Extending MISP with Python modules

MISP - Threat Sharing

CIRCL / Team MISP Project

http://www.misp-project.org/
Twitter: *@MISPProject*

13th ENISA-EC3 Workshop

2024-10-02

Extending MISP with Python modules

Extending MISP with Python modules

MISP - Threat Sharing

CIRCL / Team MISP Project

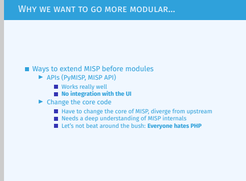
http://www.misp-project.org/
Twitter: *@MISPProject*

13th ENISA-EC3 Workshop

Why we want to go more modular...

- Ways to extend MISP before modules
  - APIs (PyMISP, MISP API)
    - Works really well
    - **No integration with the UI**
  - Change the core code
    - Have to change the core of MISP, diverge from upstream
    - Needs a deep understanding of MISP internals
    - Let’s not beat around the bush: **Everyone hates PHP**

└─Why we want to go more modular...



Why we want to go more modular...

- Ways to extend MISP before modules
  - APIs (PyMISP, MISP API)
    - Works really well
    - **No integration with the UI**
  - Change the core code
    - Have to change the core of MISP, diverge from upstream
    - Needs a deep understanding of MISP internals
    - Let’s not beat around the bush: **Everyone hates PHP**

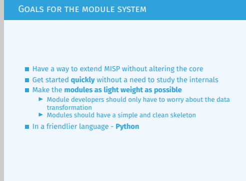
Goals for the module system

- Have a way to extend MISP without altering the core
- Get started **quickly** without a need to study the internals
- Make the **modules as light weight as possible**
  - Module developers should only have to worry about the data transformation
  - Modules should have a simple and clean skeleton
- In a friendlier language - **Python**

2024-10-02

Extending MISP with Python modules

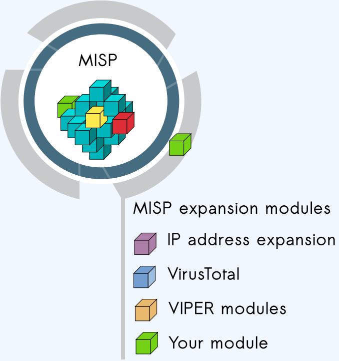
└Goals for the module system



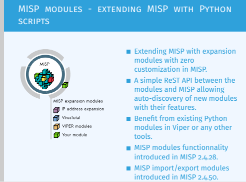
Goals for the module system

- Have a way to extend MISP without altering the core
- Get started **quickly** without a need to study the internals
- Make the **modules as light weight as possible**
  - Module developers should only have to worry about the data transformation
  - Modules should have a simple and clean skeleton
- In a friendlier language - **Python**

MISP modules - extending MISP with Python scripts



- Extending MISP with expansion modules with zero customization in MISP.
- A simple ReST API between the modules and MISP allowing auto-discovery of new modules with their features.
- Benefit from existing Python modules in Viper or any other tools.
- MISP modules functionnality introduced in MISP 2.4.28.
- MISP import/export modules introduced in MISP 2.4.50.


MISP modules - extending MISP with Python scripts

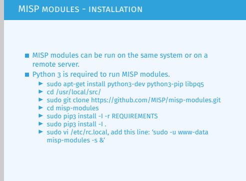
- Extending MISP with expansion modules with zero customization in MISP.
- A simple ReST API between the modules and MISP allowing auto-discovery of new modules with their features.
- Benefit from existing Python modules in Viper or any other tools.
- MISP modules functionnality introduced in MISP 2.4.28.
- MISP import/export modules introduced in MISP 2.4.50.

MISP MODULES - INSTALLATION

- MISP modules can be run on the same system or on a remote server.
- Python 3 is required to run MISP modules.
  - sudo apt-get install python3-dev python3-pip libpq5
  - cd /usr/local/src/
  - sudo git clone https://github.com/MISP/misp-modules.git
  - cd misp-modules
  - sudo pip3 install -I -r REQUIREMENTS
  - sudo pip3 install -I .
  - sudo vi /etc/rc.local, add this line: ‘sudo -u www-data misp-modules -s &‘

