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 an 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.

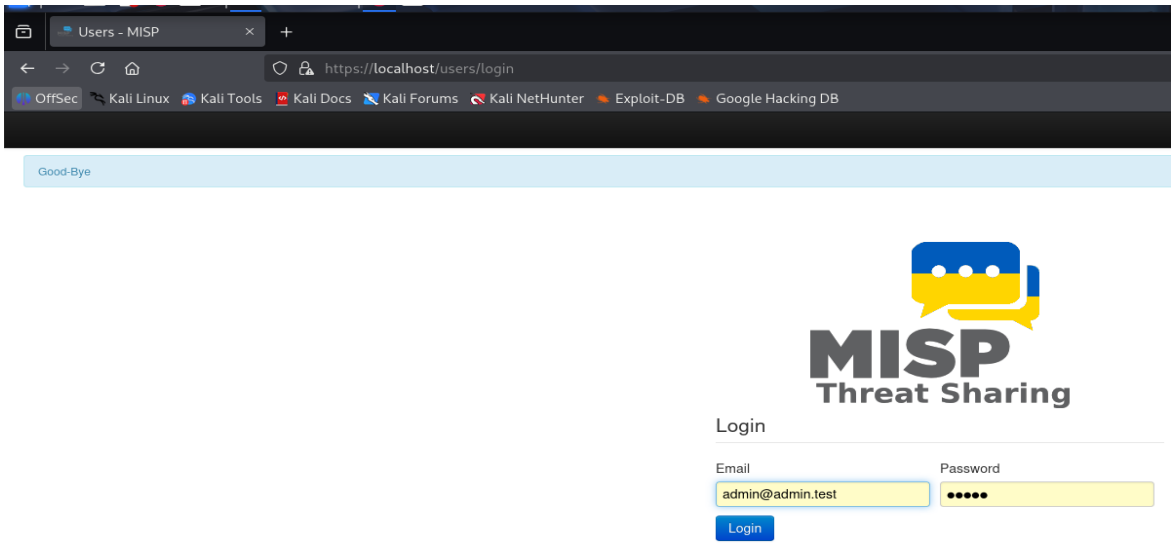
```
┌──(harsh㉿kali)-[~/Downloads/misp-docker]
└─$ sudo docker compose pull
WARN[0000] The "CRON_PULLALL" variable is not set. Defaulting to a blank string.
WARN[0000] The "CRON_PUSHALL" variable is not set. Defaulting to a blank string.
WARN[0000] The "DISABLE_IPV6" variable is not set. Defaulting to 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).

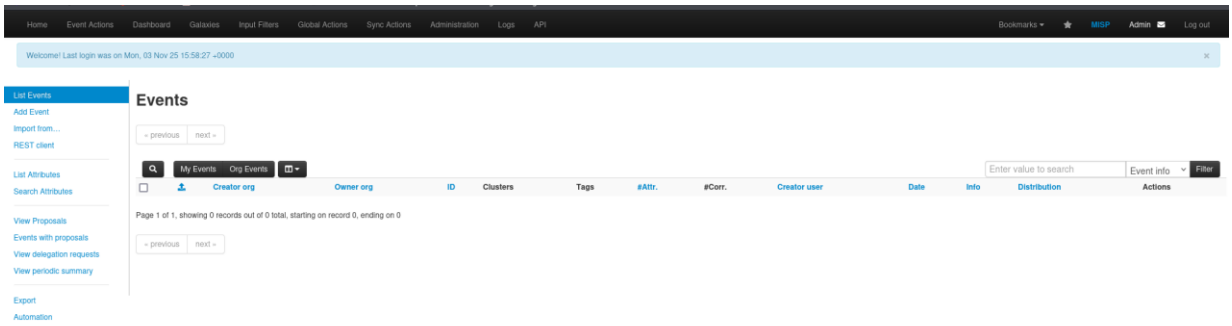
