

---

# **apiosintDS**

*Release 2.0*

**Davide Baglieri**

**Jul 15, 2023**



## CONTENTS

<b>1</b>	<b>Welcome to apiosintDS's documentation!</b>	<b>3</b>
	<b>Index</b>	<b>25</b>



Latest stable release is **v2.0** (*Changelog*)

**apiosintDS** is a python client library for public API lookup service over OSINT IoCs stored at DigitalSide Threat-Intel repository. It can be defined a **service as a library** tool designed to act both as a standard Python library to be included in your own Python application and as command line tool. Query can be performed against suspicious IPs, domains, urls and file hashes. Data stored has a 7 days retention.

```

OSINT.DigitalSide.IT Threat-Intel Repository v.2.0
Submission summary
-----
| Items parsed: 16 | Items submitted: 3 | Items found: 3 |
| Invalid(s): 12 | URL(s): 0 | URL(s): 0 |
| Duplicate(s): 1 | Hash(es): 0 | Hash(es): 0 |
| Not found: 0 | Domain(s): 2 | Domain(s): 2 |
| IP(s): 1 | IP(s): 1 |
-----
| 179[.]43[.]162[.]124 - ReLated URL(s) 11
-----
| hXXp://179.43.162.124/ex.sh
-----
| TLP:white | First Seen 2023-07-01 06:11:05 | Last Seen 2023-07-01 06:11:05
-----
| Filename: ex.sh
-----
| MD5: c3b641509084438db6e1ab8be9e82990
| SHA1: 73389eb6d835c8f9c6fb211e372785222487f61
| SHA256: 5b3e62c73008cdeed70fc70f1044c60a3caad8385d146bf5f5b7572ac29c65ca7
-----
| Size: 2053 | Type: text/x-shellscript | Observed: 1 | VT: 34/59
-----
| Observation time frame: N/A
-----
| STIX network indicators: URLs => 1 | Domains => 0 | IPs: 1
-----
Online Reports (availability depends on data retention)
-> MISP EVENT: https://osint.digitalside.it/Threat-Intel/digitalside-misp-feed/253d46f7-903e-4b88-b0a0-c4f437824b5a.json
-> MISP CSV: https://osint.digitalside.it/Threat-Intel/csv/253d46f7-903e-4b88-b0a0-c4f437824b5a.csv
-> DS Report: https://osint.digitalside.it/report/c3b641509084438db6e1ab8be9e82990.html
-> STIX: https://osint.digitalside.it/Threat-Intel/stix2/c3b641509084438db6e1ab8be9e82990.json
-----
| hXXp://179.43.162.124/SBIDIOT/arm
-----
| TLP:white | First Seen 2023-07-02 06:14:01 | Last Seen 2023-07-02 06:14:01
-----
| Filename: arm
-----

```

DigitalSide Threat-Intel (also on [GitHub.com](https://github.com)) shares a set of **Open Source Cyber Threat Intelligence** information, mostly based on malware analysis and compromised URLs, IPs and domains. The purpose of the project is to develop and test new ways to hunt, analyze, collect and share relevant sets of IoCs to be used by SOC/CSIRT/CERT with minimum effort.

This library has been specially designed for people and organizations don't want to import the whole DigitalSide Threat-Intel dataset and prefer to use it as an on demand service.



## WELCOME TO APIOSINTDS'S DOCUMENTATION!

### Documentation contents

## 1.1 Installation guide

### 1.1.1 Install python > 3.5.2

Make sure you installed on your system python > 3.5.2. Try typing python3 on your terminal.

```
~$ python3
Python 3.6.8 (default, Oct 7 2019, 12:59:55)
[GCC 8.3.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>>
```

### 1.1.2 Install from sources

Make sure you installed python3-setuptools and git packages on your system. If not, install missings according your distribution.

```
~$ cd /your/path/src/
~$ git clone https://github.com/davidonzo/apiosintDS.git
~$ cd apiosintDS/
~$ python3 -m pip install .
```

### 1.1.3 Install via pip3

Make sure you installed python3-pip package on your system. If not, install it according your distribution.

```
~$ pip3 install apiosintDS
```

## 1.1.4 Windows support

The library has never been tested on Windows platform. Actually only UNIX system are supported.

## 1.2 Usage via command line (CLI)

```
~$ apiosintDS [-h] [-e [IPv4|domain|url|hash]] [-f /path/to/file.txt] [-st]
              [-o /path/to/output.json] [-p] [-nc] [-v] [-c] [-cd /path/to/cachedir]
              [-ct [0-9]] [-cc] [-ld /path/to/git/clone/Threat-Intel/]
              [-l /path/to/logfile.log] [-ll [DEBUG|INFO|WARNING|ERROR|CRITICAL]]
              [-lc] [-i] [-s] [-vv]
```

### 1.2.1 Command line options

**-h, --help** Show the help and exit.

**Type**  
boolean  
**Default**  
False

**-e, --entity** Single item to search. Supported entities are IPv4/FQDN/URLs or file hashes in MD5, SHA1 or SHA256 format.