2024-10-02

└─MISP modules - installation

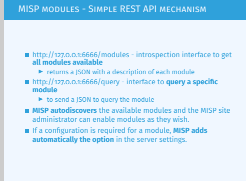


MISP MODULES - INSTALLATION

- MISP modules can be run on the same system or on a remote server.
- Python 3 is required to run MISP modules.
  - sudo apt-get install python3-dev python3-pip libpq5
  - cd /usr/local/src/
  - sudo git clone https://github.com/MISP/misp-modules.git
  - cd misp-modules
  - sudo pip3 install -I -r REQUIREMENTS
  - sudo pip3 install -I .
  - sudo vi /etc/rc.local, add this line: ‘sudo -u www-data misp-modules -s &‘

MISP modules - Simple REST API mechanism

- http://127.0.0.1:6666/modules - introspection interface to get **all modules available**
  - returns a JSON with a description of each module
- http://127.0.0.1:6666/query - interface to **query a specific module**
  - to send a JSON to query the module
- **MISP autodiscovers** the available modules and the MISP site administrator can enable modules as they wish.
- If a configuration is required for a module, **MISP adds automatically the option** in the server settings.



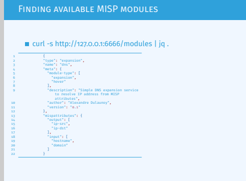
MISP modules - Simple REST API mechanism

- http://127.0.0.1:6666/modules - introspection interface to get **all modules available**
  - returns a JSON with a description of each module
- http://127.0.0.1:6666/query - interface to **query a specific module**
  - to send a JSON to query the module
- **MISP autodiscovers** the available modules and the MISP site administrator can enable modules as they wish.
- If a configuration is required for a module, **MISP adds automatically the option** in the server settings.

Finding available MISP modules

- curl -s http://127.0.0.1:6666/modules | jq .

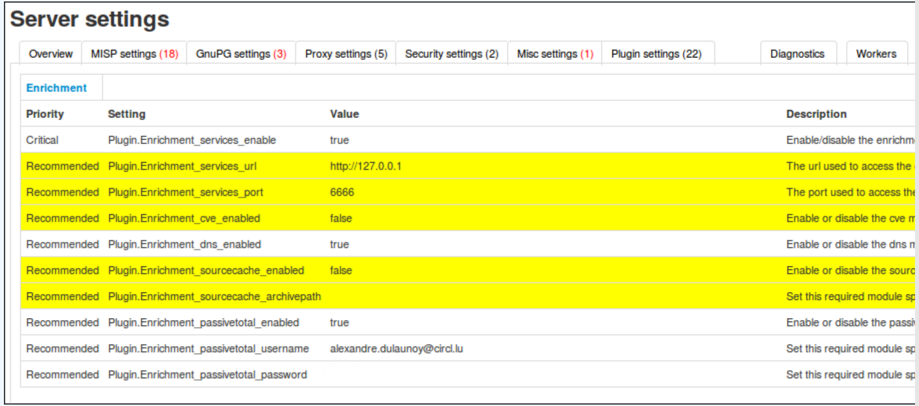
```
{
"type": "expansion",
"name": "dns",
"meta": {
  "module-type": [
    "expansion",
    "hover"
  ],
  "description": "Simple DNS expansion service
      to resolve IP address from MISP
      attributes",
  "author": "Alexandre Dulaunoy",
  "version": "0.1"
},
"mispattributes": {
  "output": [
    "ip-src",
    "ip-dst"
  ],
  "input": [
    "hostname",
    "domain"
  ]
}
```



Finding available MISP modules

curl -s http://127.0.0.1:6666/modules | jq .

MISP MODULES - CONFIGURATION IN THE UI

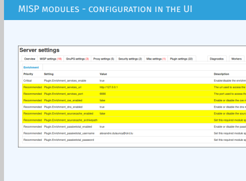


Server settings

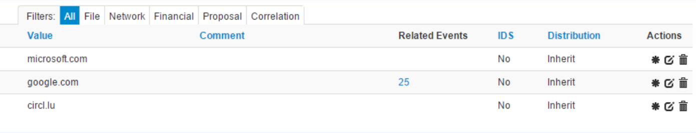
Overview | MISP settings (18) | GnuPG settings (3) | Proxy settings (5) | Security settings (2) | Misc settings (1) | Plugin settings (22) | Diagnostics | Workers