```
[+] Running 4/4
 ✔ Container misp-docker-db-1              Healthy
 ✔ Container misp-docker-misp-modules-1    Healthy
 ✔ Container misp-docker-redis-1           Healthy
 ✔ Container misp-docker-misp-core-1       Started

┌──(harsh㉿kali)-[~/Downloads/misp-docker]
└─$
```

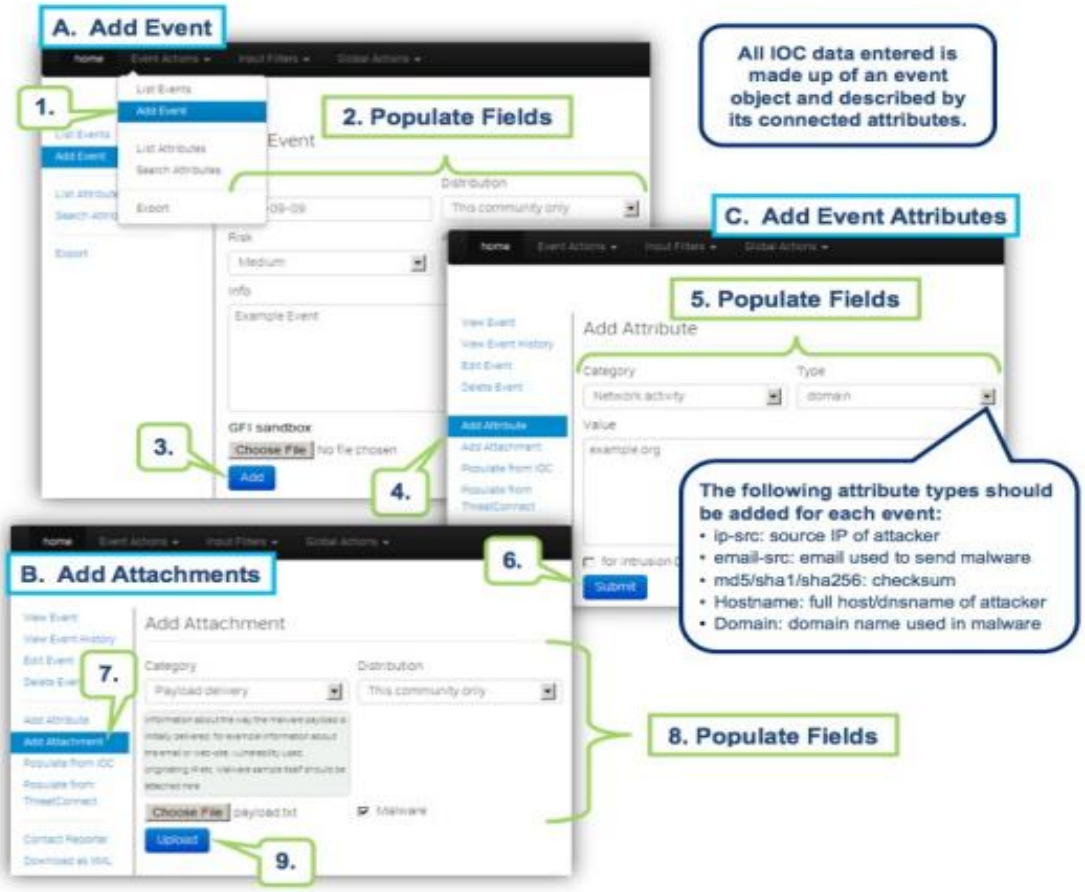
6. Once the process has finished, the MISP server will be running at **https://localhost**. You can login with the default MISP credentials:
    1. User: admin@admin.test
    2. Password: admin



