      "/decayingModel/import",
      "/decayingModel/view",
      "/decayingModel/index",
      "/decayingModel/add",

```

```

"/decayingModel/edit",
"/decayingModel/delete",
"/decayingModel/enable",
"/decayingModel/disable",
"/decayingModel/decayingTool",
"/decayingModel/getAllDecayingModels",
"/decayingModel/decayingToolBasescore",
"/decayingModel/decayingToolSimulation",
"/decayingModel/decayingToolRestSearch",
"/decayingModel/decayingToolComputeSimulation",
"/decaying_model/export",
"/decaying_model/import",
"/decaying_model/view",
"/decaying_model/index",
"/decaying_model/add",
"/decaying_model/edit",
"/decaying_model/delete",
"/decaying_model/enable",
"/decaying_model/disable",
"/decaying_model/decayingTool",
"/decaying_model/getAllDecayingModels",
"/decaying_model/decayingToolBasescore",
"/decaying_model/decayingToolSimulation",
"/decaying_model/decayingToolRestSearch",
"/decaying_model/decayingToolComputeSimulation",
"/decayingModelMapping/viewAssociatedTypes",
"/decayingModelMapping/linkAttributeTypeToModel",
"/decaying_model_mapping/viewAssociatedTypes",
"/decaying_model_mapping/linkAttributeTypeToModel",
"/eventBlocklists/add",
"/eventBlocklists/delete",
"/eventBlocklists/edit",
"/eventBlocklists/index",
"/eventBlocklists/massDelete",
"/event_blocklists/add",
"/event_blocklists/delete",
"/event_blocklists/edit",
"/event_blocklists/index",
"/event_blocklists/massDelete",
"/eventReports/add",
"/eventReports/view",
"/eventReports/viewSummary",
"/eventReports/edit",
"/eventReports/delete",
"/eventReports/reportFromEvent",
"/eventReports/restore",
"/eventReports/index",
"/eventReports/getProxyMISPElements",
"/eventReports/extractAllFromReport",
"/eventReports/extractFromReport",
"/eventReports/replaceSuggestionInReport",
"/eventReports/importReportFromUrl",
"/event_reports/add",
"/event_reports/view",
"/event_reports/viewSummary",
"/event_reports/edit",
"/event_reports/delete",
"/event_reports/reportFromEvent",
"/event_reports/restore",
"/event_reports/index",
"/event_reports/getProxyMISPElements",
"/event_reports/extractAllFromReport",
"/event_reports/extractFromReport",
"/event_reports/replaceSuggestionInReport",
"/event_reports/importReportFromUrl",
"/events/add",

```

```

"/events/addIOC",
"/events/addTag",
"/events/add_misp_export",
"/events/automation",
"/events/checkLocks",
"/events/checkPublishedStatus",
"/events/contact",
"/events/csv",
"/events/delegation_index",
"/events/delete",
"/events/deleteNode",
"/events/downloadExport",
"/events/downloadOpenIOCEvent",
"/events/edit",
"/events/enrichEvent",
"/events/export",
"/events/exportChoice",
"/events/exportModule",
"/events/filterEventIndex",
"/events/freeTextImport",
"/events/getEditStrategy",
"/events/getEventInfoById",
"/events/getEventGraphReferences",
"/events/getEventGraphTags",
"/events/getEventGraphGeneric",
"/events/getEventTimeline",
"/events/genDistributionGraph",
"/events/getDistributionGraph",
"/events/getReferenceData",
"/events/getReferences",
"/events/getObjectTemplate",
"/events/handleModuleResults",
"/events/hids",
"/events/index",
"/events/importChoice",
"/events/importModule",
"/events/merge",
"/events/nids",
"/events/proposalEventIndex",
"/events/publishSightings",
"/events/queryEnrichment",
"/events/removePivot",
"/events/removeTag",
"/events/restSearch",
"/events/runTaxonomyExclusivityCheck",
"/events/saveFreeText",
"/events/stix",
"/events/stix2",
"/events/toggleCorrelation",
"/events/unpublish",
"/events/updateGraph",
"/events/upload_analysis_file",
"/events/upload_sample",
"/events/upload_stix",
"/events/view",
"/events/viewClusterRelations",
"/events/viewEventAttributes",
"/events/viewGraph",
"/events/viewGalaxyMatrix",
"/events/xml",
"/favouriteTags/toggle",
"/favouriteTags/getToggleField",
"/favourite_tags/toggle",
"/favourite_tags/getToggleField",
"/feeds/compareFeeds",
"/feeds/feedCoverage",

```