Enrichment

Priority	Setting	Value	Description
Critical	Plugin.Enrichment_services_enable	true	Enable/disable the enrichm
Recommended	Plugin.Enrichment_services_url	http://127.0.0.1	The url used to access the
Recommended	Plugin.Enrichment_services_port	6666	The port used to access the
Recommended	Plugin.Enrichment_cve_enabled	false	Enable or disable the cve m
Recommended	Plugin.Enrichment_dns_enabled	true	Enable or disable the dns m
Recommended	Plugin.Enrichment_sourcecache_enabled	false	Enable or disable the sourc
Recommended	Plugin.Enrichment_sourcecache_archivepath		Set this required module sp
Recommended	Plugin.Enrichment_passivetotal_enabled	true	Enable or disable the passi
Recommended	Plugin.Enrichment_passivetotal_username	alexandre.dulaunoy@circl.lu	Set this required module sp
Recommended	Plugin.Enrichment_passivetotal_password		Set this required module sp

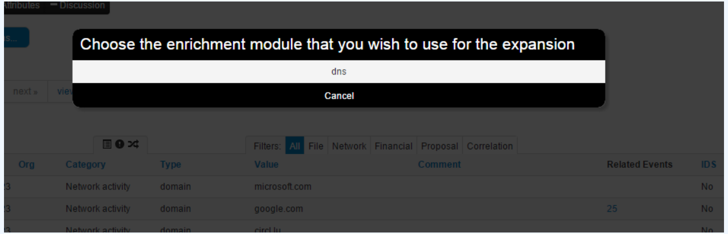


MISP modules - How it's integrated in the UI?



Filters: All File Network Financial Proposal Correlation

Value	Comment	Related Events	IDS	Distribution	Actions
microsoft.com			No	Inherit	
google.com		25	No	Inherit	
circl.lu			No	Inherit	



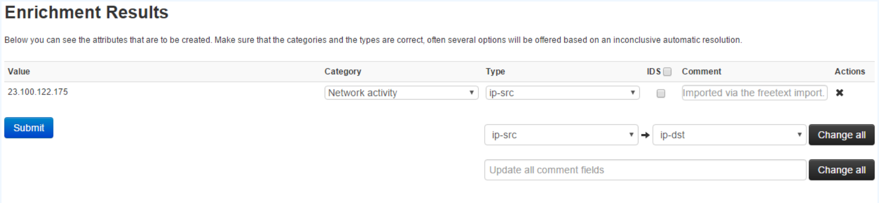
Choose the enrichment module that you wish to use for the expansion

dns

Cancel

Filters: All File Network Financial Proposal Correlation

Org	Category	Type	Value	Comment	Related Events	IDS
3	Network activity	domain	microsoft.com			No
3	Network activity	domain	google.com		25	No
3	Network activity	domain	circl.lu			No



Enrichment Results

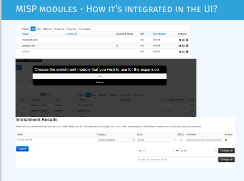
Below you can see the attributes that are to be created. Make sure that the categories and the types are correct, often several options will be offered based on an inconclusive automatic resolution.

Value	Category	Type	IDS □	Comment	Actions
23.100.122.175	Network activity	ip-src	□	Imported via the freetext import.	✖

Submit

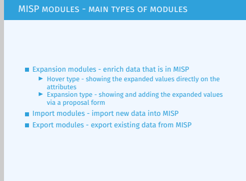
ip-src → ip-dst Change all

Update all comment fields Change all



MISP MODULES - MAIN TYPES OF MODULES

- Expansion modules - enrich data that is in MISP
  - Hover type - showing the expanded values directly on the attributes
  - Expansion type - showing and adding the expanded values via a proposal form
- Import modules - import new data into MISP
- Export modules - export existing data from MISP



MISP MODULES - MAIN TYPES OF MODULES

- Expansion modules - enrich data that is in MISP
  - Hover type - showing the expanded values directly on the attributes
  - Expansion type - showing and adding the expanded values via a proposal form
- Import modules - import new data into MISP
- Export modules - export existing data from MISP

Querying a module

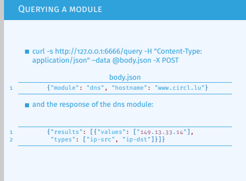
- curl -s http://127.0.0.1:6666/query -H "Content-Type: application/json" –data @body.json -X POST

body.json

```
{"module": "dns", "hostname": "www.circl.lu"}
```

- and the response of the dns module:

```
{"results": [{"values": ["149.13.33.14"],
 "types": ["ip-src", "ip-dst"]}]}
```