**Type**  
string  
**Default**  
None  
**Allowed**  
[IPv4|domain|url|hash(['md5', 'sha1', 'sha256'])]

---

**Note:** It can't be used in combination with the `--file` option.

---

**-f, --file** Path to file containing entities to search. Supported entities are IPv4/FQDN/URLs and file hashes (MD5, SHA1, SHA256). Insert one item per row.

**Type**  
string  
**Default**  
None  
**Example**  
/path/to/file.txt

---

**Note:** It can't be used in combination with the `--entity` option.

---

**-st, --stix** Download and parse additional information from online STIX report.

**Type**  
boolean



**Default**  
False

---

**Note:** STIX2 reports may be not available due to data retention policy.

---

**-o, --output** Output file. If not specified the output will be redirect to the system STDOUT.

**Type**  
string

**Default**  
STDOUT

**Example**  
/path/to/output.json

---

**Note:** It can't be used in combination with the `--pretty` option.

---

**-p, --pretty** Show results in terminal with a little bit of formatting applied.

**Type**  
boolean

**Default**  
False

---

**Note:** Default output format is JSON. Data displayed in pretty view does not cover all informations included in the JSON response format.

---

**-nc, --nocolor** Support colors in `--pretty` output. For accessibility purpose.

**Type**  
boolean

**Default**  
False

**-v, --verbose** Include unmatched results in report.

**Type**  
boolean

**Default**  
False

**-c, --cache** Enable cache mode. Downloaded lists will be stored and won't be downloaded until the cache timeout is reached.

**Type**  
boolean

**Default**  
False

**-cd, --cachedirectory** The cache directory where the script check for cached lists files and where them will be stored on cache creation or update.

**Type**  
string

**Default**

System tmp directory

**Example**

/path/to/cachedir

---

**Note:** Must be specified the same every script run unless your are using the system temp directory.

---

**-ct, --cachetimeout** Define the cache timeout in hours.

**Type**

integer

**Default**

4

---

**Note:** 0 is allowed but means no timeout. Default value is 4 hours. This option needs to be used in combination with --cache option configured to True.

---

**-cc, --clearcache** Force the script to download updated lists even if the --cachetimeout period has not yet been reached.

**Type**

boolean

**Default**

False

---

**Note:** Must be used in combination with --cache

---

**-ld, --localdirectory** Absolute path to the 'Threat-Intel' directory related to a local project clone. Searches are performed against local data.

**Type**

string

**Default**

False

**Example**

/path/to/git/clone/Threat-Intel/

---

**Note:** Before using this option, clone the GitHub project in a file system where the library has read permissions. Don't forget to use --depth=1 and --branch=master options if you don't want to download all project commits.

```
$ cd /path/to/git/clone/
$ git clone --depth=1 --branch=master https://github.com/davidonzo/Threat-Intel.git
```

When this option is in use, all cache related options are ignored. To update data in your local repository destroy the existing data and clone it again.

```
$ cd /path/to/git/clone/
$ rm -rf Threat-Intel/
$ git clone --depth=1 --branch=master https://github.com/davidonzo/Threat-Intel.git
```

**-l, --logfile** Define the log file path.

**Type**  
string

**Default**  
NONE

**Example**  
/path/to/logfile.log

---

**Note:** No log file is created by default. STDOUT is used instead.

---

**-ll, --loglevel** Define the log level.

**Type**  
enum

**Default**  
DEBUG

**Allowed**  
[DEBUG|INFO|WARNING|ERROR|CRITICAL]

**-lc, --logconsole** Suppress log messages to the console's STDOUT.

**Type**  
boolean

**Default**  
False

**-i, --info** Print information about the library.

**Type**  
boolean

**Default**  
False

**-s, --schema** Display the response json schema.

**Type**  
boolean

**Default**  
False

**-vv, --version** Show the library version.

**Type**  
boolean

**Default**  
False



(continued from previous page)

```

↪ f5e313d2-3d64-4d0f-af77-37a925bcd08f.json
  -> MISP CSV:  https://osint.digitalside.it/Threat-Intel/csv/f5e313d2-3d64-4d0f-af77-
↪ 37a925bcd08f.csv
  -> DS Report: https://osint.digitalside.it/report/bc152acad73829358847e5f5bbf3edc0.
↪ html
  -> STIX:      https://osint.digitalside.it/Threat-Intel/stix2/
↪ bc152acad73829358847e5f5bbf3edc0.json
#####