```

"/feeds/index",
"/feeds/previewEvent",
"/feeds/previewIndex",
"/feeds/searchCaches",
"/feeds/view",
"/galaxies/attachCluster",
"/galaxies/attachMultipleClusters",
"/galaxies/export",
"/galaxies/forkTree",
"/galaxies/index",
"/galaxies/relationsGraph",
"/galaxies/selectGalaxy",
"/galaxies/selectGalaxyNamespace",
"/galaxies/selectCluster",
"/galaxies/showGalaxies",
"/galaxies/view",
"/galaxies/viewGraph",
"/galaxyClusters/attachToEvent",
"/galaxyClusters/detach",
"/galaxyClusters/index",
"/galaxyClusters/restSearch",
"/galaxyClusters/view",
"/galaxyClusters/viewGalaxyMatrix",
"/galaxyClusters/viewRelations",
"/galaxyClusters/viewRelationTree",
"/galaxy_clusters/attachToEvent",
"/galaxy_clusters/detach",
"/galaxy_clusters/index",
"/galaxy_clusters/restSearch",
"/galaxy_clusters/view",
"/galaxy_clusters/viewGalaxyMatrix",
"/galaxy_clusters/viewRelations",
"/galaxy_clusters/viewRelationTree",
"/galaxyClusterRelations/index",
"/galaxyClusterRelations/view",
"/galaxy_cluster_relations/index",
"/galaxy_cluster_relations/view",
"/galaxyElements/index",
"/galaxy_elements/index",
"/jobs/cache",
"/jobs/getGenerateCorrelationProgress",
"/jobs/getProgress",
"/logs/event_index",
"/logs/returnDates",
"/modules/index",
"/modules/queryEnrichment",
"/news/index",
"/noticelists/index",
"/noticelists/view",
"/objects/add",
"/objects/addValueField",
"/objects/delete",
"/objects/edit",
"/objects/get_row",
"/objects/editField",
"/objects/fetchEditForm",
"/objects/fetchViewValue",
"/objects/quickAddAttributeForm",
"/objects/quickFetchTemplateWithValidObjectAttributes",
"/objects/restSearch",
"/objects/proposeObjectsFromAttributes",
"/objects/groupAttributesIntoObject",
"/objects/revise_object",
"/objects/view",
"/objectReferences/add",
"/objectReferences/delete",

```

```

"/objectReferences/view",
"/object_references/add",
"/object_references/delete",
"/object_references/view",
"/objectTemplates/objectChoice",
"/objectTemplates/objectMetaChoice",
"/objectTemplates/view",
"/objectTemplates/viewElements",
"/objectTemplates/index",
"/object_templates/objectChoice",
"/object_templates/objectMetaChoice",
"/object_templates/view",
"/object_templates/viewElements",
"/object_templates/index",
"/objectTemplateElements/viewElements",
"/object_template_elements/viewElements",
"/organisations/fetchSGOrgRow",
"/organisations/index",
"/organisations/view",
"/pages/display",
"/posts/add",
"/posts/delete",
"/posts/edit",
"/regexp/index",
"/restClientHistory/delete",
"/restClientHistory/index",
"/rest_client_history/delete",
"/rest_client_history/index",
"/roles/index",
"/roles/view",
"/servers/getApiInfo",
"/servers/getPyMISPVersion",
"/servers/getVersion",
"/servers/idTranslator",
"/servers/postTest",
"/servers/rest",
"/shadowAttributes/accept",
"/shadowAttributes/acceptSelected",
"/shadowAttributes/add",
"/shadowAttributes/add_attachment",
"/shadowAttributes/delete",
"/shadowAttributes/discard",
"/shadowAttributes/discardSelected",
"/shadowAttributes/download",
"/shadowAttributes/edit",
"/shadowAttributes/index",
"/shadowAttributes/view",
"/shadowAttributes/viewPicture",
"/shadow_attributes/accept",
"/shadow_attributes/acceptSelected",
"/shadow_attributes/add",
"/shadow_attributes/add_attachment",
"/shadow_attributes/delete",
"/shadow_attributes/discard",
"/shadow_attributes/discardSelected",
"/shadow_attributes/download",
"/shadow_attributes/edit",
"/shadow_attributes/index",
"/shadow_attributes/view",
"/shadow_attributes/viewPicture",
"/sharingGroups/index",
"/sharingGroups/view",
"/sharing_groups/index",
"/sharing_groups/view",
"/sightings/add",
"/sightings/restSearch",

```