Querying a module

- curl -s http://127.0.0.1:6666/query -H "Content-Type: application/json" –data @body.json -X POST

body.json

{"module": "dns", "hostname": "www.circl.lu"}

- and the response of the dns module:

{"results": [{"values": ["149.13.33.14"],
 "types": ["ip-src", "ip-dst"]}]}

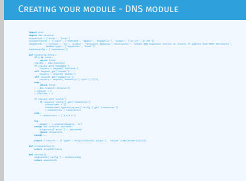
Creating your module - DNS module

```
import json
import dns.resolver
misperrors = {’error’: ’Error’}
mispattributes = {’input’: [’hostname’, ’domain’, ’domain|ip’], ’output’: [’ip-src’,’ip-dst’]}
moduleinfo = {’version’: ’0.3’, ’author’: ’Alexandre Dulaunoy’,’description’: ’Simple DNS expansion service to resolve IP address from MISP attributes’,
            ’module-type’: [’expansion’, ’hover’]}
moduleconfig = [’nameserver’]

def handler(q=False):
    if q is False:
        return False
    request = json.loads(q)
    if request.get(’hostname’):
        toquery = request[’hostname’]
    elif request.get(’domain’):
        toquery = request[’domain’]
    elif request.get(’domain|ip’):
        toquery = request[’domain|ip’].split(’|’)[0]
    else:
        return False
    r = dns.resolver.Resolver()
    r.timeout = 2
    r.lifetime = 2

    if request.get(’config’):
        if request[’config’].get(’nameserver’):
            nameservers = []
            nameservers.append(request[’config’].get(’nameserver’))
            r.nameservers = nameservers
    else:
        r.nameservers = [’8.8.8.8’]

    try:
        answer = r.resolve(toquery, ’A’)
    except dns.resolver.NXDOMAIN:
        misperrors[’error’] = "NXDOMAIN"
        return misperrors
    except ...

    return {’results’: [{’types’: mispattributes[’output’], ’values’:[str(answer[0])]}]}

def introspection():
    return mispattributes

def version():
    moduleinfo[’config’] = moduleconfig
    return moduleinfo
```

2024-10-02

Extending MISP with Python modules

└Creating your module - DNS module

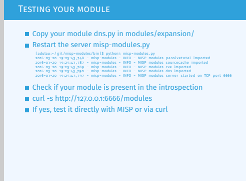


TESTING YOUR MODULE

- Copy your module dns.py in modules/expansion/
- Restart the server misp-modules.py

```
[adulau:~/git/misp-modules/bin]$ python3 misp-modules.py
2016-03-20 19:25:43,748 - misp-modules - INFO - MISP modules passivetotal imported
2016-03-20 19:25:43,787 - misp-modules - INFO - MISP modules sourcecache imported
2016-03-20 19:25:43,789 - misp-modules - INFO - MISP modules cve imported
2016-03-20 19:25:43,790 - misp-modules - INFO - MISP modules dns imported
2016-03-20 19:25:43,797 - misp-modules - INFO - MISP modules server started on TCP port 6666
```

- Check if your module is present in the introspection
- curl -s http://127.0.0.1:6666/modules
- If yes, test it directly with MISP or via curl



TESTING YOUR MODULE

- Copy your module dns.py in modules/expansion/
- Restart the server misp-modules.py

```
[adulau:~/git/misp-modules/bin]$ python3 misp-modules.py
2016-03-20 19:25:43,748 - misp-modules - INFO - MISP modules passivetotal imported
2016-03-20 19:25:43,787 - misp-modules - INFO - MISP modules sourcecache imported
2016-03-20 19:25:43,789 - misp-modules - INFO - MISP modules cve imported
2016-03-20 19:25:43,790 - misp-modules - INFO - MISP modules dns imported
2016-03-20 19:25:43,797 - misp-modules - INFO - MISP modules server started on TCP port 6666
```

- Check if your module is present in the introspection
- curl -s http://127.0.0.1:6666/modules
- If yes, test it directly with MISP or via curl

