pan-stix Documentation

Release 0.2.4

Palo Alto Networks

December 10, 2015

Contents

Contents:

CHAPTER 1

wildfire-to-stix

1.1 Usage

```
usage: wildfire-to-stix.py [--version] [-t <pan-python tag>] [--verbose]
                           [-h <hash>] [--help] [-i <report filename>]
                           [--no-pcap] [--pcap <pcap source>] [--no-sample]
                           [--sample <sample source>] [-f <output format>]
                           [-o <output filename>]

Convert Palo Alto Networks Wildfire reports to STIX/MAEC

optional arguments:
  --version             show program's version number and exit
  -t <pan-python tag>, --tag <pan-python tag>
                        pan-python tag for Wildfire API
  --verbose             verbose
  -h <hash>, --hash <hash>
                        hash of the sample
  --help                help
  -i <report filename>, --in <report filename>
                        local Wildfire report
  --no-pcap             do not include pcap
  --pcap <pcap source>  pcap filename or 'network' for retriving from Wildfire
                        API
  --no-sample           do not include sample
  --sample <sample source>
                        sample filename or 'network' for retriving from
                        Wildfire API
  -f <output format>, --outfmt <output format>
                        output format
  -o <output filename>, --out <output filename>
                        output filename
  -e <evidence score>, --evidence <evidence score>
                        minimum evidence score
```

CHAPTER 2

panstix.packaging

This module contains the main entry points for the library.

panstix.packaging.**get_maec_package_from_wfreport**(***kwargs*)
Generate a MAEC package from a Wildfire report.

The Wildfire report is retrieved using Wildfire API if *hash* and *tag* keyword arguments are specified, or read from a file passed via *report* keyword argument. *report* can be a filename or a file object.

Parameters

- **hash** (*str*) – Hash of the sample.
- **tag** (*str*) – pan-python tag used to retrieve the report.
- **report** (*str or file*) – filename of the Wildfire report or a file object.
- **pcap** (*str*) – filename of the pcap file to include or 'network' to retrive the pcap using Wildfire API via *tag*. If *None* pcap is not included in the resulting package.
- **evidence** (*float*) – can be used to retrieve only indicators associated to malicious behaviors with a score higher than this threshold

Returns A MAEC Package object with Wildfire report contents.

Return type maec.package.package.Package

panstix.packaging.**get_stix_il_package_from_wfreport**(***kwargs*)
Generate a STIX package with a list of STIX Indicators extracted from a Wildfire report.

The Wildfire report is retrieved using Wildfire API if *hash* and *tag* keyword arguments are specified, or read from a file passed via *report* keyword argument. *report* can be a filename or a file object.

Parameters

- **hash** (*str*) – Hash of the sample.
- **tag** (*str*) – pan-python tag used to retrieve the report.
- **report** (*str or file*) – filename of the Wildfire report or a file object.
- **evidence** (*float*) – can be used to retrieve only indicators associated to malicious behaviors with a score higher than this threshold

Returns A STIX Package object with the list of Indicators extracted from the Wildfire report.

Return type stix.core.STIXPackage

panstix.packaging.**get_stix_ol_package_from_wfreport**(***kwargs*)
Generate a STIX package with a list of CybOX Observables extracted from a Wildfire report.

The Wildfire report is retrieved using Wildfire API if *hash* and *tag* keyword arguments are specified, or read from a file passed via *report* keyword argument. *report* can be a filename or a file object.

Parameters

- **hash** (*str*) – Hash of the sample.
- **tag** (*str*) – pan-python tag used to retrieve the report.
- **report** (*str or file*) – filename of the Wildfire report or a file object.
- **evidence** (*float*) – can be used to retrieve only indicators associated to malicious behaviors with a score higher than this threshold

Returns A STIX Package object with the list of Observables extracted from the Wildfire report.

Return type stix.core.STIXPackage

panstix.packaging.**get_stix_package_from_wfreport**(**kwargs)

Generate a STIX package from a Wildfire report.

The Wildfire report is retrieved using Wildfire API if *hash* and *tag* keyword arguments are specified, or read from a file passed via *report* keyword argument. *report* can be a filename or a file object.

Parameters

- **hash** (*str*) – Hash of the sample.
- **tag** (*str*) – pan-python tag used to retrieve the report.
- **report** (*str or file*) – filename of the Wildfire report or a file object.
- **pcap** (*str*) – filename of the pcap file to include or 'network' to retrive the pcap using Wildfire API via *tag*. If *None* pcap is not included in the resulting package.
- **sample** (*str*) – filename of the sample file to include or 'network' to retrive the sample using Wildfire API via *tag*. If *None* sample is not included in the resulting package.
- **evidence** (*float*) – can be used to retrieve only indicators associated to malicious behaviors with a score higher than this threshold

Returns A STIX Package object with Wildfire report contents.

Return type stix.core.Package

CHAPTER 3

License

CHAPTER 4

Indices and tables

- genindex
- modindex
- search

p

G

P