# Cybercure.ai Python SDK library Documentation

cybercure.ai

Nov 01, 2020

# Contents

Release v0.4. (Installation)

Welcome to Cybercure Python SDK documentation. he pyrthon SDK allows quick and easy access to cybercure API cyber threat intelligence data.

Feel free to read the documentation and if you have improvements in mind, please let us know.

# CHAPTER 1

# Table of Contents:

## 1.1 get_ip_indicators()

### 1.1.1 Overview

Cybercure.ai IP API provides a live list of addresses that are currently known to be attacking on the internet. This list contains bots, command and controls, infected computers with malware and ip addresses that are known to be used for attacks right now.

### 1.1.2 Code example

```
>>> import cybercure
>>> active_blocked_ip = cybercure.get_ip_indicators('json')
>>> print ("Okay.. I got %s records, now showing them:" % active_blocked_ip['count'])
>>> for threat in active_blocked_ip['data']['ip']:
>>>         print "Are you blocking %s ?" % threat
```

data is always returned inside a data dictionary, in this API call the ip key will contain an array of the ip addresses that should be watched for.

### 1.1.3 Return Output

get_ip_indicators() accept 1 parameter and it should be one of the table shown below:

| Type | Description |
|---|---|
| json | returns json document with standard response. |
| csv | delimited text file that uses a comma to separate values It stores tabular data. |
| iptables | iptables firewall formatted bash script to automatically and easily digest the feed. |
| list | ip list file, each with new line. |
| cef | cef format via http for arcsight and friends. |
| stix | stix2 json format returned as a stix bundle with indicator objects. |

## 1.2 get_url_indicators()

### 1.2.1 Overview

Cybercure.ai URL API provides a live list of URL addresses that are currently known to be spreading or asscoiated with cyber attacks.

### 1.2.2 Code example

```
>>> import cybercure
>>> active_blocked_urls = cybercure.get_url_indicators('json')
>>> print ("Okay.. I got %s records, now showing them:" % active_blocked_urls['count
↪'])
>>> for threat in active_blocked_ip['data']['urls']:
>>>         print "Are you blocking %s ?" % threat
```

data is always returned inside a data dictionary, in this API call the ip key will contain an array of the ip addresses that should be watched for.

### 1.2.3 Return Output

get_ip_indicators() accept 1 parameter and it should be one of the table shown below:

| Type | Description |
|---|---|
| json | returns json document with standard response. |
| csv | delimited text file that uses a comma to separate values It stores tabular data. |
| list | ip list file, each with new line. |
| cef | cef format via http for arcsight and friends. |
| stix | stix2 json format returned as a stix bundle with indicator objects. |

## CHAPTER 2

# SDK Calls

Cyber Cure expose several calls for use with cybercure.ai api.

- get_hash_indicators() - Allows to receive Hash indicators that are known to be currently spreading in the wild.
- get_ip_indictors() - Allows to receive list of ip addresses that are currently attacking.
- get_url_indicators() - Allows to receive list of URLs that are used by malware.
- search() - Allows to search for specific indicators

several parameters can be specified for the different calls, for example, the requested output to be returned. The examples folder contains several examples to show how the API can be used to gather the intelligence and spread to different targets, for example sending by CEF format using syslog or saving the output as STIX.

**Installation**

The easiest way to install cybercure python library is by using pip:

```
pip install cybercure
```

**Code example**

```
>>> import cybercure
>>> active_blocked_ip = cybercure.get_ip_indicators(output_type)
>>> print ("Okay.. I got %s records, now showing them:" % active_blocked_ip['count'])
>>> for threat in active_blocked_ip['data']['ip']:
>>>         print "Are you blocking %s ?" % threat
```

Make sure to checkout complete and updated documentation at:

cybercure documentaion

and also check for updates on www.cybercure.ai