

MISP MANUAL INSTRUCTIONS

MISP Instance requirements

- **Introduction**
- **Core Components (The Big Picture)**
- **Sizing Your MISP Instance**
- **Database Configuration and Optimization**
- **Feed Caching and Performance Management**

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)

Sizing your MISP instance

Sizing a MISP instance highly depends on how the instance will be used. The number of users, data ingested, data points used, number of events, number of correlations and [API](#) usage are all parameters which should be considered while sizing your instance.

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.

Some considerations for what might affect your requirements:

- How highly correlating your data is (correlations are generally memory and computation intensive), if you have a high correlation ratio, consider either lowering this with better management of the data (correlate flag on attributes) or by increasing the memory and CPU available;
- Number of samples and attachments directly affect the disk usage;
- Concurrent user counts affect the memory usage and CPU utilisation, especially if you have a list of API users querying MISP frequently;
- Number of remote feeds and servers cached and kept in memory will also increase the memory requirements of the system;
- The amount of logging / activity / longevity of the server can increase the disk requirements both on the database as well as the local log file stash;

To give some indications of some of the operational servers:

- 16GB memory and 2 vcpus are quite common for smaller sharing hubs and end-point MISPs;
- large sharing communities (such as the CIRCL private sector community) use 128 GB of memory with 32 physical CPU cores on modern Xeon CPUs;
- The COVID misp runs on 8GB of memory with 4 vcpus and serves over a thousand users;
- The training instances we use, run on a meager 2GB of memory and a single vcpu (though we would not recommend using this for anything besides trainings / experimentation);

Database

The main database of MISP relies on MariaDB. Using SSDs is highly recommended to ensure a low latency on the I/O and ensure an efficient access to the database.

The type of storage used by MariaDB can also have an impact of the latency and disk space used.

Feed caching

Feed caching using RAM to store elements from the feeds enabled and cached. As an example, if you use the default available feeds, you can use up to 1.2Gb of memory if all feeds are enabled.

Using misp-docker

The most popular way to run the threat intel sharing platform MISP with Docker is the open source [misp-docker](#) project on Github.

It's a great way to quickly and easily spin up a local MISP for testing purposes, including a connected database (MariaDB) and Redis instance.

To get MISP up and running on your local machine, follow these steps:

1. First, install Docker. Make sure the the [Docker Desktop](#) application is running on your machine.
2. Clone the [misp-docker](#) repository.

```
(harsh@kali)-[~/Downloads/misp-docker]
$ git clone https://github.com/MISP/misp-docker.git
Cloning into 'misp-docker' ...
```

3. From the root of the repository, copy template.env to .env. You can leave the default environment variables as is if you only want to run Docker locally for testing.

```
(harsh@kali)-[~/Downloads/misp-docker]
$ ls -alps
total 176
4 drwxrwxr-x 16 harsh harsh 4096 Nov 3 21:26 ./
4 drwxr-xr-x 4 harsh harsh 4096 Nov 3 18:48 ../
4 drwxrwx--- 2 www-data www-data 4096 Nov 3 21:10 configs/
4 drwxrwxr-x 3 harsh harsh 4096 Nov 3 18:48 core/
4 drwxr-xr-x 6 root root 4096 Nov 3 20:49 custom/
8 -rw-rw-r-- 1 harsh harsh 4567 Nov 3 18:48 docker-bake.hcl
16 -rw-rw-r-- 1 harsh harsh 14830 Nov 3 18:48 docker-compose.yml
4 drwxrwxr-x 2 harsh harsh 4096 Nov 3 18:48 docs/
12 -rw-rw-r-- 1 harsh harsh 11684 Nov 3 18:55 .env
4 drwxrwxr-x 3 harsh harsh 4096 Nov 3 18:48 experimental/
4 drwxrwx--- 17 www-data www-data 4096 Nov 3 20:57 files/
4 drwxrwxr-x 7 harsh harsh 4096 Nov 3 18:48 .git/
4 drwxrwxr-x 3 harsh harsh 4096 Nov 3 18:48 .github/
4 -rw-rw-r-- 1 harsh harsh 144 Nov 3 18:48 .gitignore
4 drwx--- 4 www-data www-data 4096 Nov 3 20:58 gnupg/
4 drwxrwxr-x 3 harsh harsh 4096 Nov 3 18:48 guard/
4 drwxrwxr-x 3 harsh harsh 4096 Nov 3 18:48 kubernetes/
36 -rw-rw-r-- 1 harsh harsh 35149 Nov 3 18:48 LICENSE
4 drwxrwx--- 2 www-data www-data 4096 Nov 3 20:58 logs/
4 drwxrwxr-x 2 harsh harsh 4096 Nov 3 18:48 modules/
24 -rw-rw-r-- 1 harsh harsh 23045 Nov 3 18:48 README.md
4 drwxr-xr-x 2 root root 4096 Nov 3 20:56 ssl/
12 -rw-rw-r-- 1 harsh harsh 11684 Nov 3 18:48 template.env
```