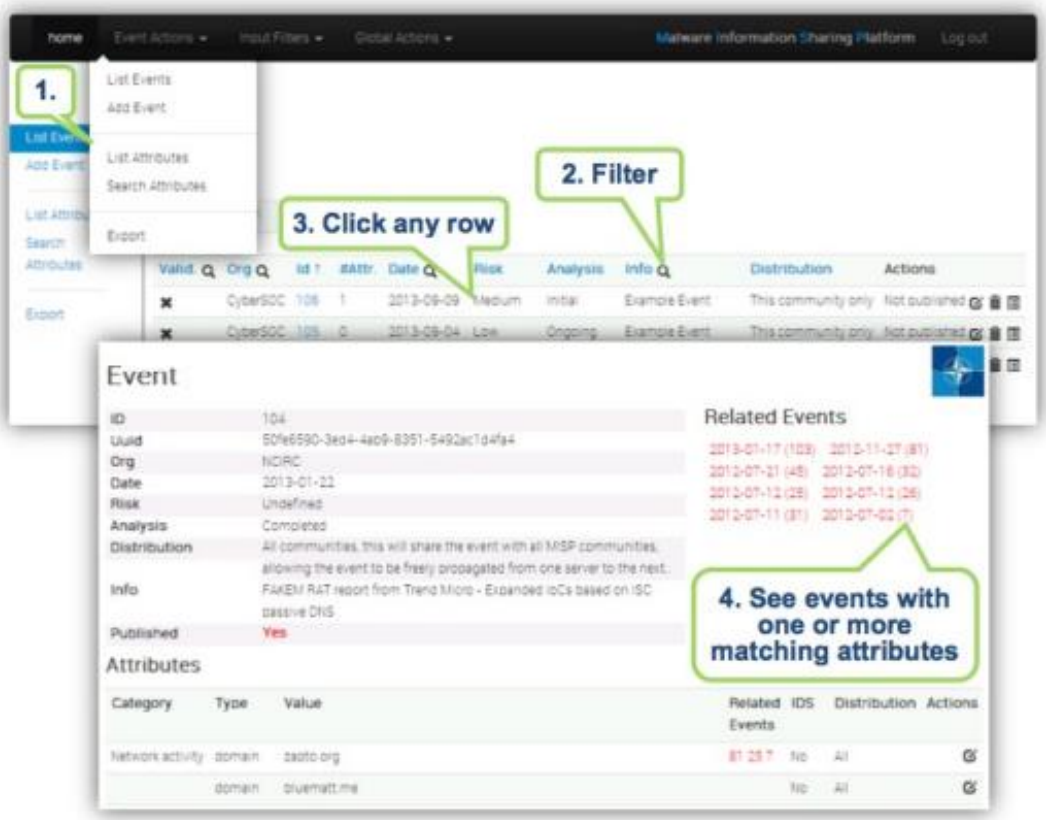
Dashboard



Create an Event

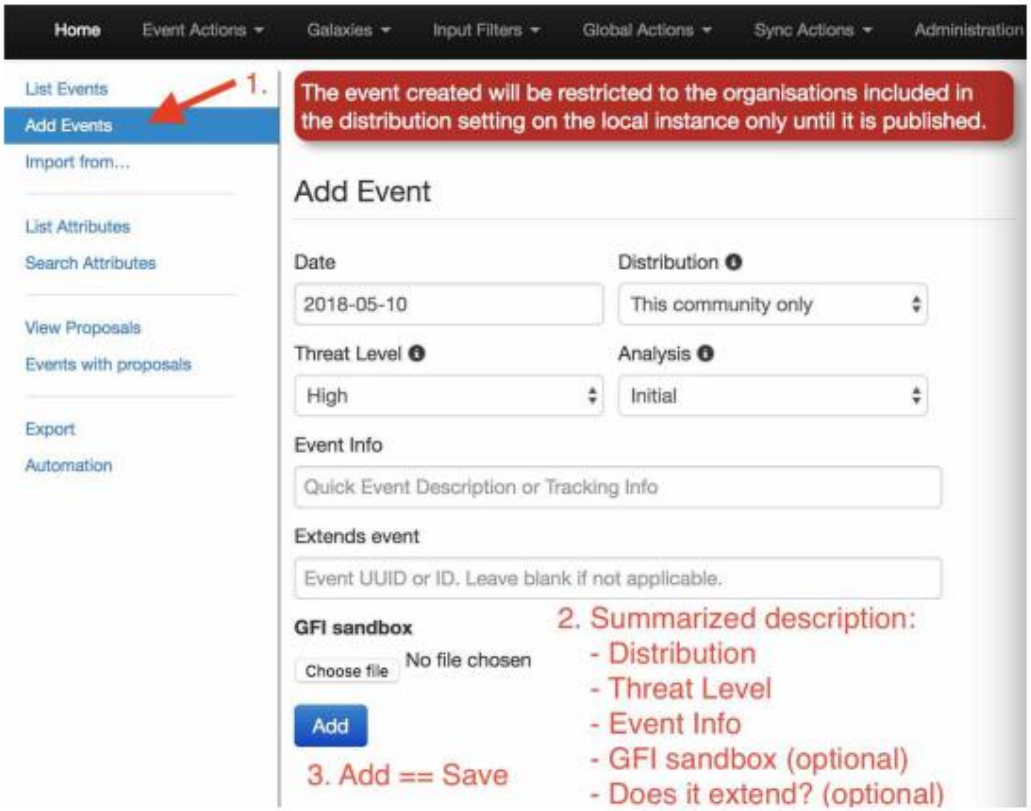


Browse Past Events



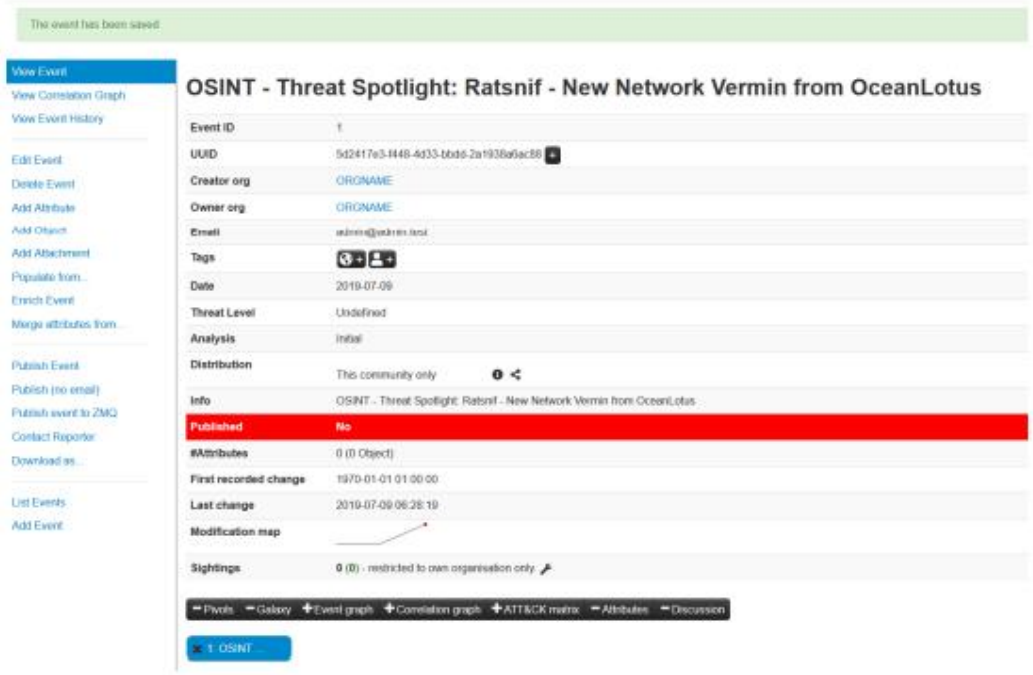
Export Events for logsearches

Create an Event



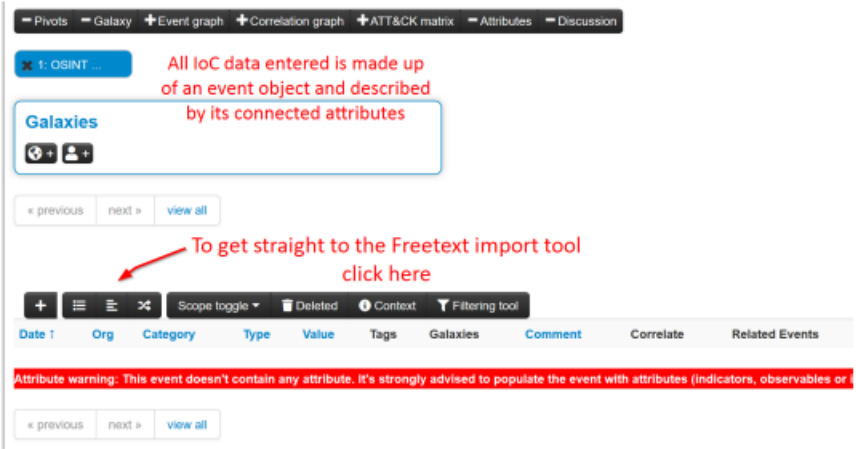
You only have to add a few pieces of information to register your Event. Further details will be specified after the Event has been added.

Describe Event

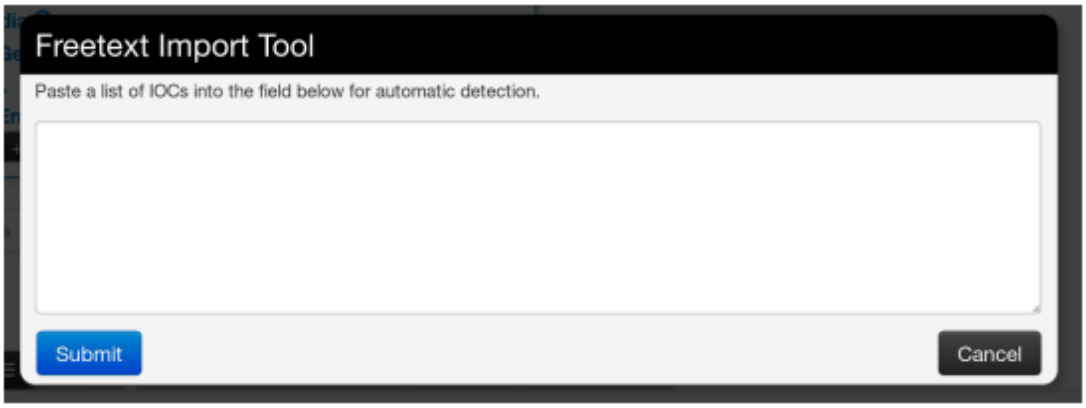


Now you can specify the information for your Event (you will need to scroll the window).

