

# 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



2024-09-11

Extending MISP with Python modules

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



# 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**

## Extending MISP with Python modules

└ 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

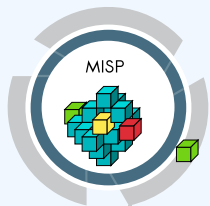
- Have a way to extend MISP without altering the core
- Get started **quickly** without a need to study the internals
- Make the **modules as light weight as possible**
  - ▶ Module developers should only have to worry about the data transformation
  - ▶ Modules should have a simple and clean skeleton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

## Extending MISP with Python modules

### └─ 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 functionality introduced in MISP 2.4.28.
- MISP import/export modules introduced in MISP 2.4.50.

## Extending MISP with Python modules

### └ MISP modules - extending MISP with Python scripts



MISP expansion modules

- 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 functionality introduced in MISP 2.4.28.
- MISP import/export modules introduced in MISP 2.4.50.

- 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 - 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.

### └─ 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 .`

```
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 }
```

## Extending MISP with Python modules

└─ Finding available MISP modules

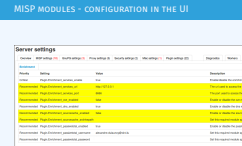
2024-09-11

```
■ 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 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				

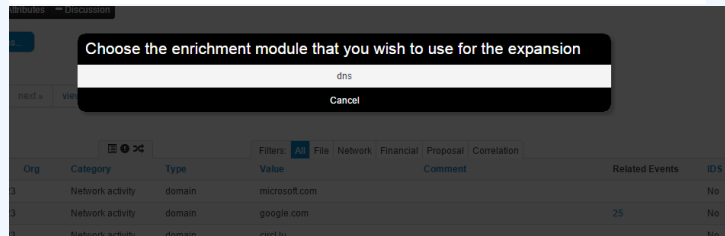
### └─ MISP modules - configuration in the UI





# 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	✖️🔗🗑️	



## 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	ID \$	Comment	Actions
23.100.122.175	Network activity	ip-src	<input type="checkbox"/>	Imported via the freetext import.	✕

→

## Extending MISP with Python modules

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

2024-09-11



- 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

```
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"]}]}
```

## Extending MISP with Python modules

### └ Querying a module

2024-09-11

```
■ 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"]}]}
```

```
import json
import dns.resolver
mispperrors = {'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']

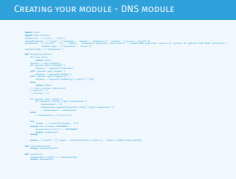
    try:
        answer = r.resolve(toquery, 'A')
    except dns.resolver.NXDOMAIN:
        mispperrors['error'] = "NXDOMAIN"
        return mispperrors
    except ...

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

def introspection():
    return mispattributes

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

### 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

2024-09-11

### └─ Testing your module

#### TESTING YOUR MODULE

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

```
python3 /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 = PassiveSSLParser(attribute, authentication)
```

