

EXTENDING MISP WITH PYTHON MODULES

MISP - THREAT SHARING

CIRCL / TEAM MISP PROJECT

[HTTP://WWW.MISP-PROJECT.ORG/](http://www.misp-project.org/)

TWITTER: @MISPPROJECT

13TH ENISA-EC3 WORKSHOP



Extending MISP with Python modules

2024-10-02

EXTENDING MISP WITH PYTHON MODULES

MISP - THREAT SHARING

CIRCL / Team MISP Project

[HTTP://WWW.MISP-PROJECT.ORG/](http://www.misp-project.org/)
TWITTER: @MISPPROJECT

13TH ENISA-EC3 WORKSHOP



■ 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**

2024-10-02

└ 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**

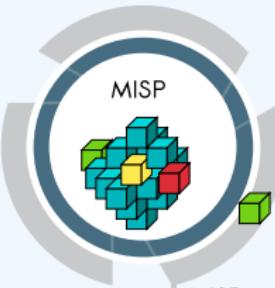
- Have a way to extend MISP without altering the core
- Get started **quickly** without a need to study the internals
- Make the **modules as light weight as possible**
 - ▶ Module developers should only have to worry about the data transformation
 - ▶ Modules should have a simple and clean skeleton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

2024-10-02

└ 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



MISP expansion modules

- IP address expansion
- VirusTotal
- VIPER modules
- Your module

- 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.

Extending MISP with Python modules

2024-10-02

└ MISP modules - extending MISP with Python scripts



- 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 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 &'

- <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.

2024-10-02

└ 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.

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

```
1   {
2     "type": "expansion",
3     "name": "dns",
4     "meta": {
5       "module-type": [
6         "expansion",
7         "hover"
8       ],
9       "description": "Simple DNS expansion service
10      to resolve IP address from MISP
11      attributes",
12      "author": "Alexandre Dulaunoy",
13      "version": "0.1"
14    },
15    "mispattributes": {
16      "output": [
17        "ip-src",
18        "ip-dst"
19      ],
20      "input": [
21        "hostname",
22        "domain"
23      ]
24    }
25 }
```

2024-10-02

└ Finding available MISP modules

```
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"]}}
```

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 enrichment services module.								
Recommended	Plugin.Enrichment_services_url	http://127.0.0.1	The url used to access the enrichment services module.								
Recommended	Plugin.Enrichment_services_port	6666	The port used to access the enrichment services module.								
Recommended	Plugin.Enrichment_cve_enabled	false	Enable or disable the cve module.								
Recommended	Plugin.Enrichment_dns_enabled	true	Enable or disable the dns module.								
Recommended	Plugin.Enrichment_sourcecache_enabled	false	Enable or disable the sourcecache module.								
Recommended	Plugin.Enrichment_sourcecache_archivepath		Set this required module specific path.								
Recommended	Plugin.Enrichment_passivetotal_enabled	true	Enable or disable the passivetotal module.								
Recommended	Plugin.Enrichment_passivetotal_username	alexandre.dulaunoy@circl.lu	Set this required module specific username.								
Recommended	Plugin.Enrichment_passivetotal_password		Set this required module specific password.								

Extending MISP with Python modules

2024-10-02

└ MISP modules - configuration in the UI



MISP MODULES - HOW IT'S INTEGRATED IN THE UI?

The screenshot shows the MISP web interface. At the top, there's a navigation bar with filters: All, File, Network, Financial, Proposal, Correlation. Below it is a table with columns: Value, Comment, Related Events, ID\$ (with a checkbox), Distribution (with a checkbox), and Actions (with three icons). The table contains three rows: microsoft.com, google.com, and circl.lu. Below this is a modal dialog titled "Choose the enrichment module that you wish to use for the expansion". Inside the modal, there's a single option: "dns". At the bottom of the modal is a "Cancel" button. Below the modal is another table with columns: Org, Category, Type, Value, Comment, Related Events, and ID\$. It has three rows: Network activity, domain, microsoft.com; Network activity, domain, google.com; and Network activity, domain, circl.lu. At the bottom of the page is a section titled "Enrichment Results" with a note: "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." It shows a table with a single row: Value (23.100.122.175), Category (Network activity), Type (ip-src), ID\$ (checkbox checked), Comment (imported via the freetext import), and Actions (checkbox checked). There are also dropdown menus for Category and Type, and buttons for "Submit", "Change all", and "Update all comment fields".