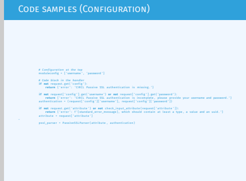
Code samples (Configuration)

```
# Configuration at the top
moduleconfig = ['username', 'password']

# Code block in the handler
if not request.get('config'):
    return {'error': 'CIRCL Passive SSL authentication is missing.'}

if not request['config'].get('username') or not request['config'].get('password'):
    return {'error': 'CIRCL Passive SSL authentication is incomplete, please provide your username and password.'}
authentication = (request['config']['username'], request['config']['password'])

if not request.get('attribute') or not check_input_attribute(request['attribute']):
    return {'error': f'{standard_error_message}, which should contain at least a type, a value and an uuid.'}
attribute = request['attribute']

pssl_parser = PassiveSSLParser(attribute, authentication)
```

2024-10-02

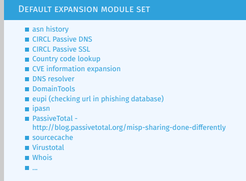
Extending MISP with Python modules

└Code samples (Configuration)



Default expansion module set

- asn history
- CIRCL Passive DNS
- CIRCL Passive SSL
- Country code lookup
- CVE information expansion
- DNS resolver
- DomainTools
- eupi (checking url in phishing database)
- ipasn
- PassiveTotal - http://blog.passivetotal.org/misp-sharing-done-differently
- sourcecache
- Virustotal
- Whois
- ...

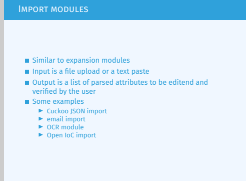


Default expansion module set

- asn history
- CIRCL Passive DNS
- CIRCL Passive SSL
- Country code lookup
- CVE information expansion
- DNS resolver
- DomainTools
- eupi (checking url in phishing database)
- ipasn
- PassiveTotal - http://blog.passivetotal.org/misp-sharing-done-differently
- sourcecache
- Virustotal
- Whois
- ...

Import modules

- Similar to expansion modules
- Input is a file upload or a text paste
- Output is a list of parsed attributes to be editend and verified by the user
- Some examples
  - Cuckoo JSON import
  - email import
  - OCR module
  - Open IoC import

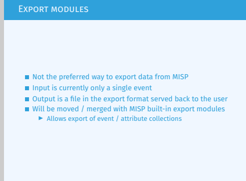


Import modules

- Similar to expansion modules
- Input is a file upload or a text paste
- Output is a list of parsed attributes to be editend and verified by the user
- Some examples
  - Cuckoo JSON import
  - email import
  - OCR module
  - Open IoC import

Export modules

- Not the preferred way to export data from MISP
- Input is currently only a single event
- Output is a file in the export format served back to the user
- Will be moved / merged with MISP built-in export modules
    - Allows export of event / attribute collections



Export modules

- Not the preferred way to export data from MISP
- Input is currently only a single event
- Output is a file in the export format served back to the user
- Will be moved / merged with MISP built-in export modules
    - Allows export of event / attribute collections

New expansion & import modules format

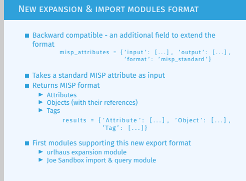
- Backward compatible - an additional field to extend the format

```
misp_attributes = {'input': [...], 'output': [...],
                   'format': 'misp_standard'}
```

- Takes a standard MISP attribute as input
- Returns MISP format
  - Attributes
  - Objects (with their references)
  - Tags

```
results = {'Attribute': [...], 'Object': [...],
           'Tag': [...]}
```

- First modules supporting this new export format
  - urlhaus expansion module
  - Joe Sandbox import & query module



New expansion & import modules format

- Backward compatible - an additional field to extend the format

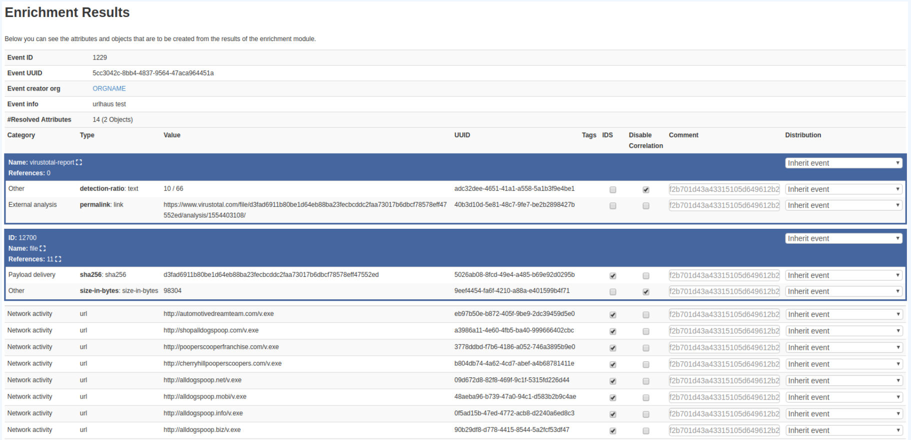
```
misp_attributes = {'input': [...], 'output': [...],
                   'format': 'misp_standard'}
```