```

"/sightings/advanced",
"/sightings/delete",
"/sightings/index",
"/sightings/listSightings",
"/sightings/quickDelete",
"/sightings/viewSightings",
"/sightings/bulkSaveSightings",
"/sightings/quickAdd",
"/tagCollections/index",
"/tagCollections/view",
"/tag_collections/index",
"/tag_collections/view",
"/tags/attachTagToObject",
"/tags/index",
"/tags/removeTagFromObject",
"/tags/search",
"/tags/selectTag",
"/tags/selectTaxonomy",
"/tags/showEventTag",
"/tags/showAttributeTag",
"/tags/showTagControllerTag",
"/tags/tagStatistics",
"/tags/view",
"/tags/viewGraph",
"/tags/viewTag",
"/taxonomies/index",
"/taxonomies/taxonomyMassConfirmation",
"/taxonomies/taxonomyMassHide",
"/taxonomies/taxonomyMassUnhide",
"/taxonomies/view",
"/taxonomies/unhideTag",
"/taxonomies/hideTag",
"/templateElements/index",
"/template_elements/index",
"/templates/deleteTemporaryFile",
"/templates/index",
"/templates/populateEventFromTemplate",
"/templates/submitEventPopulation",
"/templates/templateChoices",
"/templates/uploadFile",
"/templates/view",
"/threads/index",
"/threads/view",
"/threads/viewEvent",
"/users/attributeHistogram",
"/users/change_pw",
"/users/checkIfLoggedIn",
"/users/dashboard",
"/users/downloadTerms",
"/users/edit",
"/users/email_otp",
"/users/searchGpgKey",
"/users/fetchGpgKey",
"/users/histogram",
"/users/login",
"/users/logout",
"/users/register",
"/users/resetauthkey",
"/users/request_API",
"/users/routeafterlogin",
"/users/statistics",
"/users/tagStatisticsGraph",
"/users/terms",
"/users/updateLoginTime",
"/users/view",
"/users/getGpgPublicKey",

```

```

        "/userSettings/index",
        "/userSettings/view",
        "/userSettings/setSetting",
        "/userSettings/getSetting",
        "/userSettings/delete",
        "/userSettings/setHomePage",
        "/user_settings/index",
        "/user_settings/view",
        "/user_settings/setSetting",
        "/user_settings/getSetting",
        "/user_settings/delete",
        "/user_settings/setHomePage",
        "/warninglists/checkValue",
        "/warninglists/index",
        "/warninglists/view",
        "/allowedlists/index",
        "/eventGraph/view",
        "/eventGraph/add",
        "/eventGraph/delete",
        "/event_graph/view",
        "/event_graph/add",
        "/event_graph/delete"
    ]
}
}

```

Getting a list of all accessible controllers and actions in MISP

```
https://<misp url>/servers/queryACL/printAllFunctionNames
```

This URL will return a JSON with all controller and all mapped functions within them.

Viewing a list of yet unmapped functions