4. Run docker compose pull.

```
(harsh@kali)-[~/Downloads/misp-docker]
$ sudo docker compose pull
WARN[0000] The "CRON_PULLALL" variable is not set. Defaulting to a blank string.
WARN[0000] The "CRON_PUSALL" variable is not set. Defaulting to a blank string.
WARN[0000] The "DISABLE_IPV6" variable is not set. Defaulting to a blank string.
WARN[0000] The "DISABLE_SSL_REDIRECT" variable is not set. Defaulting to a blank string.
WARN[0000] The "GUARD_COMMIT" variable is not set. Defaulting to a blank string.
WARN[0000] The "GUARD_ARGS" variable is not set. Defaulting to a blank string.
[+] Pulling 31/31
✓ redis Pulled
✓ misp-core Pulled
✓ db Pulled
✓ misp-modules Pulled
✓ mail Pulled
```

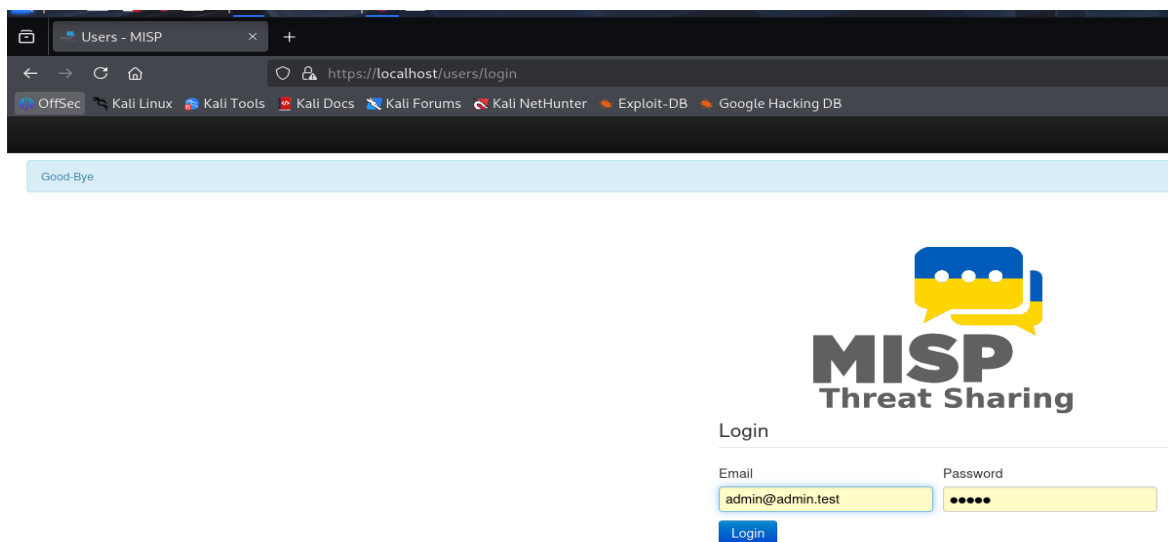
5. Run docker compose up. Note: if you have problems with volume mounting, try changing the file sharing implementation for your containers to osxfs (Legacy).

```
[+] Running 4/4
✓ Container misp-docker-db-1           Healthy
✓ Container misp-docker-misp-modules-1 Healthy
✓ Container misp-docker-redis-1        Healthy
✓ Container misp-docker-misp-core-1    Started

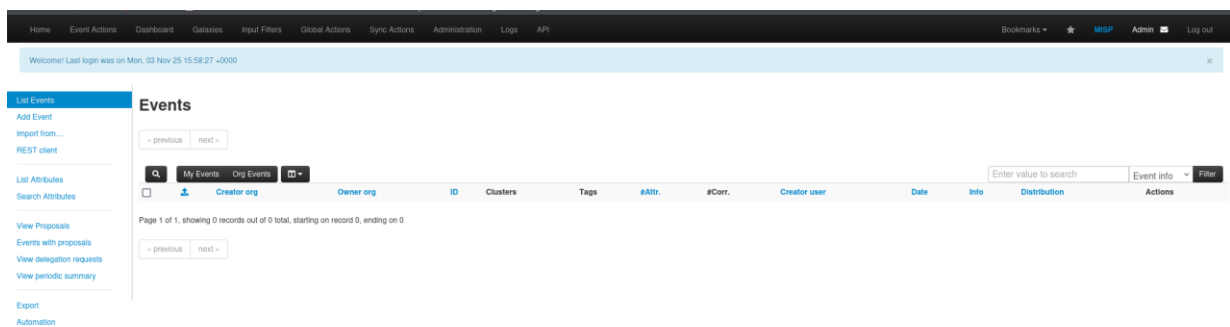
(harsh@kali)-[~/Downloads/misp-docker]
$
```