Extending MISP with Python modules

2024-10-02

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

The screenshot shows the MISP web interface. At the top, there's a navigation bar with filters: All, File, Network, Financial, Proposal, Correlation. Below it is a table with columns: Value, Comment, Related Events, ID\$, Distribution, and Actions. The table contains three rows: microsoft.com, google.com, and circl.lu. Below this is a section titled "Choose the enrichment module that you wish to use for the expansion". Inside the section, there's a dropdown menu with the option "dns". At the bottom of the section is a "Cancel" button. Below the section is another table with columns: Org, Category, Type, Value, Comment, Related Events, and ID\$. It has three rows: Network activity, domain, microsoft.com; Network activity, domain, google.com; and Network activity, domain, circl.lu. At the bottom of the page is a section titled "Enrichment Results" with a note: "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." It shows a table with a single row: Value (23.100.122.175), Category (Network activity), Type (ip-src), ID\$ (checkbox checked), Comment (imported via the freetext import), and Actions (checkbox checked). There are also dropdown menus for Category and Type, and buttons for "Submit", "Change all", and "Update all comment fields".

- 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

2024-10-02

└ 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

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

body.json

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

- and the response of the dns module:

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

2024-10-02

Querying a module

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"]}]}
```

```
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']

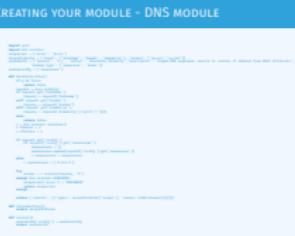
    try:
        answer = r.resolve(tquery, 'A')
    except dns.resolver.NXDOMAIN:
        misperrors['error'] = "NXDOMAIN"
        return misperrors
    except ...
    return {'results': [{}{'types': mispattributes['output'], 'values':str(answer[0])}]}

def introspection():
    return mispattributes

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

2024-10-02

└ 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

Extending MISP with Python modules

2024-10-02

└ Testing your 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

```
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 = PassiveSSLPParser(attribute, authentication)
```

2024-10-02

## └ 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
- ...

## Extending MISP with Python modules

2024-10-02

### └ Default expansion module set

| DEFAULT EXPANSION MODULE SET                                                                                                                            |                                                                                                                                                         |
|---------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|
| ■ asn history                                                                                                                                           | ■ CIRCL Passive DNS                                                                                                                                     |
| ■ CIRCL Passive SSL                                                                                                                                     | ■ Country code lookup                                                                                                                                   |
| ■ CVE information expansion                                                                                                                             | ■ DNS resolver                                                                                                                                          |
| ■ DNS resolver                                                                                                                                          | ■ DomainTools                                                                                                                                           |
| ■ DomainTools                                                                                                                                           | ■ eupi (checking url in phishing database)                                                                                                              |
| ■ eupi (checking url in phishing database)                                                                                                              | ■ ipasn                                                                                                                                                 |
| ■ ipasn                                                                                                                                                 | ■ PassiveTotal -<br><a href="http://blog.passivetotal.org/misp-sharing-done-differently">http://blog.passivetotal.org/misp-sharing-done-differently</a> |
| ■ PassiveTotal -<br><a href="http://blog.passivetotal.org/misp-sharing-done-differently">http://blog.passivetotal.org/misp-sharing-done-differently</a> | ■ sourcecache                                                                                                                                           |
| ■ sourcecache                                                                                                                                           | ■ Virustotal                                                                                                                                            |
| ■ Virustotal                                                                                                                                            | ■ Whois                                                                                                                                                 |
| ■ Whois                                                                                                                                                 | ■ ...                                                                                                                                                   |

- 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

2024-10-02

## └ 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

2024-10-02

### └ 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

# Extending MISP with Python modules

2024-10-02

## └ New expansion & import modules format

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
  - ▶ 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.