```

### 1.3.2 Multiple items using --file with --pretty output

Example file ioc.txt.

```

~$ cat ioc.txt
7cb796c875cccc9233d82854a4e2fdf0
monke.re

```

Response.

```

~$ apiosintDS -f ioc.txt -p -nc -st

  _ _ _ _ _  ( )  _ _ _ _ _  ( )  _ _ _ _ _  | | |  _ _ _ _ _  |
 / _ \ | ' _ \ | / _ \ | / _ \ | | ' _ \ | | | \ _ _ \
| ( | | | ) | | ( ) \ _ _ \ | | | | | | | | | | | | | | | |
 \ _ , | . _ / | _ \ \ _ _ / | _ _ / | _ \ | | _ \ | _ _ / | _ _ / v.2.0
    | _ | OSINT.DigitalSide.IT Threat-Intel Repository

Submission summary
-----
| Items parsed: 2 | Items submitted: 2 | Items found: 2 |
-----
| Invalid(s): 0 | URL(s): 0 | URL(s): 0 |
| Duplicate(s): 0 | Hash(es): 1 | Hash(es): 1 |
| Not found: 0 | Domain(s): 1 | Domain(s): 1 |
| | IP(s): 0 | IP(s): 0 |
-----
| 7cb796c875cccc9233d82854a4e2fdf0 |
-----
| TLP:white | First Seen 2023-07-04 09:33:03 | Last Seen 2023-07-04 09:33:03 |
-----
| Filename: plugmanzx.exe |
-----
| MD5: 7cb796c875cccc9233d82854a4e2fdf0 |
| SHA1: 158514acfa87d0b99e2af07a28004480bbf66e83 |
| SHA256: 49e64d72d5ed4fb7967da4b6851d94cdceffe4ba0316587767a13901fe580239 |
-----
| Size: 924672 | Type: application/x-dosexec | Observed: 1 | VT: 32/71 |
-----
| Observation time frame: N/A |

```

(continues on next page)

(continued from previous page)

```

-----
| STIX network indicators: URLs => 1 | Domains => 0 | IPs: 1 |
-----
Online Reports (availability depends on data retention)
-> MISP EVENT: https://osint.digitalside.it/Threat-Intel/digitalside-misp-feed/
↪d6146389-4294-4a41-b4ca-6e74c74b7f8b.json
-> MISP CSV: https://osint.digitalside.it/Threat-Intel/csv/d6146389-4294-4a41-b4ca-
↪6e74c74b7f8b.csv
-> DS Report: https://osint.digitalside.it/report/7cb796c875cccc9233d82854a4e2fdf0.
↪html
-> STIX: https://osint.digitalside.it/Threat-Intel/stix2/
↪7cb796c875cccc9233d82854a4e2fdf0.json
#####
-----
| monke[.]re - Related URL(s) 2 |
-----
| hXXp://monke.re/arm7 |
-----
| TLP:white | First Seen 2023-07-06 23:51:01 | Last Seen 2023-07-06 23:51:01 |
-----
| Filename: arm7 |
-----
| MD5: 318323c9da34bf25833f7da32eab23d6 |
| SHA1: e2bb927b08ebcbaad8f304d02309af776312c9bf |
| SHA256: bb1f9e108daa389e62b79067d1cdbef548f9934c9cc85a92565da7063cf36f89 |
-----
| Size: 57148 | Type: application/x-executable | Observed: 1 | VT: 14/61 |
-----
| Observation time frame: N/A |
-----
| STIX network indicators: URLs => 1 | Domains => 1 | IPs: 0 |
-----
Online Reports (availability depends on data retention)
-> MISP EVENT: https://osint.digitalside.it/Threat-Intel/digitalside-misp-feed/
↪f83d06e6-aa2f-452e-a19d-59d40e874355.json
-> MISP CSV: https://osint.digitalside.it/Threat-Intel/csv/f83d06e6-aa2f-452e-a19d-
↪59d40e874355.csv
-> DS Report: https://osint.digitalside.it/report/318323c9da34bf25833f7da32eab23d6.
↪html
-> STIX: https://osint.digitalside.it/Threat-Intel/stix2/
↪318323c9da34bf25833f7da32eab23d6.json
-----
| hXXp://monke.re/mips |
-----
| TLP:white | First Seen 2023-07-07 00:31:02 | Last Seen 2023-07-07 00:31:02 |
-----
| Filename: mips |
-----
| MD5: 579081f528d9279a87b298b9838c377b |
| SHA1: 45048073aad5997881dffe41e32f9b17beb1c2e1 |