- Takes a standard MISP attribute as input
- Returns MISP format
  - Attributes
  - Objects (with their references)
  - Tags

```
results = {'Attribute': [...], 'Object': [...],
           'Tag': [...]}
```

- First modules supporting this new export format
  - urlhaus expansion module
  - Joe Sandbox import & query module

NEW EXPANSION & IMPORT MODULES VIEW (MISP 2.4.110)



Enrichment Results

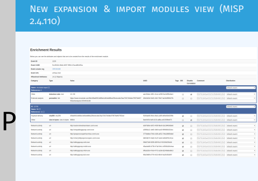
Below you can see the attributes and objects that are to be created from the results of the enrichment module.

Event ID	1229
Event UUID	5cc3042c-8bb4-4837-9564-47aca964451a
Event creator org	ORGNAME
Event info	urlhaus test
#Resolved Attributes	14 (2 Objects)

Category	Type	Value	UUID	Tags	IDS	Disable Correlation	Comment	Distribution
Name: virustotal-report **References:** 0								Inherit event ▾
Other	**detection-ratio**: text	10 / 66	adc32dee-4651-41a1-a558-5a1b3f9e4be1		☐	☑	f2b701d43a43315105d649612b2	Inherit event ▾
External analysis	**permalink**: link	https://www.virustotal.com/file/d3fad6911b80be1d64eb88ba23fecbcddc2faa73017b6dbcf78578eff47552ed/analysis/1554403108/	40b3d10d-5e81-48c7-9fe7-be2b2898427b		☐	☐	f2b701d43a43315105d649612b2	Inherit event ▾
ID: 12700 **Name:** file **References:** 11								Inherit event ▾
Payload delivery	**sha256**: sha256	d3fad6911b80be1d64eb88ba23fecbcddc2faa73017b6dbcf78578eff47552ed	5026ab08-8fcd-49e4-a485-b69e92d0295b		☑	☐	f2b701d43a43315105d649612b2	Inherit event ▾
Other	**size-in-bytes**: size-in-bytes	98304	9eef4454-fa6f-4210-a88a-e401599b4f71		☐	☑	f2b701d43a43315105d649612b2	Inherit event ▾
Network activity	url	http://automotivedreamteam.com/v.exe	eb97b50e-b872-405f-9be9-2dc39459d5e0		☑	☐	f2b701d43a43315105d649612b2	Inherit event ▾
Network activity	url	http://shopalldogspoop.com/v.exe	a3986a11-4e60-4fb5-ba40-999666402cbc		☑	☐	f2b701d43a43315105d649612b2	Inherit event ▾
Network activity	url	http://pooperscooperfranchise.com/v.exe	3778ddbd-f7b6-4186-a052-746a3895b9e0		☑	☐	f2b701d43a43315105d649612b2	Inherit event ▾
Network activity	url	http://cherryhillpooperscoopers.com/v.exe	b804db74-4a62-4cd7-abef-a4b68781411e		☑	☐	f2b701d43a43315105d649612b2	Inherit event ▾
Network activity	url	http://alldogspoop.net/v.exe	09d672d8-82f8-469f-9c1f-5315fd226d44		☑	☐	f2b701d43a43315105d649612b2	Inherit event ▾
Network activity	url	http://alldogspoop.mobi/v.exe	48aeba96-b739-47a0-94c1-d583b2b9c4ae		☑	☐	f2b701d43a43315105d649612b2	Inherit event ▾
Network activity	url	http://alldogspoop.info/v.exe	0f5ad15b-47ed-4772-acb8-d2240a6ed8c3		☑	☐	f2b701d43a43315105d649612b2	Inherit event ▾
Network activity	url	http://alldogspoop.biz/v.exe	90b29df8-d778-4415-8544-5a2fcf53df47		☑	☐	f2b701d43a43315105d649612b2	Inherit event ▾