### 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)
```

## 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
- ...

2024-09-11

## Extending MISP with Python modules

└─ Default expansion module set

### 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
- ...

- 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



- 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

## Extending MISP with Python modules

### └─ 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
- 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

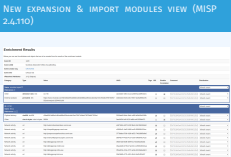
Below you can see the attributes and objects that are to be created from the results of the enrichment module.

Event ID	1229						
Event UUID	5cc3042c-8bb4-4837-9564-47aca964451a						
Event creator org	ORONAME						
Event info	urhaus test						
#Resolved Attributes	14 (2 Objects)						
Category	Type	Value	UUID	Tags	IDS	Disable Correlation	Distribution
Name: virustotal-report ⓘ References: 0							
Other	detection-ratio: text	10 / 66	adc32d9e-4651-41a1-4558-5a1039fe4be1			<input checked="" type="checkbox"/>	<input type="text" value="inherit event"/>
External analysis	permalink: link	https://www.virustotal.com/file13fad9911b80be1d64e688ba23fcbcd8c21aa73017b6bdc78570ef47552ed/analysis/1554403108/	40b3d1d0-5e81-48c7-9fe7-be2b2898427b			<input type="checkbox"/>	<input type="text" value="inherit event"/>
ID: 12700 Name: file ⓘ References: 11 ⓘ							
Payload delivery	sha256: sha256	d3fad9911b80be1d64e688ba23fcbcd8c21aa73017b6bdc78570ef47552ed	5026ab08-8f0c-40e4-a485-b69e92d0295b			<input checked="" type="checkbox"/>	<input type="text" value="inherit event"/>
Other	size-in-bytes: size-in-bytes	98304	9ee14454-fef4-4210-a88a-e401599b4f71			<input checked="" type="checkbox"/>	<input type="text" value="inherit event"/>
Network activity	url	http://automotivedreamteam.com/v.exe	e697650e-b672-405f-9be9-2dc39459d5e0			<input checked="" type="checkbox"/>	<input type="text" value="inherit event"/>
Network activity	url	http://shopalldogspoop.com/v.exe	a3986a11-4e60-4b5-ba40-999666402cbc			<input checked="" type="checkbox"/>	<input type="text" value="inherit event"/>
Network activity	url	http://pooperscoopfranchise.com/v.exe	3778dbd0-f7b6-4186-a052-746a38909e0			<input checked="" type="checkbox"/>	<input type="text" value="inherit event"/>
Network activity	url	http://cherryhillpooperscoopers.com/v.exe	b804db74-4a62-4cd7-abef-a4b68781411e			<input checked="" type="checkbox"/>	<input type="text" value="inherit event"/>
Network activity	url	http://alldogspoop.net/v.exe	09d672d8-62f9-469f-9c1f-5319d226d44			<input checked="" type="checkbox"/>	<input type="text" value="inherit event"/>
Network activity	url	http://alldogspoop.mobi/v.exe	48a6ba06-b739-47ad-04c1-d583b2b9c4ae			<input checked="" type="checkbox"/>	<input type="text" value="inherit event"/>
Network activity	url	http://alldogspoop.info/v.exe	0f5ad15b-47ed-4772-act8-d2240a6e08c3			<input checked="" type="checkbox"/>	<input type="text" value="inherit event"/>
Network activity	url	http://alldogspoop.biz/v.exe	90c29d88-d778-4415-8544-5a2fcf53d47			<input checked="" type="checkbox"/>	<input type="text" value="inherit event"/>

2024-09-11

## Extending MISP with Python modules

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

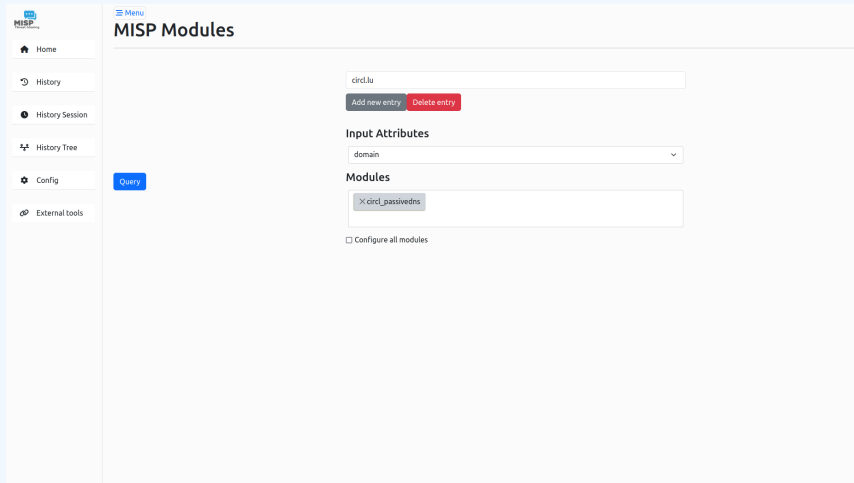