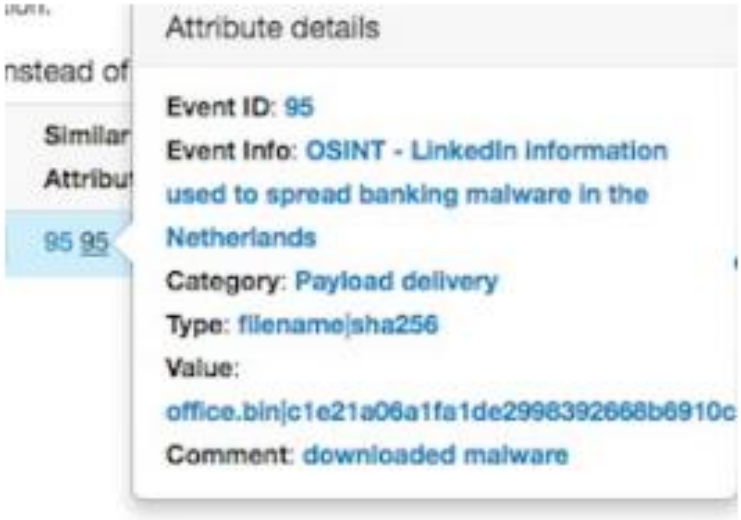
Free-Text Import Tool



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



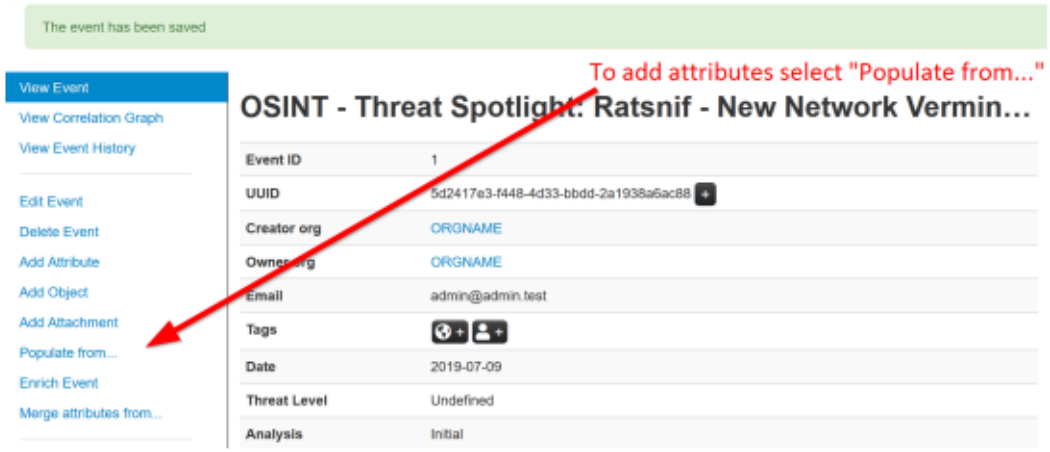
The tool will help you to find similarities between your import and other issues already registered in MISP.

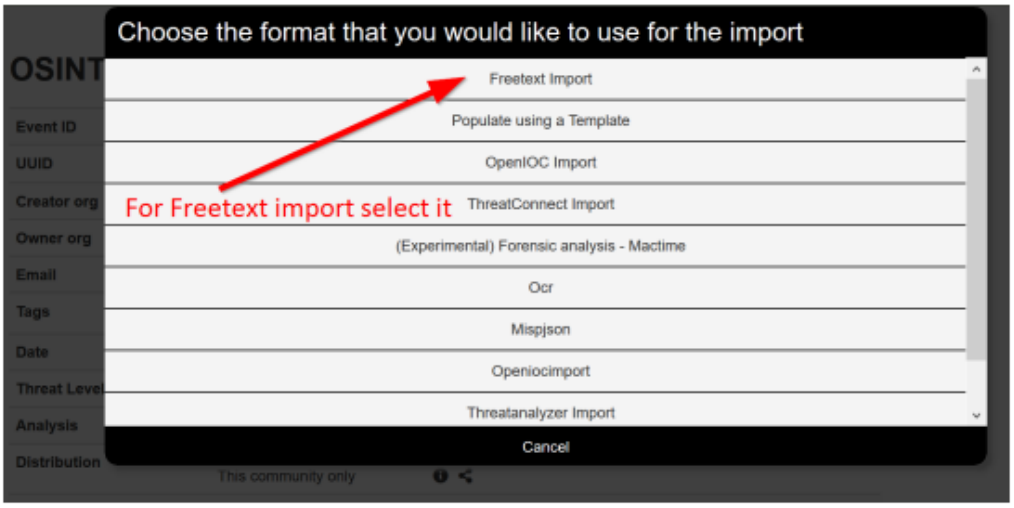


For example, you can see the ID of all related Events and view their information.