```

(continues on next page)

(continued from previous page)

```

| SHA256: 8186a1d140631e6391978c08c35e01efb58963f65a86fddf7dec44eec7681c6b |
-----
| Size: 48272 | Type: application/x-executable | Observed: 1 | VT: 12/61 |
-----
| Observation time frame: N/A |
-----
| STIX network indicators: URLs => 1 | Domains => 1 | IPs: 0 |
-----
Online Reports (availability depends on data retention)
-> MISP EVENT: https://osint.digitalside.it/Threat-Intel/digitalside-misp-feed/
↪ d01c2ad1-0e2c-4b26-9725-f8a86025bd75.json
-> MISP CSV: https://osint.digitalside.it/Threat-Intel/csv/d01c2ad1-0e2c-4b26-9725-
↪ f8a86025bd75.csv
-> DS Report: https://osint.digitalside.it/report/579081f528d9279a87b298b9838c377b.
↪ html
-> STIX: https://osint.digitalside.it/Threat-Intel/stix2/
↪ 579081f528d9279a87b298b9838c377b.json
#####
↪ #####

```

### 1.3.3 Multiple items using --file with JSON output

Example file ioc.txt.

```

~$ cat ioc.txt
7cb796c875cccc9233d82854a4e2fdf0
monke.re

```

Response.

```

~$ apiosintDS -f ioc.txt -st
{
  "domain": {
    "items": [
      {
        "item": "monke.re",
        "response": true,
        "response_text": "Item found in latestdomains.txt list",
        "related_urls": [
          {
            "url": "h[REMOVED]p://monke.re/arm7",
            "hashes": {
              "md5": "318323c9da34bf25833f7da32eab23d6",
              "sha1": "e2bb927b08ebcbaad8f304d02309af776312c9bf",
              "sha256":
↪ "bb1f9e108daa389e62b79067d1cdbef548f9934c9cc85a92565da7063cf36f89"
            },
            "online_reports": {
              "MISP_EVENT": "https://osint.digitalside.it/Threat-Intel/
↪ digitalside-misp-feed/f83d06e6-aa2f-452e-a19d-59d40e874355.json",

```

(continues on next page)

(continued from previous page)

```

        "MISP_CSV": "https://osint.digitalside.it/Threat-Intel/csv/
↪ f83d06e6-aa2f-452e-a19d-59d40e874355.csv",
        "OSINTDS_REPORT": "https://osint.digitalside.it/report/
↪ 318323c9da34bf25833f7da32eab23d6.html",
        "STIX": "https://osint.digitalside.it/Threat-Intel/stix2/
↪ 318323c9da34bf25833f7da32eab23d6.json",
        "STIXDETAILS": {
            "observed_time_frame": false,
            "indicators_count": {
                "hashes": 3,
                "urls": 1,
                "domains": 1,
                "ipv4": 0
            },
            "tlp": "white",
            "first_observed": "2023-07-06 23:51:01",
            "last_observed": "2023-07-06 23:51:01",
            "virus_total": {
                "vt_detection_ratio": "14/61",
                "vt_report": "https://www.virustotal.com/gui/file/
↪ bb1f9e108daa389e62b79067d1cdbef548f9934c9cc85a92565da7063cf36f89/detection"
            },
            "filename": "arm7",
            "filesize": 57148,
            "mime_type": "application/x-executable",
            "number_observed": 1
        }
    },
    {
        "url": "h[REMOVED]p://monke.re/mips",
        "hashes": {
            "md5": "579081f528d9279a87b298b9838c377b",
            "sha1": "45048073aad5997881dffe41e32f9b17beb1c2e1",
            "sha256":
↪ "8186a1d140631e6391978c08c35e01efb58963f65a86fddf7dec44eec7681c6b"
        },
        "online_reports": {
            "MISP_EVENT": "https://osint.digitalside.it/Threat-Intel/
↪ digitalside-misp-feed/d01c2ad1-0e2c-4b26-9725-f8a86025bd75.json",
            "MISP_CSV": "https://osint.digitalside.it/Threat-Intel/csv/
↪ d01c2ad1-0e2c-4b26-9725-f8a86025bd75.csv",
            "OSINTDS_REPORT": "https://osint.digitalside.it/report/
↪ 579081f528d9279a87b298b9838c377b.html",
            "STIX": "https://osint.digitalside.it/Threat-Intel/stix2/
↪ 579081f528d9279a87b298b9838c377b.json",
            "STIXDETAILS": {
                "observed_time_frame": false,
                "indicators_count": {
                    "hashes": 3,
                    "urls": 1,
                    "domains": 1,

```

(continues on next page)