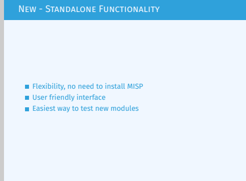
Extending MISP with Python modules

└─New expansion & import modules view (MISP 2.4.110)



New - Standalone Functionality

- Flexibility, no need to install MISP
- User friendly interface
- Easiest way to test new modules

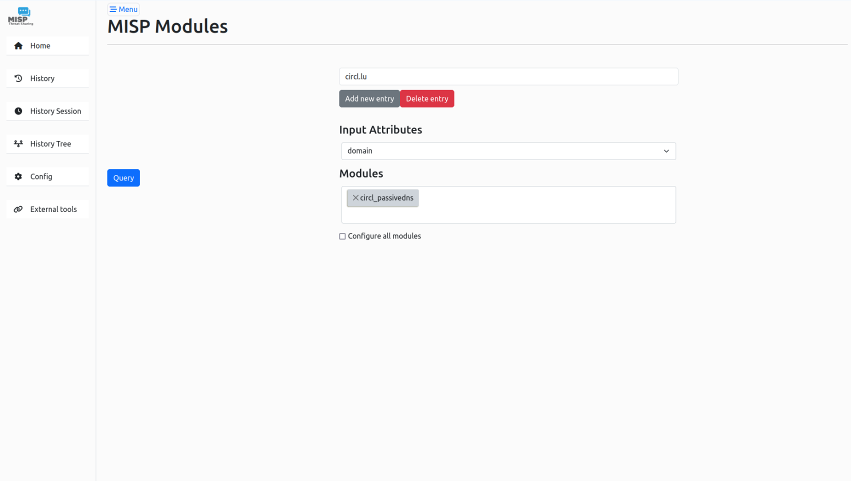


New - Standalone Functionality

- Flexibility, no need to install MISP
- User friendly interface
- Easiest way to test new modules

Web interface - Query

- Add multiple entries
- Choose different modules



MISP Modules

circl.lu

Add new entry Delete entry

Input Attributes

domain

Modules

× circl_passivedns

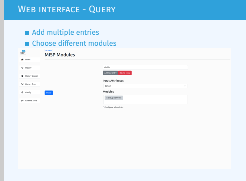
□ Configure all modules

Query

2024-10-02

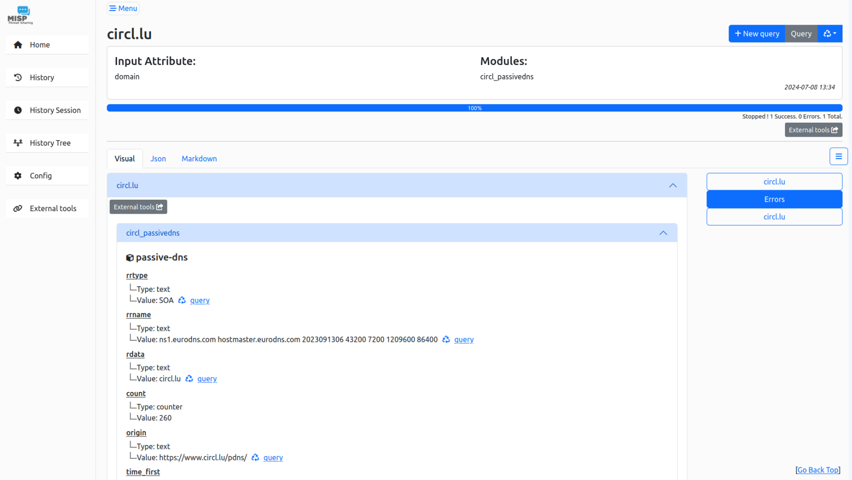
Extending MISP with Python modules

└─Web interface - Query



Web interface - Results

- Multiple tabs for visualization in different formats



circl.lu

Input Attribute:
domain

Modules:
circl_passivedns

2024-07-08 13:34

100%

Stopped ! 1 Success. 0 Errors. 1 Total.