Alternative to import

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

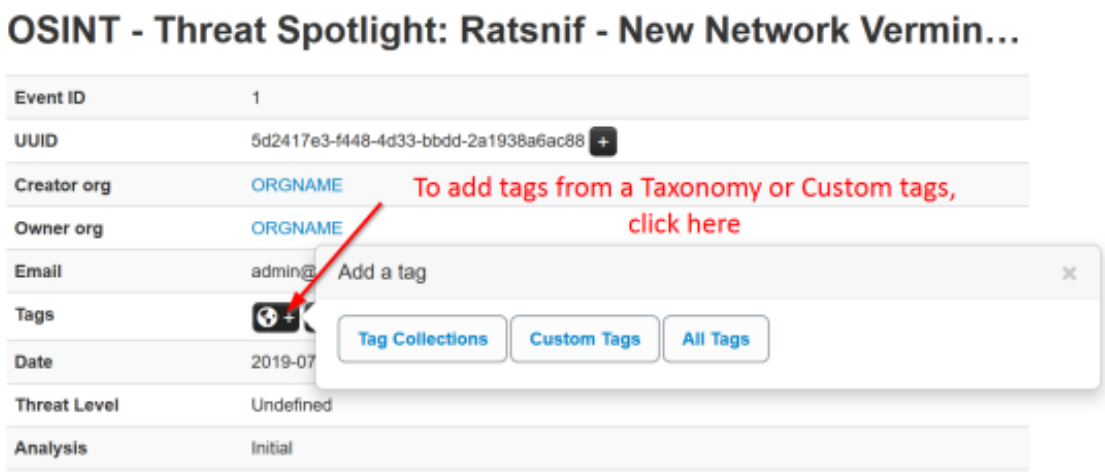




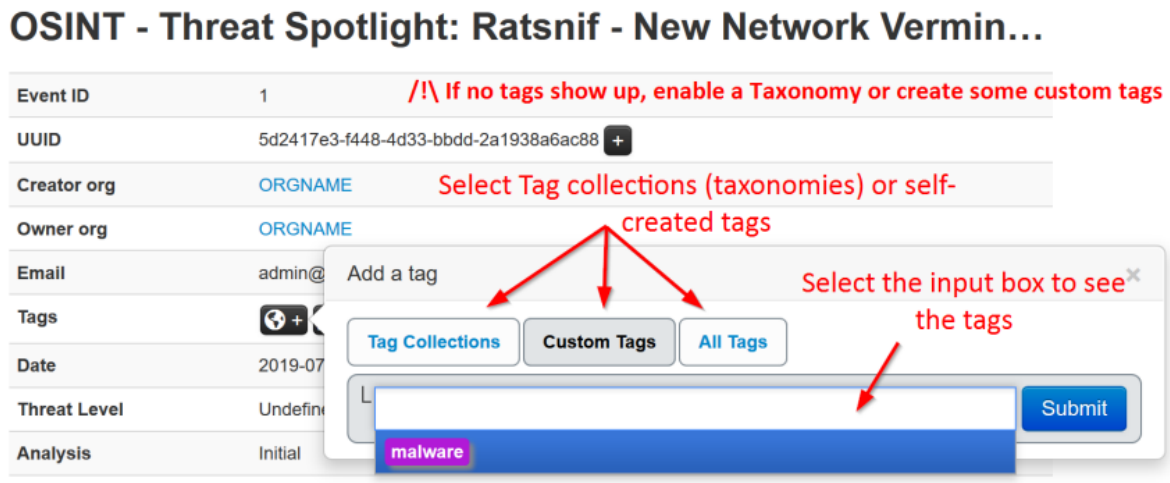
Tags and Taglist

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 ans circl:incident-classification="information-leak).

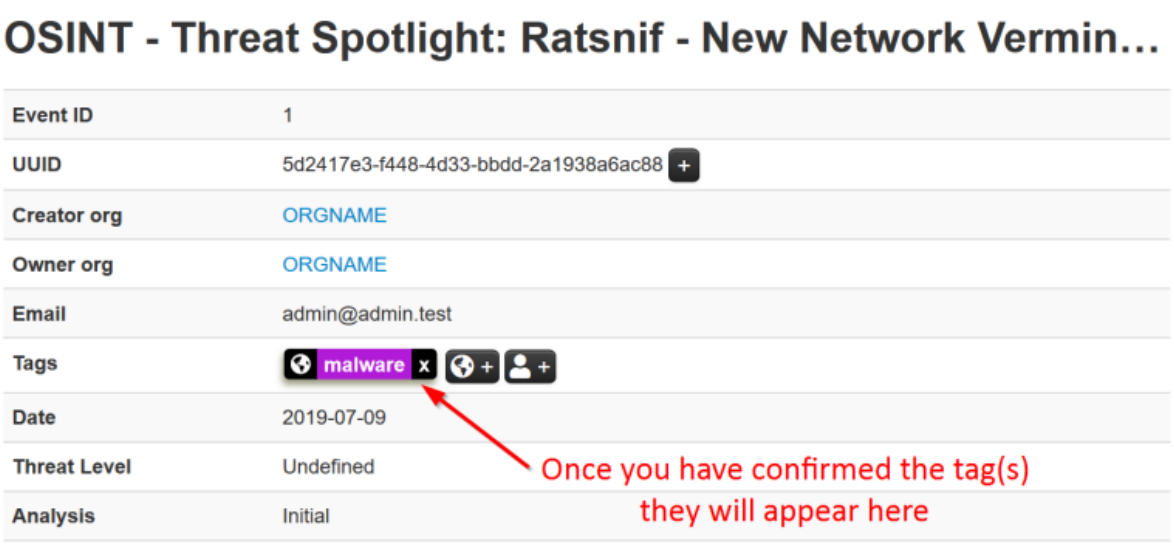


By clicking the button, you can add more tags from an existing Taglist.