```
https://<misp url>/servers/queryACL/findMissingFunctionNames
```

Functions that have not been tied into the new ACL yet show up here. These functions will (until added to the ACL) only be accessible to site admins.

Appendix C: Official MISP developments

This section lists the projects that can be found on the main [MISP GitHub](#) page e know of but not officially support and rely on their respective maintainers to keep up to date to the MISP 2.4 developments.

Project	Description	Status
misp-objects	Definition, description and relationship types of MISP objects	Core to MISP, frequently updated and tested
Best Practices in ThreatIntel	Best practices in threat intelligence	Book available here: https://www.misp-project.org/best-practices-in-threat-intelligence.html

Appendix D: Third-party development

This section lists some projects we know of but not officially support and rely on their respective maintainers to keep up to date to the MISP 2.4 developments.

Project	Description	Status
MISP-STIX-ESM	Exports MISP events to STIX and ingest into McAfee ESM	Not tested by MISP core team
Docker MISP	Automated Docker MISP container	Not tested by MISP core team
misp42splunk	A Splunk app to use MISP in background and combine with TheHive	Not tested by MISP core team
getmisploc	getiocmisp is a Splunk custom search command that helps to extract IOCs from a MISP instance .	Not tested by MISP core team
OTX MISP	Imports Alienvault OTX pulses to a MISP instance	Not tested by MISP core team
BTG	BTG's purpose is to make fast and efficient search on IOC	Not tested by MISP core team
MISP OSINT Collection	Collection of best practices to add OSINT into MISP and/or MISP communities	Not tested by MISP core team
IBM XFE module	Various IBM X-Force Exchange modules	Not tested by MISP core team
MISP dockerized	MISP dockerized is a project designed to provide an easy-to-use and easy-to-install 'out of the box' MISP instance that includes everything you need to run MISP with minimal host-side requirements.	Not tested by MISP core team
MISP dockerized modules	MISP-modules for MISP dockerized	Not tested by MISP core team
FireMISP	FireEye Alert json files to MISP Malware information sharing platform (Alpha)	Not tested by MISP core team
MISP Chrome Plugin	MISP Chrome plugin for adding and looking up indicators	Not tested by MISP core team
PySight2MISP	PySight2MISP is a project that can be run to be used as glue between iSight intel API and MISP API	Not tested by MISP core team
tie2misp	Import DCSO TIE IOCs as MISP events	Not tested by MISP core team
security onion MISP	Grab NIDS rules and Bro Intel generated from a MISP instance and use them in Security Onion	Not tested by MISP core team

Project	Description	Status
virustream	A script to track malware IOCs with OSINT on Twitter.	Not tested by MISP core team
LAC CSV Import	Register MISP events based on information described in files such as CSV and TSV.	Not tested by MISP core team
The Hive	TheHive: a Scalable, Open Source and Free Security Incident Response Platform	Strong links between core team members, tested and known working
puppet-misp	This module installs and configures MISP - puppet forge site	Not tested by MISP core team
Ansible MISP	Ansible playbook to install Malware Information Sharing Platform (MISP)	unmaintained
ansible MISP	ansible role to setup MISP	Not tested by MISP core team
OpenDXL ATD MISP	Automated threat intelligence collection with McAfee ATD, OpenDXL and MISP	Not tested by MISP core team
IMAP Proxy	Modular IMAP proxy (including PyCIRCleanMail and MISP forward modules)	Not tested by MISP core team
AutoMISP	automate your MISP installs - This shell script is designed to automatically install MISP and the misp-modules extension on either Ubuntu 16.04, or 18.04.	Not tested by MISP core team
Palo Alto Networks report_to_misp	Parse a report and import the events into MISP	Not tested by MISP core team
Palo Alto Networks minemeld-misp	MineMeld nodes for MISP	Not tested by MISP core team
golang-misp	Golang Library to interact with your MISP instance	Not tested by MISP core team
go-misp	Golang MISP API Client	Not tested by MISP core team
MISP MAR	Integration between MISP platform and McAfee Active Response	Not tested by MISP core team

Project	Description	Status
MISP IoC Validator	Validate IOC from MISP ; Export results and iocs to SIEM and sensors using syslog and CEF format	Not tested by MISP core team
vt2misp	Script to fetch data from virustotal and add it to a specific event as an object	Not tested by MISP core team
Threat Pinch Lookup	Documentation and Sharing Repository for ThreatPinch Lookup Chrome & Firefox Extension	Not tested by MISP core team
dovehawk	Dovehawk is a Bro module that automatically imports MISP indicators and reports Sightings	Not tested by MISP core team
yara-exporter	Exporting MISP event attributes to yara rules usable with Thor apt scanner	Not tested by MISP core team
volatility-misp	Volatility plugin to interface with MISP	Not tested by MISP core team
misp2bro	Python script that gets IOC from MISP and converts it into BRO intel files.	Not tested by MISP core team
TA-misp	Splunk integration with MISP	Not tested by MISP core team
MISP QRadar	The Project can used to integrate QRadar with MISP Threat Sharing Platform	Not tested by MISP core team
pymisp-suricata_search	Multi-threaded suricata search module for MISP	Not tested by MISP core team
MISP-ThreatExchange	Script to interface MISP with Facebook ThreatExchange	Not tested by MISP core team
aptc	Automated Payload Test Controller	Not tested by MISP core team
aptmap	A map displaying threat actors from the misp-galaxy	Not tested by MISP core team
mispy	Another MISP module for Python	Not tested by MISP core team
MispSharp	C# Library for MISP	Not tested by MISP core team

Project	Description	Status
misp_btc	get BTC addresses from MISP and fetch BTC transactions	Tested by MISP core team
Privacy Aware Sharing of IoCs in MISP	Master Thesis including MISP data.	Master thesis
sam-bot	Bot to create MISP events from data in Slack	Not tested by MISP core team
Polarity.io Connector	"Polarity is the memory augmentation platform that makes your team smarter"	Not tested by MISP core team

Appendix E: Other Threat Intel Ressources

A brief list of online ressources that around #ThreatIntel

- [A curated list of awesome malware analysis tools and resources](#). Inspired by [awesome-python](#) and [awesome-php](#).
- [An authoritative list of awesome devsecops tools with the help from community experiments and contributions.DEV.SEC.OPS](#)
- [Advance Python IoC extractor](#)

Appendix F: LDAP Authentication

MISP supports LDAP authentication from version 2.4.xxx. This manual will show how to configure LDAP authentication.

Installation and configuration

1. Install `mod_ldap` PHP module