(continued from previous page)

```

        "ipv4": 0
      },
      "tlp": "white",
      "first_observed": "2023-07-07 00:31:02",
      "last_observed": "2023-07-07 00:31:02",
      "virus_total": {
        "vt_detection_ratio": "12/61",
        "vt_report": "https://www.virustotal.com/gui/file/
↪8186a1d140631e6391978c08c35e01efb58963f65a86fddf7dec44eec7681c6b/detection"
      },
      "filename": "mips",
      "filesize": 48272,
      "mime_type": "application/x-executable",
      "number_observed": 1
    }
  }
}
],
"statistics": {
  "itemsFound": 1,
  "itemsSubmitted": 1
},
"list": {
  "file": "latestdomains.txt",
  "date": "2023-07-07 08:03:07+02:00",
  "url": "https://raw.githubusercontent.com/davidonzo/Threat-Intel/master/
↪lists/latestdomains.txt"
},
},
"hash": {
  "items": [
    {
      "item": "7cb796c875cccc9233d82854a4e2fdf0",
      "response": true,
      "response_text": "Item found in latesthashes.json list",
      "hashes": {
        "md5": "7cb796c875cccc9233d82854a4e2fdf0",
        "sha1": "158514acfa87d0b99e2af07a28004480bbf66e83",
        "sha256":
↪"49e64d72d5ed4fb7967da4b6851d94cdceffe4ba0316587767a13901fe580239"
      },
      "online_reports": {
        "MISP_EVENT": "https://osint.digitalside.it/Threat-Intel/digitalside-
↪misp-feed/d6146389-4294-4a41-b4ca-6e74c74b7f8b.json",
        "MISP_CSV": "https://osint.digitalside.it/Threat-Intel/csv/d6146389-
↪4294-4a41-b4ca-6e74c74b7f8b.csv",
        "OSINTDS_REPORT": "https://osint.digitalside.it/report/
↪7cb796c875cccc9233d82854a4e2fdf0.html",
        "STIX": "https://osint.digitalside.it/Threat-Intel/stix2/
↪7cb796c875cccc9233d82854a4e2fdf0.json",

```

(continues on next page)

(continued from previous page)

```
      "STIXDETAILS": {
        "observed_time_frame": false,
        "indicators_count": {
          "hashes": 3,
          "urls": 1,
          "domains": 0,
          "ipv4": 1
        },
        "tlp": "white",
        "first_observed": "2023-07-04 09:33:03",
        "last_observed": "2023-07-04 09:33:03",
        "virus_total": {
          "vt_detection_ratio": "32/71",
          "vt_report": "https://www.virustotal.com/gui/file/
↪49e64d72d5ed4fb7967da4b6851d94cdceffe4ba0316587767a13901fe580239/detection"
        },
        "filename": "plugmanzx.exe",
        "filesize": 924672,
        "mime_type": "application/x-dosexec",
        "number_observed": 1
      }
    },
    "related_urls": [
      "h[REMOVED]p://185.246.220.60/plugmanzx.exe"
    ]
  }
],
"statistics": {
  "itemsFound": 1,
  "itemsSubmitted": 1
},
"list": {
  "file": "latesthashes.json",
  "date": "2023-07-07 08:03:29+02:00",
  "url": "https://raw.githubusercontent.com/davidonzo/Threat-Intel/master/
↪lists/latesthashes.json"
}
},
"generalstatistics": {
  "url": 0,
  "ip": 0,
  "domain": 1,
  "hash": 1,
  "invalid": 0,
  "duplicates": 0,
  "itemsFound": 2,
  "itemsSubmitted": 2,
  "urlfound": 0,
  "ipfound": 0,
  "domainfound": 1,
  "hashfound": 1
},
},
```

(continues on next page)

(continued from previous page)

```
"apiosintDSversion": "apiosintDS v.2.0"
}
```

## 1.4 Using as Python library

Below a few examples of how to use **apiosintDS** in your code.

```
#!/usr/bin/env python3
from apiosintDS import apiosintDS

try:
    OSINTCHECK = apiosintDS.request(
        entities=['192.168.1.54',
↪ '0a2d170abbf5031566377b01431e3b82d3426301',
        ↪ 'somehost.ext',
        ↪ 'http://www.example.com/malicious.exe'],
        stix=True,
        cache=True,
        cachedirectory="/tmp",
        verbose=True)

    print(OSINTCHECK) # print dict results
except ValueError as e:
    print(e) # some error
```

### 1.4.1 Module contents

**apiosintDS.request**(*entities=list, stix=False, cache=False, cachedirectory=None, clearcache=False, cachetimeout=False, verbose=False, loglevel='DEBUG', logconsole=True, logfile=False, localdirectory=False, \*args, \*\*kwargs*)

Uniq method to query the service. Return a dict that can be validated against the json schema returned by the **apiosintDS.schema()** method.