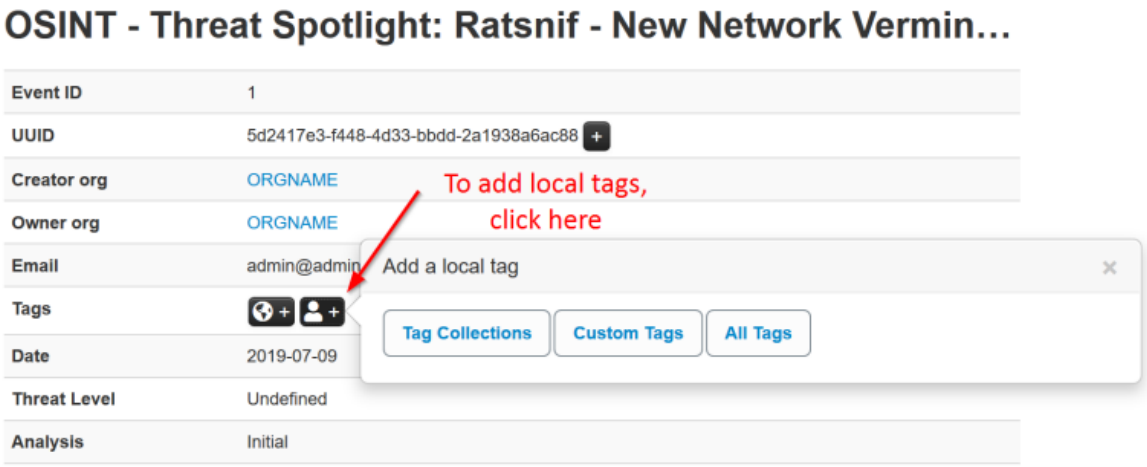
In particular the "Taxonomy Library: circl" Taglist is very complete.

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

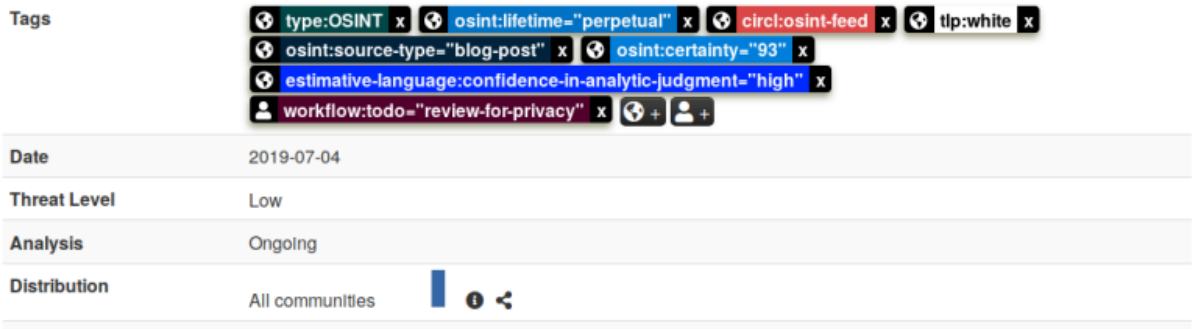


Local tags

Local tags can be added in a similar fashion.

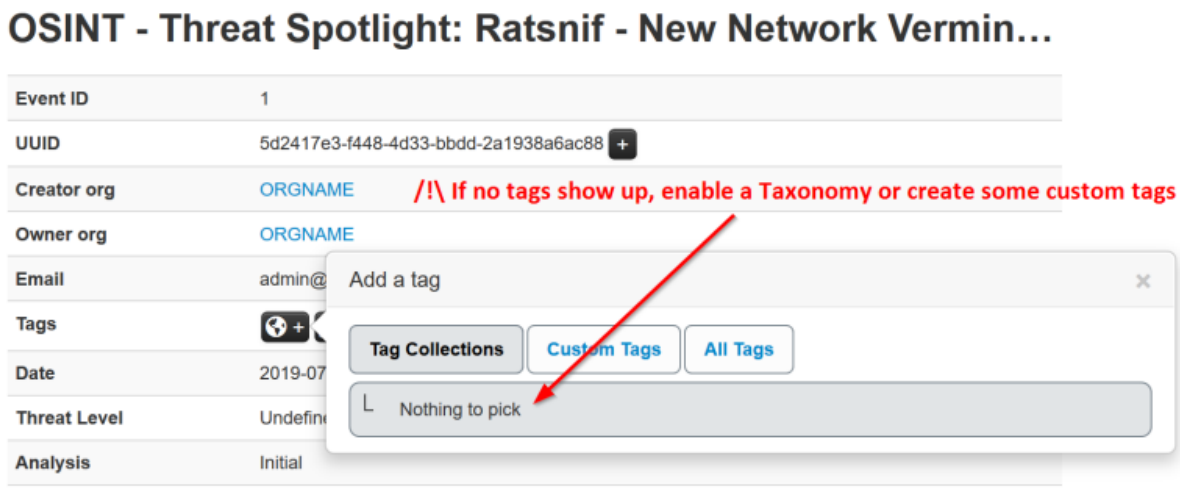


They will be identified by a corresponding icon.



