

PyMISP

API Documentation

August 12, 2015

Contents

Contents	1
1 Package pymisp	2
1.1 Modules	2
1.2 Variables	2
2 Module pymisp.api	3
2.1 Variables	3
2.2 Class PyMISPErrror	3
2.2.1 Methods	3
2.2.2 Properties	3
2.3 Class NewEventError	4
2.3.1 Methods	4
2.3.2 Properties	4
2.4 Class NewAttributeError	5
2.4.1 Methods	5
2.4.2 Properties	5
2.5 Class PyMISP	5
2.5.1 Methods	6
2.5.2 Properties	8
Index	9

1 Package pymisp

1.1 Modules

- **api**: Python API using the REST interface of MISP
(Section 2, p. 3)

1.2 Variables

Name	Description
<code>--package--</code>	Value: 'pymisp'

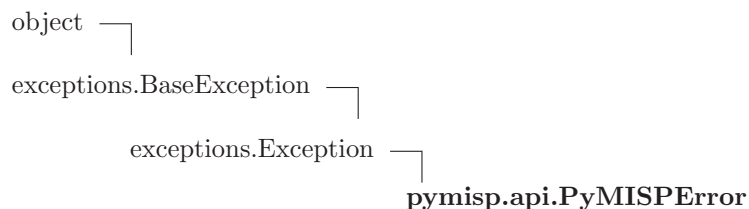
2 Module pymisp.api

Python API using the REST interface of MISP

2.1 Variables

Name	Description
<code>--package--</code>	Value: 'pymisp'

2.2 Class PyMISPErrror



Known Subclasses: `pymisp.api.NewAttributeError`, `pymisp.api.NewEventError`

2.2.1 Methods

<pre> __init__(self, message) x.__init__(...) initializes x; see help(type(x)) for signature Overrides: object.__init__ extit(inherited documentation) </pre>

Inherited from exceptions.Exception

```
__new__()
```

Inherited from exceptions.BaseException

```
__delattr__(), __getattr__(), __getitem__(), __getslice__(), __reduce__(), __repr__(),
__setattr__(), __setstate__(), __str__(), __unicode__()
```

Inherited from object

```
__format__(), __hash__(), __reduce_ex__(), __sizeof__(), __subclasshook__()
```

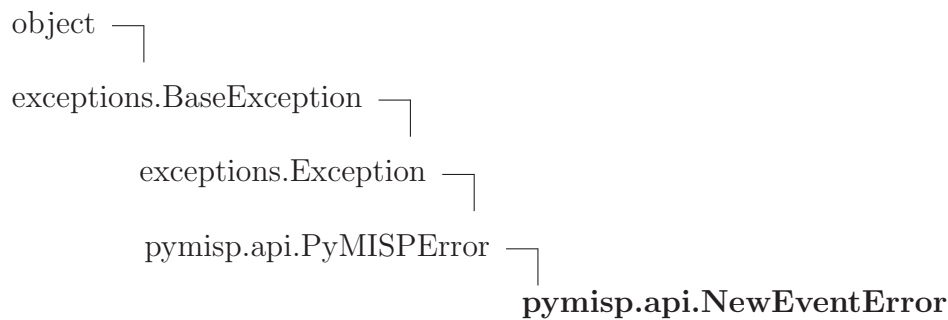
2.2.2 Properties

Name	Description
<i>Inherited from exceptions.BaseException</i>	

continued on next page

Name	Description
<code>args, message</code>	
<i>Inherited from object</i>	
<code>__class__</code>	

2.3 Class `NewEventError`



2.3.1 Methods

Inherited from `pymisp.api.PyMISPError` (Section 2.2)

`__init__()`

Inherited from `exceptions.Exception`

`__new__()`

Inherited from `exceptions.BaseException`

`__delattr__()`, `__getattr__()`, `__getitem__()`, `__getslice__()`, `__reduce__()`, `__repr__()`,
`__setattr__()`, `__setstate__()`, `__str__()`, `__unicode__()`

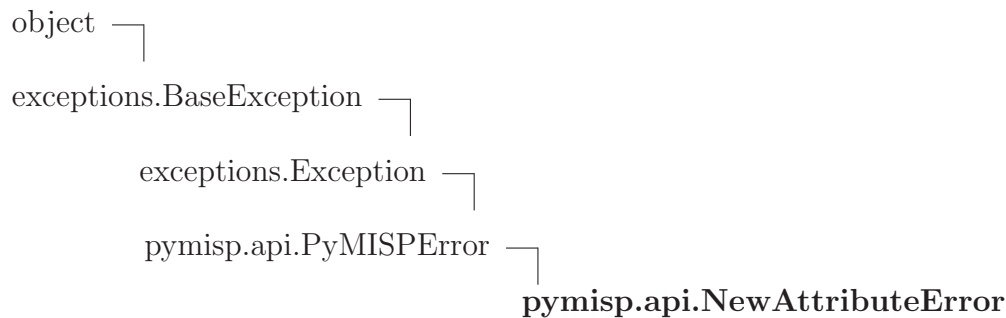
Inherited from `object`

`__format__()`, `__hash__()`, `__reduce_ex__()`, `__sizeof__()`, `__subclasshook__()`