6. Once the process has finished, the MISP server will be running at **https://localhost**. You can login with the default MISP credentials:

1. User: admin@admin.test
2. Password: admin



Dashboard



Create an Event

A. Add Event

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

2. Populate Fields: Fill in the 'Event' form with details like 'OS-OS', 'This community only', 'Medium', and 'Example Event'.

3. Click 'Choose File' to select a file for the GFI sandbox.

4. Click 'Add' to save the event.

B. Add Attachments

6. Click 'Add Attachment' in the left sidebar.

7. Click 'Add Attachment' in the top left of the form.

8. Populate Fields: Fill in the 'Add Attachment' form with details like 'Payload delivery', 'This community only', and 'payload.txt'.

9. Click 'Upload' to save the attachment.

C. Add Event Attributes

5. Populate Fields: Fill in the 'Add Attribute' form with details like 'Network activity', 'domain', and 'example.org'.

Callouts:

- 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 shows the Malware Information Sharing Platform interface. On the left, a sidebar menu has 'List Events' highlighted with a green box and a callout '1. List Events'. The main area displays a table of events with columns: Valid, Org, Id, Status, Date, Risk, Analysis, Info, Distribution, and Actions. Two rows are visible, both for 'CyberSOC' with IDs 108 and 109. A callout '2. Filter' points to the search filters above the table. A callout '3. Click any row' points to the first row. Below the table, a detailed view of an event is shown. It includes fields for ID, UUID, Org, Date, Risk, Analysis, Distribution, and Info. A callout '4. See events with one or more matching attributes' points to the 'Related Events' section, which lists dates and counts of related events. The 'Attributes' section at the bottom shows a table with columns: Category, Type, Value, Related Events, IDS, Distribution, and Actions. It lists two attributes: 'Network activity - domain' and 'domain'.