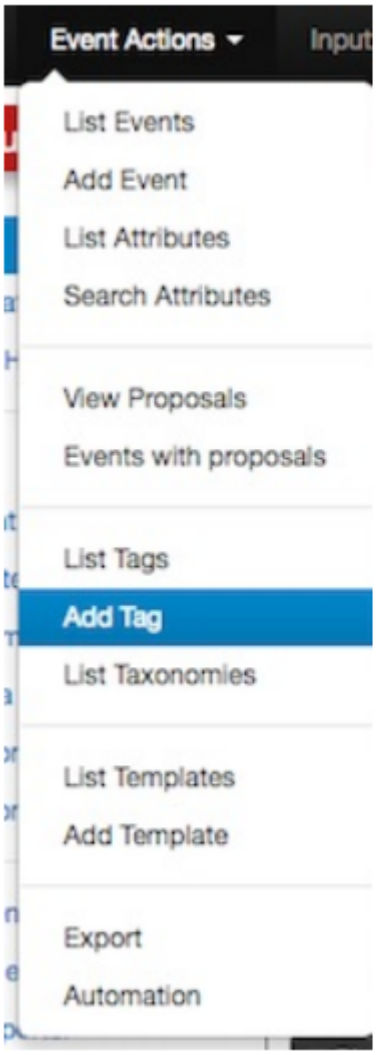
No tags in list

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

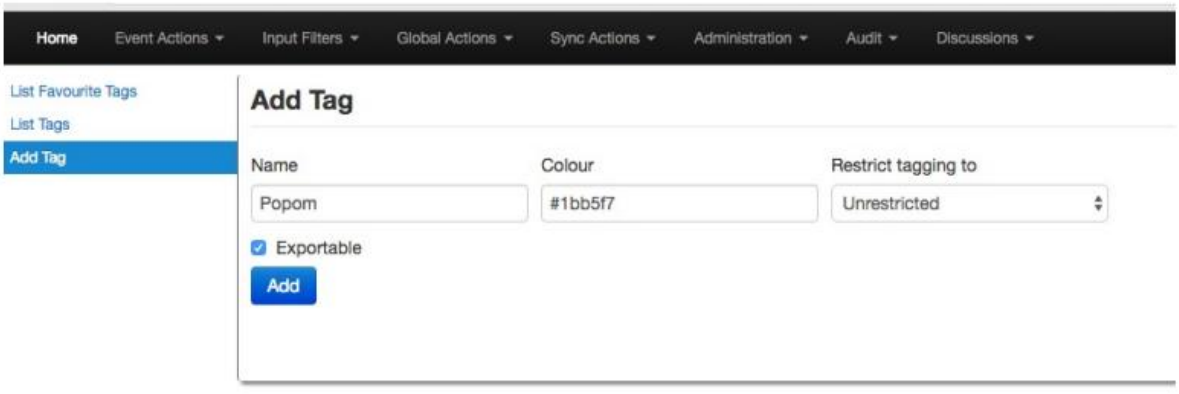


Make your own Taglist

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



You will see the following window:



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

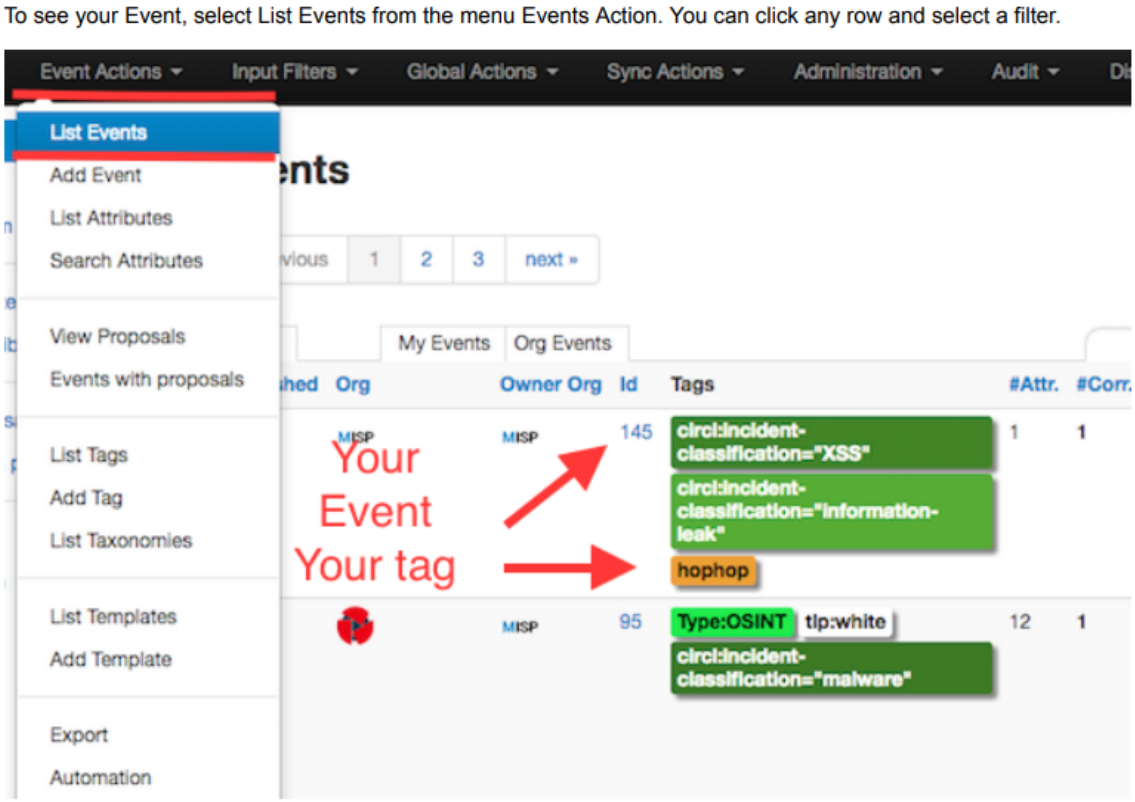
Suggestions

The following attribute types should be added for each Event: ip-src:

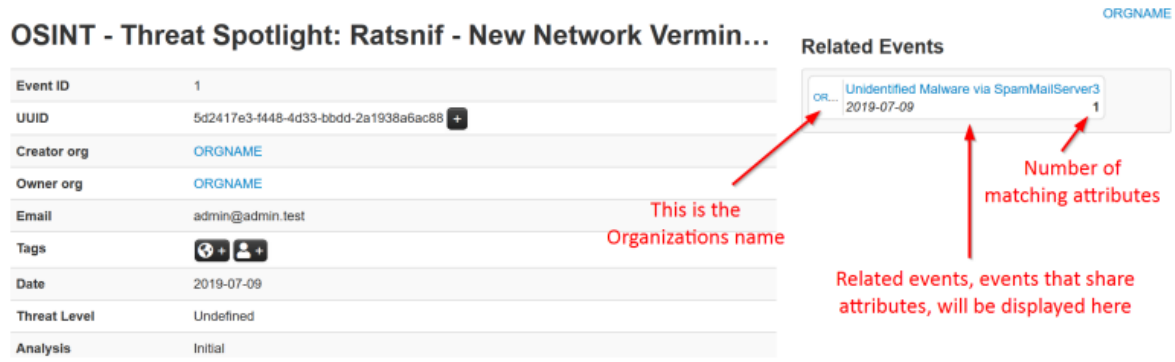
- source IP of attacker