#### Parameters

**entities** List of entities to be submitted. One per row.

##### Type

list

##### Default

None

##### Allowed

[IPv4|domain|url|hash(['md5', 'sha1', 'sha256'])]

**stix** Download and parse additional information from online STIX report.

**Type**  
boolean

**Default**  
False

---

**Note:** STIX2 reports may be not available due to data retention policy.

---

**cache** Enable cache mode. Downloaded lists will be stored and won't be downloaded until the cache timeout is reached.

**Type**  
boolean

**Default**  
False

**cachedirectory** The cache directory where the script check for cached lists files and where them will be stored on cache creation or update.

**Type**  
string

**Default**  
System tmp directory

**Example**  
/path/to/cachedir

---

**Note:** Must be specified the same every script run unless your are using the system temp directory.

---

**clearcache** Force the script to download updated lists even if the *cachetimeout* period has not yet been reached.

**Type**  
boolean

**Default**  
False

---

**Note:** Must be used in combination with *cache*

---

**cachetimeout** Define the cache timeout in hours.

**Type**  
integer

**Default**  
4

---

**Note:** 0 is allowed but means no timeout. Default value is 4 hours. This option needs to be used in combination with *cache* option configured to True.

---

**verbose** Include unmatched results in report.

**Type**  
boolean

**Default**  
False

**loglevel** Define the log level.

**Type**  
enum

**Default**  
DEBUG

**Allowed**  
[DEBUG | INFO | WARNING | ERROR | CRITICAL]

**logconsole** Suppress log messages to the console's STDOUT.

**Type**  
boolean

**Default**  
True

**logfile** Define the log file path.

**Type**  
string

**Default**  
False

**Example**  
/path/to/logfile.log

---

**Note:** No log file is created by default. STDOUT is used instead.

---

**localdirectory** Associate path to the 'Threat-Intel' directory related to a local project clone. Searches are performed against local data.

**Type**  
string

**Default**  
False

**Example**  
/path/to/git/clone/Threat-Intel/

---

**Note:** Before using this option, clone the GitHub project in a file system where the library has read permissions. Don't forget to use `-depth=1` and `-branch=master` options if you don't want to download all project commits.

```
$ cd /path/to/git/clone/
$ git clone --depth=1 --branch=master https://github.com/davidonzo/Threat-Intel.git
```

When this option is in use, all cache related options are ignored. To update data in your local repository destroy the existing data and clone it again.

```
$ cd /path/to/git/clone/  
$ rm -rf Threat-Intel/  
$ git clone --depth=1 --branch=master https://github.com/davidonzo/Threat-Intel.git
```

apiosintDS.schema()

Return an object containing the json schema.

## 1.5 apiosintDS MISP Module

**apiosintDS** is included as enrichment module in the official [MISP-Modules repository](#). This guide assume you have your MISP instance up and running with MISP Modules correctly initialized.

The module has been specially designed for people and organizations don't want to subscribe the [DigitalSide Threat-Intel MISP Feed](#) and prefer to query it as an on demand service.

**Warning:** If [DigitalSide Threat-Intel MISP Feed](#) is enabled and regularly fetched by your MISP instance, don't use this plugin. All information retrivable by the plugin are just included in your MISP events dataset. The MISP correlation engine should be used instead.

### 1.5.1 Input / Output

**Module type** MISP module type.

**Module-type**

['hover', 'expansion']

**Input** The module runs against the following MISP attributes type.

**Input-attributes**

["domain", "domain|ip", "hostname", "ip-dst", "ip-src", "ip-dst|port",  
"ip-src|port"] ["url", "md5", "sha1", "sha256", "filename|md5",  
"filename|sha1", "filename|sha256"]

**Output** The module returns the following MISP attributes type.

**Output-attributes**

["domain", "ip-dst", "url", "comment", "md5", "sha1", "sha256", "link",  
"text"]

### 1.5.2 Configuration

Go to your MISP web interface and login with a user account able to edit plugins configuration. Once logged in go to Administration >> Server Settings & Maintenance >> Plugin and select the Enrichment tab. Put in the search input filter apiosintds in order to show only the needed configuration settings.