Valid	Org	Id	Status	Date	Risk	Analysis	Info	Distribution	Actions
X	CyberSOC	108	1	2013-09-09	Medium	Initial	Example Event	This community only	Not published
X	CyberSOC	109	0	2013-09-04	Low	Ongoing	Example Event	This community only	Not published

Event Details:

- ID: 104
- UUID: 50fe6590-3ed4-4a09-8351-5492ac1d4fa4
- Org: NCRC
- Date: 2013-01-21
- Risk: Undefined
- Analysis: Completed
- Distribution: All communities, this will share the event with all MSP 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 (123)
- 2013-01-21 (45)
- 2013-01-12 (25)
- 2013-01-11 (31)
- 2013-01-27 (81)
- 2013-01-16 (32)
- 2013-01-12 (26)
- 2013-01-02 (7)

Attributes:

Category	Type	Value	Related Events	IDS	Distribution	Actions
Network activity - domain	domain	aa00c.org	81 23 7	No	All	
domain	domain	truematt.me		No	All	

Export Events for logsearches

The screenshot shows the 'Export' page of the Malware Information Sharing Platform. On the left, a sidebar menu has 'Export' highlighted with a green box and a callout '1. Export'. The main area contains text explaining the export functionality: 'Export functionality is designed to automatically generate signatures attribute. Signature field of this attribute must be set to Yes. Note that support NIDS signature generation for IP, domains, host names, user id for more attribute types is planned.' Below this text, there are two buttons: 'Download all as XML' and 'Download all as CSV'. A callout '2. Download for log correlation' points to the 'Download all as CSV' button. The text below the buttons says: 'Click this to download all events and attributes that you have access to' and 'Click this to download all attributes that you have access to'.

Export

Export functionality is designed to automatically generate signatures attribute. Signature field of this attribute must be set to Yes. Note that support NIDS signature generation for IP, domains, host names, user id for more attribute types is planned.

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

Download all as XML

Click this to download all events and attributes that you have access to

Download all as CSV

Click this to download all attributes that you have access to

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

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	5d2417e3-1448-4d33-bb86-2a1938a9ac58
Creator org	ORCNAME
Owner org	ORCNAME
Email	admin@oceanlotus.net
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

[Pivots](#) [Galaxy](#) [Event graph](#) [Correlation graph](#) [ATT&CK matrix](#) [Attributes](#) [Discussion](#)





[1 OSINT](#)





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

Galaxies

[previous](#) [next](#) [view all](#)

Scope toggle  Deleted  Context  Filtering tool 

[Date ↑](#) [Org](#) [Category](#) [Type](#) [Value](#) [Tags](#) [Galaxies](#) [Comment](#) [Correlate](#) [Related Events](#)

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

[previous](#) [next](#) [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

Freetext Import Tool

Paste a list of IOCs into the field below for automatic detection.

Submit
Cancel

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
c1e21a06a1fa1de2996392668b6910c	95 95	Payload delivery	sha256	<input checked="" type="checkbox"/>	Imported via the Freetext Import	✕

Submit

sha256 → authentihash Change all

Update all comment fields Change all

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

instead of

Similar Attributes

95 95

Attribute details

Event ID: 95

Event Info: OSINT - LinkedIn information used to spread banking malware in the Netherlands

Category: Payload delivery

Type: filename|sha256

Value: office.bin|c1e21a06a1fa1de2996392668b6910c

Comment: downloaded malware

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..."

OSINT

Event ID

UUID

Creator org

Owner org

Email

Tags

Date

Threat Level

Analysis

Distribution

Choose the format that you would like to use for the import

Freetext Import

Populate using a Template

OpenIOC Import

ThreatConnect Import

(Experimental) Forensic analysis - Mactime

Ocr

Mispjson

Openiocimport

Threatanalyzer Import

Cancel


For Freetext import select it

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:incidentclassification=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	ORNAME
Owner org	ORNAME
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	ORNAME	Select Tag collections (taxonomies) or self-created tags
Owner org	ORNAME	
Email	admin@	
Tags		
Date	2019-07	
Threat Level	Undefined	
Analysis	Initial	

Add a tag

Tag Collections Custom Tags All Tags

Select the input box to see the tags



malware

Submit

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	ORNAME
Owner org	ORNAME
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	ORNAME
Owner org	ORNAME
Email	admin@admin.test
Tags	  
Date	2019-07-09
Threat Level	Undefined
Analysis	Initial

To add local tags,
click here

Add a local tag 

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

They will be identified by a corresponding icon.