| Category                | Type                         | Value                                                                                                                                                                                                                                                     | UUID                                 | Tags                                | IDS                                 | Disable Correlation      | Comment                     | Distribution  |
|-------------------------|------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------|-------------------------------------|-------------------------------------|--------------------------|-----------------------------|---------------|
| Name: virustotal-report |                              |                                                                                                                                                                                                                                                           |                                      |                                     |                                     |                          |                             |               |
| References: 0           |                              |                                                                                                                                                                                                                                                           |                                      |                                     |                                     |                          |                             |               |
| Other                   |                              |                                                                                                                                                                                                                                                           |                                      |                                     |                                     |                          |                             |               |
| External analysis       | detection-ratio: text        | 10 / 66                                                                                                                                                                                                                                                   | ad:32d9e-4651-41a1-a550-5a1b39fe4be1 | <input type="checkbox"/>            | <input checked="" type="checkbox"/> | <input type="checkbox"/> | f2b701d43a43315105d649612b2 | Inherit event |
| External analysis       | permalink: link              | <a href="https://www.virustotal.com/file/d3fd6911b00e1d64eb08a29fecc0dc2f1aa73017b6d0cf78579ef47552ed552edanalysis/1554403108/">https://www.virustotal.com/file/d3fd6911b00e1d64eb08a29fecc0dc2f1aa73017b6d0cf78579ef47552ed552edanalysis/1554403108/</a> | 40b3d105-5e01-48c7-94e7-be2b289427b  | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/> | f2b701d43a43315105d649612b2 | Inherit event |
| ID: 12700               |                              |                                                                                                                                                                                                                                                           |                                      |                                     |                                     |                          |                             |               |
| Name: file              |                              |                                                                                                                                                                                                                                                           |                                      |                                     |                                     |                          |                             |               |
| References: 0           |                              |                                                                                                                                                                                                                                                           |                                      |                                     |                                     |                          |                             |               |
| Payload delivery        | sha256: sha256               | d3fd6911b00e1d64eb08a29fecc0dc2f1aa73017b6d0cf78579ef47552ed                                                                                                                                                                                              | 5026ab08-8fc8-49e4-a485-b69e92d02950 | <input checked="" type="checkbox"/> | <input type="checkbox"/>            | <input type="checkbox"/> | f2b701d43a43315105d649612b2 | Inherit event |
| Other                   | size-in-bytes: size-in-bytes | 98304                                                                                                                                                                                                                                                     | 9eeff454-fa8f-4210-a88a-e4d1569047f1 | <input type="checkbox"/>            | <input checked="" type="checkbox"/> | <input type="checkbox"/> | f2b701d43a43315105d649612b2 | Inherit event |
| Network activity        | url                          | <a href="http://automotivedreamteam.com/v.exe">http://automotivedreamteam.com/v.exe</a>                                                                                                                                                                   | e197650e-b872-405f-9be9-2d39459d5e0  | <input checked="" type="checkbox"/> | <input type="checkbox"/>            | <input type="checkbox"/> | f2b701d43a43315105d649612b2 | Inherit event |
| Network activity        | url                          | <a href="http://shopalldogscoop.com/v.exe">http://shopalldogscoop.com/v.exe</a>                                                                                                                                                                           | a399fa11-4e60-4f05-ba40-999664a02dbc | <input checked="" type="checkbox"/> | <input type="checkbox"/>            | <input type="checkbox"/> | f2b701d43a43315105d649612b2 | Inherit event |
| Network activity        | url                          | <a href="http://pooperscoopfranchise.com/v.exe">http://pooperscoopfranchise.com/v.exe</a>                                                                                                                                                                 | 3778ddbd-f7b6-4186-aa52-74a389569e0  | <input checked="" type="checkbox"/> | <input type="checkbox"/>            | <input type="checkbox"/> | f2b701d43a43315105d649612b2 | Inherit event |
| Network activity        | url                          | <a href="http://cherhillpooperscoops.com/v.exe">http://cherhillpooperscoops.com/v.exe</a>                                                                                                                                                                 | b834db74-4a82-4c07-abef-a4b68781411e | <input checked="" type="checkbox"/> | <input type="checkbox"/>            | <input type="checkbox"/> | f2b701d43a43315105d649612b2 | Inherit event |
| Network activity        | url                          | <a href="http://alldogscoop.net/v.exe">http://alldogscoop.net/v.exe</a>                                                                                                                                                                                   | 09d072d8-b2b6-4659-9c11-5315bf226d44 | <input checked="" type="checkbox"/> | <input type="checkbox"/>            | <input type="checkbox"/> | f2b701d43a43315105d649612b2 | Inherit event |
| Network activity        | url                          | <a href="http://alldogscoop.mobiv.exe">http://alldogscoop.mobiv.exe</a>                                                                                                                                                                                   | 4baea6b6-0739-47a0-94d1-d583b294e4e  | <input checked="" type="checkbox"/> | <input type="checkbox"/>            | <input type="checkbox"/> | f2b701d43a43315105d649612b2 | Inherit event |
| Network activity        | url                          | <a href="http://alldogscoop.info/v.exe">http://alldogscoop.info/v.exe</a>                                                                                                                                                                                 | 0f5ad15b-47ed-4772-acb8-d2240afed8c3 | <input checked="" type="checkbox"/> | <input type="checkbox"/>            | <input type="checkbox"/> | f2b701d43a43315105d649612b2 | Inherit event |
| Network activity        | url                          | <a href="http://alldogscoop.biz/v.exe">http://alldogscoop.biz/v.exe</a>                                                                                                                                                                                   | 90b29d18-d778-4415-8544-5a2fcf53d4f7 | <input checked="" type="checkbox"/> | <input type="checkbox"/>            | <input type="checkbox"/> | f2b701d43a43315105d649612b2 | Inherit event |

# Extending MISP with Python modules

2024-10-02

## New expansion & import modules view (MISP 2.4.110)

NEW EXPANSION & IMPORT MODULES VIEW (MISP 2.4.110)

The screenshot shows the 'Enrichment Results' section of the MISP interface. It displays a table with columns for Category, Type, Value, UUID, Tags, IDS, Disable Correlation, Comment, and Distribution. The table lists various enrichment results, such as 'virustotal-report' and 'file' entries, along with their corresponding UUIDs, tags, and distribution details. The 'Distribution' column includes dropdown menus like 'Inherit event'.

