mfe$_{s}aw$*Documentation*

Release 0.4.0

Andy Walden

Oct 24, 2019

Contents

McAfee SIEM API Wrapper (MFE_SAW) ==========+

Contents:

McAfee SIEM API Wrapper - MFE_SAW

MFE_SAW is a wrapper around the McAfee ESM API versions 10.x and above.

This project attempts to provide a pythonic interface for specific aspects of the product including: * ESM Monitoring * Datasource Management (add, edit, del) * Simplified Query interface [TBD] * Watchlist Operations [TBD]

The first target of this project is datasource management. With this library and accompanied front-end CLI interface, datasources can be easily added by providing a few details.

dsconf/new_ds_cfg.txt ‘‘‘ name=DC01_DNS ip=10.10.1.34 rec_ip=172.16.15.10 type=linux

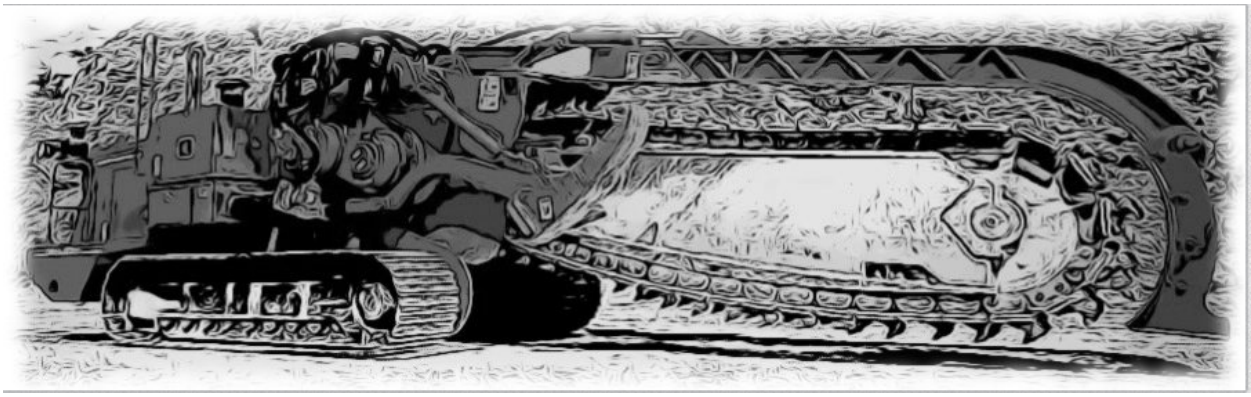
$ mfe_saw -a

$ mfe_saw -s “DC01_DNS”

‘‘‘

Here is an example:

```
 >>> esm = ESM()
 >>> esm.login(host, username, passwd)
 >>> esm.time()
 '2017-07-07T19:47:49.0+0000'
 >>> devtree = DevTree()
 >>> 'loghost-245' in devtree
 True
 >>> devtree.search('3.1.1.1')
{'dev_type': '0', 'name': 'NXLog-Client-1', 'id': '144119586172698880',
'enabled': 'T', 'ds_ip': '3.1.1.1', 'hostname': 'nxlog-client-1',
'typeID': '0', 'vendor': 'InterSect Alliance', 'model':
'Snare for Windows', 'tz_id': '', 'date_order': '', 'port': '',
'syslog_tls': 'F', 'client_groups': '0'}
```



CHAPTER 1

Feature Support

- Pythonic implementation
- Authentication and session tracking across objects
- Built-in multiprocessing for high performance
- Pass through of native API methods
- CLI interface
- Get info for existing datasources
- Add new datasources
- ESM status methods
- More to come!

mfe_saw officially supports Python 3.5–3.7 on Windows and Linux.

CHAPTER 2

Installation

To install MFE_SAW, use pip:

```
$ pip install mfe_saw
```

CHAPTER 3

Documentation

Documentation is available at http://mfe-saw.readthedocs.io/en/latest/index.html

CHAPTER 4

Installation

At the command line:

```
$ easy_install mfe_saw
```

Or, if you have virtualenvwrapper installed:

```
$ mkvirtualenv mfe_saw
$ pip install mfe_saw
```

CHAPTER 5

Usage

To use mfe_saw in a project:

```
import mfe_saw
```

User Guide: ESM Datasources Queries Watchlists

API R:

ESM DevTree DataSource Query Watchlist

User Guide