```
# for Centos or RHEL
yum install rh-php72-php-ldap
# for Ubuntu or debian
apt install php-ldap
```

2. Prepare variables for configuration

3. ``` - a full LDAP URI of server. For example: `ldap://example.com``.

4. ``` - DN for path that contains users. For example: `cn=users,cn=accounts,dc=example,dc=com``.

5. ``` - user that can read. For example: `uid=misp,cn=sysaccounts,cn=etc,dc=example,dc=com``.

6. ```` - password for that user.

7. ``` - group with access to MISP. For example: `cn=misp-users,cn=groups,cn=accounts,dc=example,dc=com``.
8. Configure MISP ApacheSecureAuth in `app/Config/config.php`

```
'LdapAuth' => array(
    'enabled' => true,
    'name' => 'My Identity provider',
    'ldapServer' => '',
    'ldapDN' => '',
    'ldapSearchFilter' => '(objectclass=inetuser)',
    'ldapReaderUser' => '',
    'ldapReaderPassword' => '',
    'ldapUserGroup' => '',
    'updateUser' => true,
);
```

Required variables:

- `enabled` – if it is true, all users must log in through LDAP account.
- `ldapServer` – a full LDAP URI of the form `ldap://hostname:port` or `ldaps://hostname:port` for TLS encryption.
- `ldapDN` – DN for a path that contains users.

Optional variables:

- `name` – identity provider name. Will be shown in the login screen and user editing for. Can contain HTML.
- `ldapReaderUser` – DN or RDN LDAP user with permission to read LDAP information about users.
- `ldapReaderPassword` – password for that user.
- `ldapSearchFilter` - LDAP search filter.
- `ldapSearchAttribute` - LDAP attribute that contains username. Default: `uid`.
- `ldapEmailField` - LDAP attribute (string) or attributes (array) that will be checked if contains user e-mail address. If you want to change or add field, you should also add that field/fields to `ldapAttributes`. Default: `mail`.
- `ldapAttributes` – fields that will be fetched from LDAP server. Default: `mail` and `memberof`.
- `ldapUserGroup` - LDAP group that must be assigned to user to access MISP. Default: not set.
- `createUser` - if `true`, MISP will create new user from LDAP. Default `true`.
- `updateUser` - if `true`, MISP will update existing users information (e-mail address and role) from LDAP after login. Default: `false`.
- `ldapDefaultOrg` – default organization ID for user from LDAP. By default it is the first organization in the database.
- `ldapDefaultRoleId` - default role for newly created user. It can be integer or array when key contains LDAP group and value assigned role ID. Must be defined if `updateUser` is set to `true` (without that variable, user will be disabled).
- `ldapProtocol` - protocol version used. Default: 3.
- `ldapNetworkTimeout` - timeout for communication with LDAP server in seconds. Default: 5 seconds.

- `ldapAllowReferrals` - follow referrals returned by the LDAP server. Default: `false` .
- `ldapStartTls` - enable STARTTLS. Default: `true` .

Debugging

Setting LDAP authentication can be sometimes tricky. For debugging, you can check MISP error log (by default in `/var/www/MISP/app/tmp/logs/error.log`) or debug log (by default in `/var/www/MISP/app/tmp/logs/debug.log`) that can contain useful information with problem description.

Migrating existing user to LDAP

Because LDAP and MISP users are paired by e-mail address, it is possible to migrate existing user account to LDAP managed. When you enable LDAP support and LDAP user will try to log in, an existing user in MISP with the same e-mail address will be found and then assigned to LDAP user.

Caveats

- When a user is disabled in LDAP or is removed from the required group, it will be not automatically disabled in MISP. That means that user will be disabled when he tries to login (with form or with Auth key), but for example, notification e-mails will still work until he tries to log in.
- When a user is disabled in LDAP and also in MISP and then enabled in LDAP, it will be enabled in MISP for next login just when `updateUser` is set to `true` .
- Currently it is not possible to log in with both LDAP and local (MISP) accounts.
- Admins can change users email address. But when `updateUser` is set to `true`, when the user will log in again, the e-mail address will be updated from LDAP.
- `Security.require_password_confirmation` setting currently doesnt work with LDAP authentication. But on the other hand, since user cannot change e-mail address and password, this setting is not important.