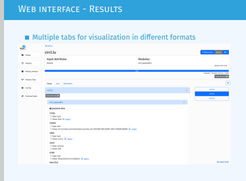
passive-dns

```
rrtype
 └Type: text
 └Value: SOA  query
rrname
 └Type: text
 └Value: ns1.eurodns.com hostmaster.eurodns.com 2023091306 43200 7200 1209600 86400  query
rdata
 └Type: text
 └Value: circl.lu  query
count
 └Type: counter
 └Value: 260
origin
 └Type: text
 └Value: https://www.circl.lu/pdns/  query
time_first
```

2024-10-02

Extending MISP with Python modules

└Web interface - Results

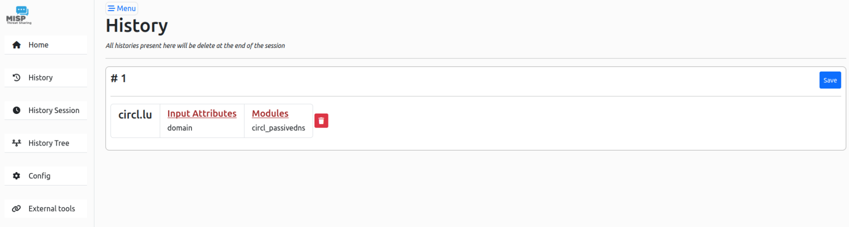


Web interface - Results

Multiple tabs for visualization in different formats

Web interface - History

- Save your researches and pivot from them



History

All histories present here will be delete at the end of the session

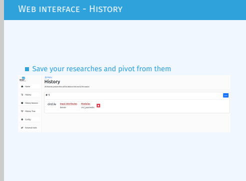
1

circl.lu	Input Attributes	Modules
	domain	circl_passivedns

2024-10-02

Extending MISP with Python modules

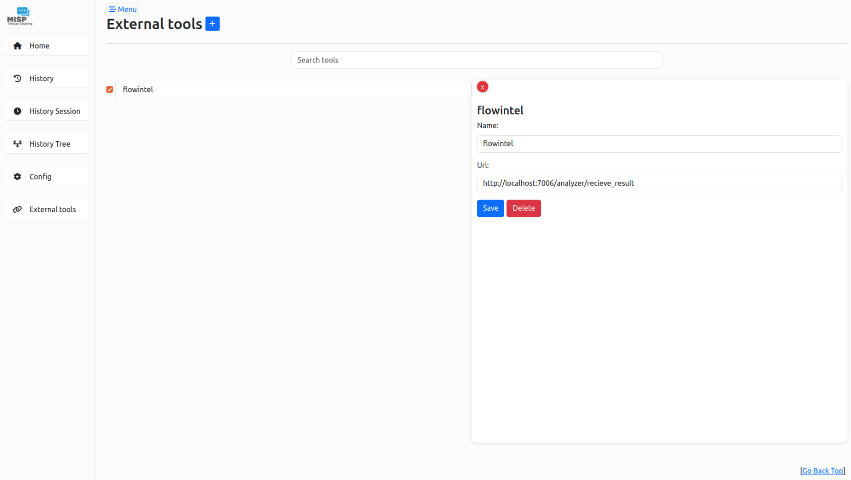
└Web interface - History


Web interface - History

Save your researches and pivot from them

Web interface - External tools (Dev)

- Export results to other tools. (Still in dev)



External tools

Search tools

☑ flowintel

flowintel

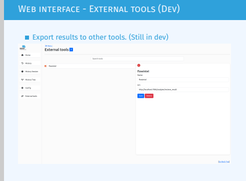
Name: flowintel

Url: http://localhost:7006/analyzer/recieve_result

Extending MISP with Python modules

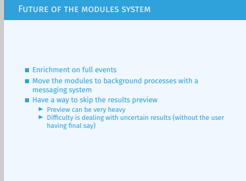
2024-10-02

└Web interface - External tools (Dev)


Web interface - External tools (Dev)
Export results to other tools. (Still in dev)

Future of the modules system

- Enrichment on full events
- Move the modules to background processes with a messaging system
- Have a way to skip the results preview
    - Preview can be very heavy
    - Difficulty is dealing with uncertain results (without the user having final say)



Future of the modules system

- Enrichment on full events
- Move the modules to background processes with a messaging system
- Have a way to skip the results preview
    - Preview can be very heavy
    - Difficulty is dealing with uncertain results (without the user having final say)

Q&A

Threat Sharing

- https://github.com/MISP/misp-modules
- https://github.com/MISP/
- We welcome new modules and pull requests.
- MISP modules can be designed as standalone application.

Extending MISP with Python modules

2024-10-02

└Q&A

Q&A

Threat Sharing

- https://github.com/MISP/misp-modules
- https://github.com/MISP/
- We welcome new modules and pull requests.
- MISP modules can be designed as standalone application.