## Enrichment

Recommended	Plugin.Enrichment_apiosintds_enabled	false	[Enable or disable the apiosintds module.] On demand
Recommended	Plugin.Enrichment_apiosintds_restrict	ORGNAME	Restrict the apiosintds module to the given organisation.
Recommended	Plugin.Enrichment_apiosintds_STIX2_details	yes	Set this required module specific setting.
Recommended	Plugin.Enrichment_apiosintds_import_related	yes	Set this required module specific setting.
Recommended	Plugin.Enrichment_apiosintds_cache	false	Set this required module specific setting.
Recommended	Plugin.Enrichment_apiosintds_cache_directory	false	Set this required module specific setting.
Recommended	Plugin.Enrichment_apiosintds_cache_timeout_h	4	Set this required module specific setting.
Recommended	Plugin.Enrichment_apiosintds_local_directory	/usr/local/src/Threat-Intel	Set this required module specific setting.

**Plugin.Enrichment.apiosintds.enabled** MISP internal configuration to enable or disable the module.

**Type**  
boolean

**Default**  
false

---

**Note:** To enable the plugin configure the value to true.

---

**Plugin.Enrichment.apiosintds\_restrict** Restrict the plugin use to a single organization.

**Type**  
enum

**Default**  
No organization selected

**Allowed**  
ORG in the given MISP instance

**Plugin.Enrichment.apiosintds\_STIX2\_details** Download and parse additional information from online STIX report.

**Type**  
enum

**Default**  
no

**Allowed**  
[yes|no]

---

**Note:** STIX2 reports may be not available due to data retention policy.

---

**Plugin.Enrichment.apiosintds\_import\_related** Parse and include in the results related items.

**Type**  
enum

**Default**  
no

**Allowed**  
[yes|no]

---

**Note:** Is strongly recommended to configure it to `yes` to obtain best results.

---

**Plugin Enrichment `apiosintds_cache`** Enable cache mode. Downloaded lists will be stored and won't be downloaded until the cache timeout is reached.

**Type**  
enum  
**Default**  
no  
**Allowed**  
[yes|no]

**Plugin Enrichment `apiosintds_cache_directory`** The cache directory where the script check for cached list files and where them will be stored on cache creation or update.

**Type**  
string  
**Default**  
None  
**Example**  
/path/to/cachedir

---

**Note:** Read and write permissions are required for the system user running the MISP instance (depends on your installation configuration, should be one between `www-data`, `misp`, `apache`, others...)

---

**Plugin Enrichment `apiosintds_cache_timeout_h`** Define the cache timeout in hours.

**Type**  
integer  
**Default**  
4

---

**Note:** `0` is allowed but means no timeout. Default value is 4 hours. This option needs to be used in combination with `apiosintds_cache` option configured to `True`.

---

**Plugin Enrichment `apiosintds_local_directory`** Absolute path to the Threat-Intel directory related to a local project clone. Searches are performed against local data.

**Type**  
string  
**Default**  
Empty  
**Example**  
/path/to/git/clone/Threat-Intel/

---

**Note:** Before using this option, clone the GitHub project in a file system where the library has read permissions. Don't forget to use `-depth=1` and `-branch=master` options if you don't want to download all project commits. Make sure the system user running the MISP instance has read permissions on the directory.



```
$ cd /path/to/git/clone/
$ git clone --depth=1 --branch=master https://github.com/davidonzo/Threat-Intel.git
$ chown -R $MISP_SYSTEM_USER:$MISP_SYSTEM_GROUP Threat-Intel
```

When this option is in use, all cache related options are ignored. To update data in your local repository destroy the existing data and clone it again.

```
$ cd /path/to/git/clone/
$ rm -rf Threat-Intel/
$ git clone --depth=1 --branch=master https://github.com/davidonzo/Threat-Intel.git
$ chown -R $MISP_SYSTEM_USER:$MISP_SYSTEM_GROUP Threat-Intel
```

### 1.5.3 Usage: hover

Using the module as hover plugin retrieved data will be displayed as follow.

```

Apiosintds:
IoC 'itrevolution.in' found in OSINT.DigitalSide.it repository.
List file: latestdomains.txt. Date list: 2023-07-08 08:03:29+02:00
#####
-----
Related URLs count: 3
-----
Related URL http://itrevolution.in/3qN9jJaXKsSA8e0LiGHt.exe
MD5: 173f2817975d278fcc3163d9b5302467
SHA1: 2791a718e4b410d4a24167609278267292c6d957
SHA256: e71dc666516aef6a041e1d0320bc62cdc13ba901ff5ce978f79c93f8dcb37389
-----
Online Reports (availability depends on retention)
MISP Event => https://osint.digitalside.it/Threat-Intel/digitalside-misp-feed/44bb970c-9106-4ec1-b2a7-6be1209fd6fc.json
MISP CSV => https://osint.digitalside.it/Threat-Intel/csv/44bb970c-9106-4ec1-b2a7-6be1209fd6fc.csv
DigitalSide report => https://osint.digitalside.it/report/173f2817975d278fcc3163d9b5302467.html
STIX report => https://osint.digitalside.it/Threat-Intel/stix2/173f2817975d278fcc3163d9b5302467.json
-----
STIX2 report details
TLP:white | Observation: 1 | First seen: 2023-07-08 06:19:03 | First seen: 2023-07-08 06:19:03
Filename: 3qN9jJaXKsSA8e0LiGHt.exe
Filesize in bytes: 547328
Filetype: application/x-dosexec
VirusTotal Ratio: 39/70
-----

```

## 1.5.4 Usage: enrichment

Using the module as enrichment plugin retrieved data will be imported as follow.