# NEW - STANDALONE FUNCTIONALITY

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

## Extending MISP with Python modules

2024-10-02

### └ 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

X circl\_passivedns

Configure all modules

# Extending MISP with Python modules

2024-10-02

## Web interface - Query

WEB INTERFACE - QUERY

Add multiple entries

Choose different modules

MISP Modules

circl\_passivedns

## WEB INTERFACE - RESULTS

### ■ Multiple tabs for visualization in different formats

The screenshot shows the MISP web interface with the following details:

- Left Sidebar:** Includes links for Home, History, History Session, History Tree, Config, and External tools.
- Header:** Shows the URL "circl.lu", the input attribute "domain", the module "cird\_passivedns", and a timestamp "2024-07-08 13:34".
- Content Area:** Features three tabs: Visual, Json, and Markdown. The Visual tab is selected, displaying a tree view of DNS records for "circl.lu". The tree includes nodes for "rrtype", "rname", "rdata", "count", "origin", and "time\_first". The "rrtype" node has children for "text" and "SOA". The "rname" node has a child for "ns1.eurodns.com". The "rdata" node has a child for "circ.lu". The "count" node has a value of 260. The "origin" node has a child for "https://www.circl.lu/pdns/".
- Right Panel:** Displays a summary of the query results: "Stopped 1 Success, 0 Errors, 1 Total". It also shows a "External tools" section with a single entry for "circl.lu".

21

## Extending MISP with Python modules

2024-10-02

### └ Web interface - Results

The screenshot shows the MISP web interface with the following details:

- Header:** Shows the URL "circl.lu", the input attribute "domain", the module "cird\_passivedns", and a timestamp "2024-07-08 13:34".
- Content Area:** Features three tabs: Visual, Json, and Markdown. The Visual tab is selected, displaying a tree view of DNS records for "circl.lu". The tree includes nodes for "rrtype", "rname", "rdata", "count", "origin", and "time\_first". The "rrtype" node has children for "text" and "SOA". The "rname" node has a child for "ns1.eurodns.com". The "rdata" node has a child for "circ.lu". The "count" node has a value of 260. The "origin" node has a child for "https://www.circl.lu/pdns/".
- Right Panel:** Displays a summary of the query results: "Stopped 1 Success, 0 Errors, 1 Total". It also shows a "External tools" section with a single entry for "circl.lu".

25

## ■ Save your researches and pivot from them

The screenshot shows the MISP web interface's History page. On the left is a sidebar with links: Home, History (which is selected), History Session, History Tree, Config, and External tools. The main content area has a header "History" with a sub-instruction "All histories present here will be deleted at the end of the session". Below this is a table with one row, labeled "# 1". The row contains three columns: "circl.lu" (highlighted in red), "Input Attributes" (highlighted in red), and "Modules" (highlighted in red). Under "Input Attributes" are the values "domain" and "circl\_passivedns". A "Save" button is located at the top right of the table row.

2024-10-02

## └ Web interface - History

The screenshot shows the MISP web interface's History page. At the top, there is a header "WEB INTERFACE - HISTORY" and a sub-header "Save your researches and pivot from them". The main content area displays a single history entry titled "history". The entry includes a "Save" button and a "Delete" button. The page also features a sidebar with various navigation links.

## ■ Export results to other tools. (Still in dev)

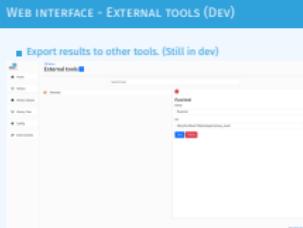
The screenshot shows the MISP web interface with a sidebar on the left containing links: Home, History, History Session, History Tree, Config, and External tools (which is currently selected). The main content area is titled "External tools" and contains a search bar labeled "Search tools". A single entry named "flowintel" is listed, with a red "x" icon to its left. The entry details are as follows:

- Name: flowintel
- Url: `http://localhost:7006/analyzer/receive_result`

At the bottom of the entry card are two buttons: "Save" and "Delete".

2024-10-02

## └ Web interface - External tools (Dev)



- 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)

2024-10-02

## └ 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)



- <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.

MISP  
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.

2024-10-02

└ Q&A