Tags	type:OSINT x osint:lifetime="perpetual" x circl:osint-feed x tlp: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 📌 🔍 🔗

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	ORGNAME /!\ If no tags show up, enable a Taxonomy or create some custom tags
Owner org	ORGNAME
Email	admin@
Tags	🌐 +
Date	2019-07
Threat Level	Undefined
Analysis	Initial

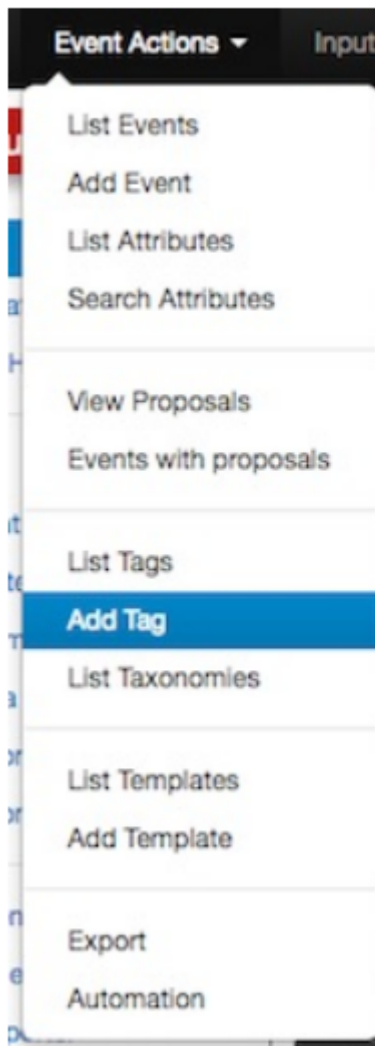
Add a tag
×

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:

A screenshot of the 'Add Tag' form in the application. The form is located in the main content area, and the sidebar on the left shows the 'Add Tag' option selected. The form has three input fields: 'Name' with the value 'Popom', 'Colour' with the value '#1bb5f7', and 'Restrict tagging to' with a dropdown menu set to 'Unrestricted'. There is a checkbox for 'Exportable' which is checked, and a blue 'Add' button at the bottom.

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.

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

The screenshot shows the MISP interface. On the left, a dropdown menu is open under 'Event Actions', with 'List Events' selected. The main area displays a table of events. Two red arrows originate from the text 'Your Event' and 'Your tag'. One arrow points to the event ID '145' in the 'Id' column, and the other points to the 'hophop' tag in the 'Tags' column of the same event row.

Org	Owner Org	Id	Tags	#Attr.	#Corr.
MISP	MISP	145	<code>circl:incident-classification="XSS"</code> <code>circl:incident-classification="information-leak"</code> hophop	1	1
MISP	MISP	95	Type:OSINT tip:white <code>circl:incident-classification="malware"</code>	12	1

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	1
	2019-07-09	

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.

[Home](#) [Event Actions](#) [Input Filters](#) [Global Actions](#) [Sync Actions](#) [Admin](#)

List Events

[Add Event](#)

[Import From MISP Export](#)

[List Attributes](#)

[Search Attributes](#)

[View Proposals](#)

[Events with proposals](#)

[Export](#)

[Automation](#)

Events

« previous 1 2 3 next »

My Events Org Events

Published	Org	Owner Org	Id	Tags
✓	MISP	MISP	145	<div>circl:incident-classification="X</div> <div>circl:incident-classification="in leak"</div> <div>hophop</div>
✓		MISP	95	<div>Type:OSINT tlp:</div> <div>circl:incident-classification="m</div>

Click to go

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 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	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

THANK YOU