2.3.2 Properties

Name	Description
<i>Inherited from <code>exceptions.BaseException</code></i>	
<code>args, message</code>	
<i>Inherited from <code>object</code></i>	
<code>__class__</code>	

2.4 Class NewAttributeError



2.4.1 Methods

Inherited from pymisp.api.PyMISPError(Section 2.2)

`__init__()`

Inherited from exceptions.Exception

`__new__()`

Inherited from exceptions.BaseException

`__delattr__()`, `__getattr__()`, `__getitem__()`, `__getslice__()`, `__reduce__()`, `__repr__()`,
`__setattr__()`, `__setstate__()`, `__str__()`, `__unicode__()`

Inherited from object

`__format__()`, `__hash__()`, `__reduce_ex__()`, `__sizeof__()`, `__subclasshook__()`

2.4.2 Properties

Name	Description
<i>Inherited from exceptions.BaseException</i> args, message	
<i>Inherited from object</i> __class__	

2.5 Class PyMISP



Python API for MISP

:param url: URL of the MISP instance you want to connect to
 :param key: API key of the user you want to use
 :param ssl: can be True or False (to check ot not the validity of the certificate. Or a CA_BUNDLE in case of self signed certiifcate (the concatenation of all the *.crt of the chain)
 :param out_type: Type of object (json or xml)

2.5.1 Methods

```
__init__(self, url, key, ssl=True, out_type='json')
```

x.__init__(...) initializes x; see help(type(x)) for signature

Overrides: object.__init__ extit(inherited documentation)

```
get_index(self)
```

Return the index.

Warning, there's a limit on the number of results

```
get_event(self, event_id)
```

Get an event

:param event_id: Event id to get

```
add_event(self, event)
```

Add a new event

:param event: Event as JSON object / string or XML to add

```
update_event(self, event_id, event)
```

Update an event

:param event_id: Event id to update :param event: Event as JSON object / string or XML to add

delete_event(*self, event_id*)

Delete an event

:param event_id: Event id to delete

prepare_attribute(*self, event_id, distribution, to_ids, category, info, analysis, threat_level_id*)

prepare_sample(*self, filename, filepath*)

prepare_samplelist(*self, filepaths*)

upload_sample(*self, filename, filepath, event_id, distribution, to_ids, category, info, analysis, threat_level_id*)

upload_samplelist(*self, filepaths, event_id, distribution, to_ids, category, info, analysis, threat_level_id*)

search_all(*self, value*)

search(*self, values=None, not_values=None, type_attribute=None, category=None, org=None, tags=None, not_tags=None, date_from=None, date_to=None, last=None*)

Search via the Rest API

:param values: values to search for :param not_values: values **not** to search for
 :param type_attribute: Type of attribute :param category: Category to search
 :param org: Org reporting the event :param tags: Tags to search for
 :param not_tags: Tags **not** to search for :param date_from: First date
 :param date_to: Last date :param last: Last updated events (for example 5d or 12h or 30m)

get_attachement(*self, event_id*)

Get attachement of an event (not sample)

:param event_id: Event id from where the attachements will be fetched

download_samples (<i>self</i> , <i>sample_hash</i> =None, <i>event_id</i> =None, <i>all_samples</i> =False)

download_last (<i>self</i> , <i>last</i>)
--

Download the last updated events.

:param last: can be defined in days, hours, minutes (for example 5d or 12h or 30m)

download_all (<i>self</i>)

Download all event from the instance

download_all_suricata (<i>self</i>)
--

Download all suricata rules events.

download_suricata_rule_event (<i>self</i> , <i>event_id</i>)

Download one suricata rule event.

:param event_id: ID of the event to download (same as get)

download (<i>self</i> , <i>event_id</i> , <i>with_attachment</i> =False)
--

Download one event in XML

:param event_id: Event id of the event to download (same as get)

Inherited from object

`--delattr--()`, `--format--()`, `--getattr--()`, `--hash--()`, `--new--()`, `--reduce--()`, `--reduce_ex--()`, `--repr--()`, `--setattr--()`, `--sizeof--()`, `--str--()`, `--subclasshook--()`

2.5.2 Properties

Name	Description
<i>Inherited from object</i>	
<code>--class--</code>	

Index

- pymisp (*package*), 2
 - pymisp.api (*module*), 3–8
 - pymisp.api.NewAttributeError (*class*), 4–5
 - pymisp.api.NewEventError (*class*), 4
 - pymisp.api.PyMISP (*class*), 5–8
 - pymisp.api.PyMISPErrors (*class*), 3–4