- email-src: email used to send malware
- md5/sha1/sha256: checksum
- Hostname: full host/dnsname of attacker
- Domain: domain name used in malware

Browsing Events

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

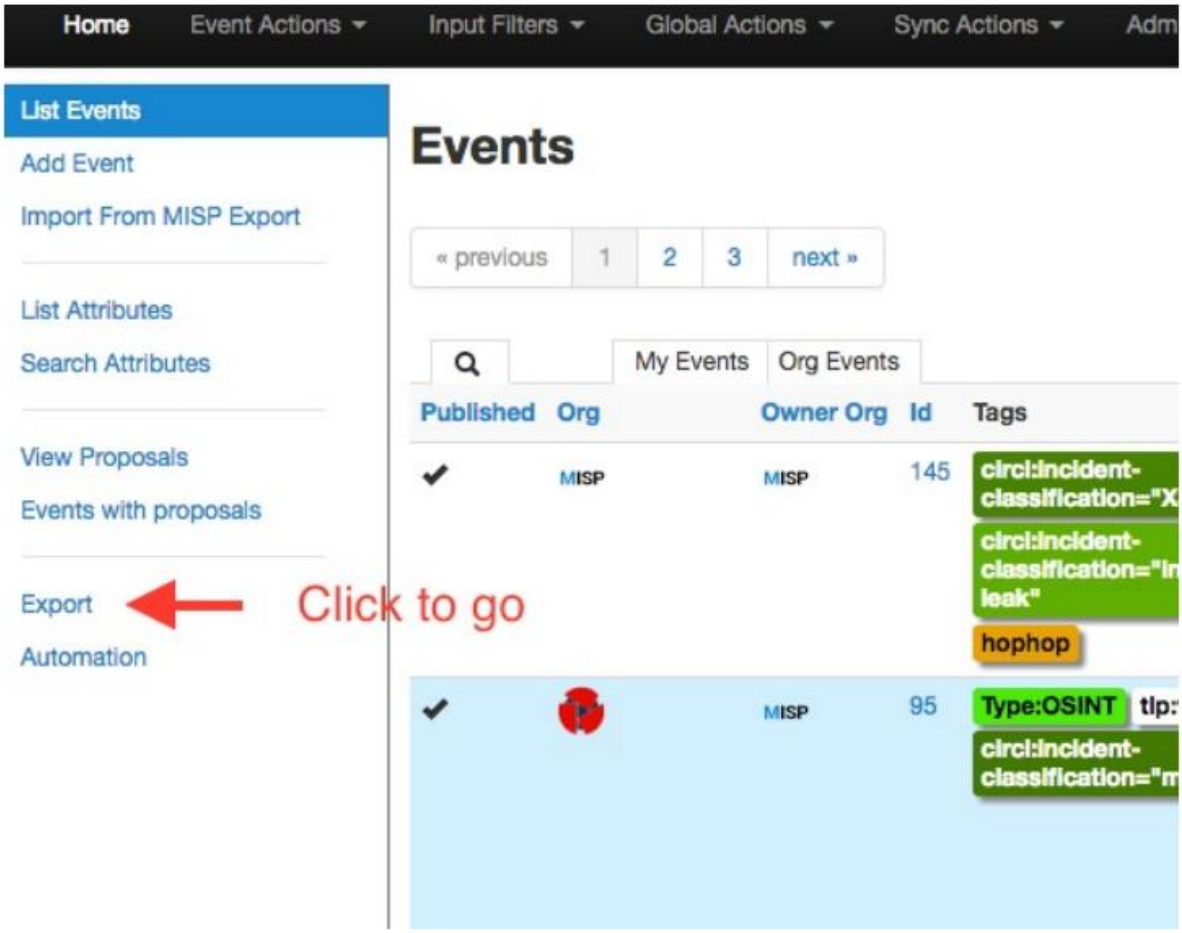


If you click on your Event's number, you can see all the information related to your Event.

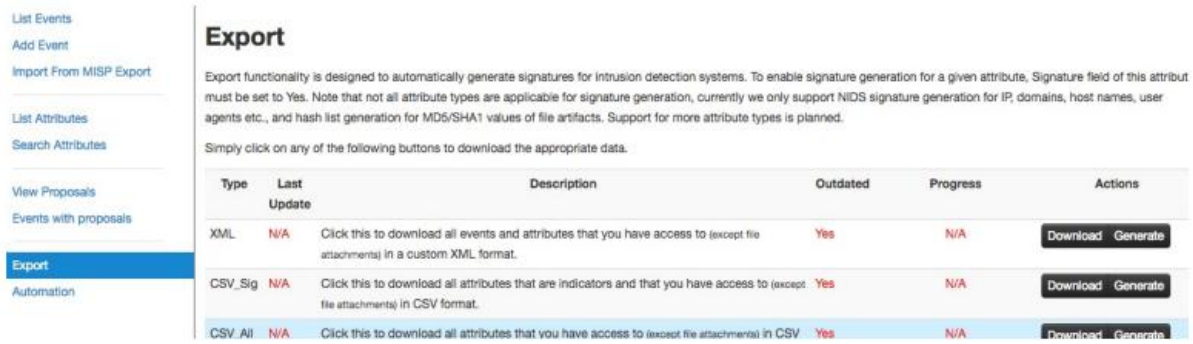


Export Events for Log Search

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.



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



THANK YOU