CIF Python SDK Documentation

Release 0.3

CSIRT Gadgets Foundation

March 22, 2016

Contents

Contents:

CHAPTER 1

cif manual page

1.1 SYNOPSIS

cif [–config] [–remote] [–token] [-q] [–limit] [–feed] [–format] example.org

cif –otype ipv4 –format csv –feed

cif –otype ipv4 –format bro –feed

1.2 DESCRIPTION

cif is a command line tool for searching the CIF API.

1.3 OPTIONS

-h, --help	Show the default help message
-v, --verbose	Verbose mode, more output from successful actions will be shown.
-d, --debug	Debug mode, more output from actions will be shown.
--token	Specify the API Token to be used, overrides any token specified in the config file.
--config	Specify the configuration file to be used.
--remote	Specify the remote api url.
--limit	Override the default search results LIMIT when searching.
--format	Specify an output format to represent the data (table, csv, etc..).
--no-verify-ssl	Disable TLS verification for the remote API.
--timeout	Specify a timeout for the remote API.
-p, --ping	Ping the remote API.
--sort	Sort the results from a search.
--submit	Pass a JSON encoded set of observables through STD to the API.
-q, --search	Search the API.
--firsttime	Filter results by firsttime >= 'YYYY-MM-DDTHH:mm:ssZ'

--lasttime	Filter results by lasttime >= 'YYYY-MM-DDTHH:mm:ssZ'
--tags	Filter results by a set of tags (ex: 'botnet,zeus').
--description	Filter results by description (ex: 'zeus')
--otype	Filter results by otype (ex: ipv4)
--cc	Filter results by country code (ex: US)
--confidence	Filter results by confidence >= N
--rdata	Filter results by rdata
--provider	Filter results by provider
--asn	Filter results by ASN number
--feed	Perform a "feed aggregation" of the results.
--whitelist-limit	Specify a limit on a generated whitelist [requires –feed].
--last-day	Filter results by the last 24hours.
--days	Filter results by the N days.
--aggregate	Aggregate the results based on 'observable'

1.4 FILES

~/.cif.yml – Config file, used if present to connect to the CIF API

1.5 SEE ALSO

Extensive documentation is available in the documentation site: <py-cifsdk.rtfd.org>.

CHAPTER 2

cif.yml manual page

2.1 DESCRIPTION

cif.yml is the config file used to set defaults for the *cif* commands.

2.2 OPTIONS

client specify the client section of the config.

remote specify the API url

token specify a token for the API

no_verify_ssl turn off TLS verification

2.3 EXAMPLES

```
---
client:
    remote: https://cif.test
    token: 12341234
    no_verify_ssl: true
```

2.4 SEE ALSO

Extensive documentation is available in the documentation site: <py-cifsdk.rtfd.org>.

CHAPTER 3

Indices and tables

- genindex
- modindex
- search