- Flexibility, no need to install MISP
- User friendly interface
- Easiest way to test new modules

### └─ New - Standalone Functionality

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

- Add multiple entries
- Choose different modules



The screenshot shows the MISP Web Interface - Query page. On the left is a sidebar with navigation links: Home, History, History Session, History Tree, Config, and External tools. The main content area is titled "MISP Modules" and features a search bar with the text "cird.lu". Below the search bar are two buttons: "Add new entry" and "Delete entry". Under the "Input Attributes" section, there is a dropdown menu currently showing "domain". The "Modules" section displays a list of modules, with "cird\_passivedns" selected. At the bottom, there is a checkbox labeled "Configure all modules".

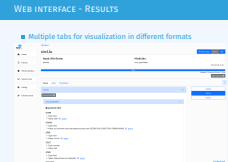
Web interface - Query



## ■ Multiple tabs for visualization in different formats

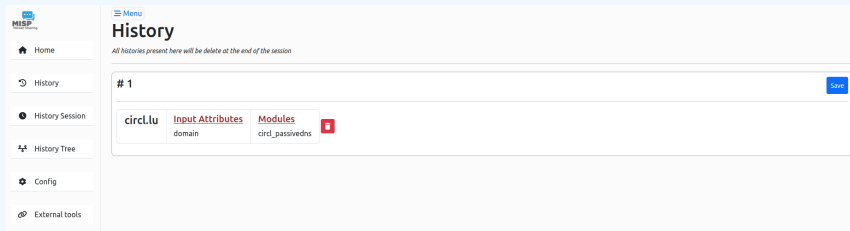
The screenshot displays the MISP Web Interface. On the left is a sidebar with navigation links: Home, History, History Session, History Tree, Config, and External tools. The main content area is titled 'circl.lu' and shows the results of a query. The 'Input Attribute' is 'domain' and the 'Modules' used are 'circl\_passivedns'. A progress bar indicates 100% completion, with a status of 'Stopped: 1 Success, 0 Errors, 1 Total'. Below this, there are tabs for 'Visual', 'Json', and 'Markdown'. The 'Visual' tab is active, showing a hierarchical tree of results. The tree includes nodes for 'circl.lu', 'External tools', 'circl\_passivedns', and 'passive-dns'. Under 'passive-dns', there are several sub-nodes: 'rrtype' (Type: text, Value: SOA), 'rrname' (Type: text, Value: ns1.eurodns.com hostmaster.eurodns.com), 'rdata' (Type: text, Value: circl.lu), 'count' (Type: counter, Value: 260), 'origin' (Type: text, Value: https://www.circl.lu/pdns/), and 'time\_first'. A 'Go Back Top' link is at the bottom right of the results area.

## └ Web interface - Results



# WEB INTERFACE - HISTORY

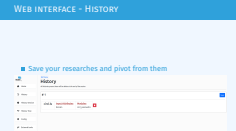
## ■ Save your researches and pivot from them



The screenshot shows the MISP Web Interface. On the left is a sidebar with navigation links: Home, History, History Session, History Tree, Config, and External tools. The main content area is titled 'History' and includes a sub-header 'All histories present here will be delete at the end of the session'. Below this, there is a list of history items. The first item, labeled '# 1', is highlighted and contains the following details: 'circl.lu' (domain), 'Input Attributes' (domain), 'Modules' (circl\_passivedns), and a red square icon. A 'Save' button is located to the right of the item.

## Extending MISP with Python modules

### └ Web interface - History



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

Menu

### External tools +

Search tools

☒ flowintel

**flowintel**

Name:

flowintel

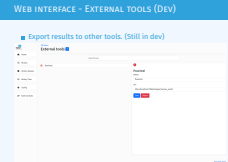
Url:

http://localhost:7006/analyzer/recieve\_result

Save Delete

[\[Go Back Top\]](#)

### └─ 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)

### └ 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.



- <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.