### Enrichment Results

Below you can see the attributes that are to be created. Make sure that the categories and the types are correct, often several options will be offered based on an inconclusive automatic resolution.

Proposals instead of attributes

Value	Similar Attributes	Category	Type	IDS <input type="checkbox"/>	Disable Correlation <input type="checkbox"/>	Distribution	Comment
IoC 'itrevolution.in' found in OSINT.DigitalSide.it repository. List fil		Other	text	<input type="checkbox"/>	<input type="checkbox"/>	Inherit event	itrevolution.in: Enriched via the aq
http://itrevolution.in/3qN9jJaXKsSA8e0LiGHt.exe	1 802	Network activity	url	<input type="checkbox"/>	<input type="checkbox"/>	Inherit event	Download URL for 173f2817975d
173f2817975d278fcc3163d9b5302467	802	Payload delivery	md5	<input type="checkbox"/>	<input type="checkbox"/>	Inherit event	Related to: http://itrevolution.in/3c
2791a718e4b410d4a24167609278267292c6d957	802	Payload delivery	sha1	<input type="checkbox"/>	<input type="checkbox"/>	Inherit event	Related to: http://itrevolution.in/3c
e71dc666516aef6a041e1d0320bc62cdc13ba901ff5ce978f79c93	802	Payload delivery	sha256	<input type="checkbox"/>	<input type="checkbox"/>	Inherit event	Related to: http://itrevolution.in/3c
https://osint.digitalside.it/Threat-Intel/digitalside-misp-feed/44bb9		External analysis	link	<input type="checkbox"/>	<input type="checkbox"/>	Inherit event	MISP Event related to: itrevolution
https://osint.digitalside.it/Threat-Intel/csw/44bb970c-9106-4ec1-b		External analysis	link	<input type="checkbox"/>	<input type="checkbox"/>	Inherit event	MISP CSV related to: itrevolution.
https://osint.digitalside.it/report/173f2817975d278fcc3163d9b530		External analysis	link	<input type="checkbox"/>	<input type="checkbox"/>	Inherit event	DigitalSide report related to: itrev
https://osint.digitalside.it/Threat-Intel/stix2/173f2817975d278fcc3		External analysis	link	<input type="checkbox"/>	<input type="checkbox"/>	Inherit event	STIX2 report related to: itrevolution
TLP:white   Observation: 1   First seen: 2023-07-08 06:19:03   Fil		Other	comment	<input type="checkbox"/>	<input type="checkbox"/>	Inherit event	STIX2 details for: itrevolution.in
3qN9jJaXKsSA8e0LiGHt.exe	802	Payload delivery	filename	<input type="checkbox"/>	<input type="checkbox"/>	Inherit event	STIX2 details for: itrevolution.in
547328		Other	size-in-bytes	<input type="checkbox"/>	<input type="checkbox"/>	Inherit event	STIX2 details for: itrevolution.in
application/x-dosexec	20 21 22 23 24 25 27 28 29 30 <small>10 +more</small>	Artifacts dropped	mime-type	<input type="checkbox"/>	<input type="checkbox"/>	Inherit event	STIX2 details for: itrevolution.in
VirusTotal Ratio: 39/70		Other	comment	<input type="checkbox"/>	<input type="checkbox"/>	Inherit event	STIX2 details for: itrevolution.in

## 1.6 Changelog

### 1.6.1 2.0.1 (2023-07-07)

- Bug fix to stix reports cache management

### 1.6.2 2.0 (2023-07-07)

- Many minor bug fixes
- Implemented python getLogger as suggested in issue #2
- Added --stix option. Dowload and parse additional information from online STIX report.
- Added --pretty option. Show results in terminal with a little bit of formatting applied.
- Added --nocolor option. Suppers colors in --pretty output. For accessibility purpose.
- Added --cachetimeout option. Define the cache timeout in hours.
- Added --localdirectory option. Absolute path to the 'Threat-Intel' directory related to a local project clone. Searches are performed against local data.
- Added --logfile option. Define the log file path.
- Added --loglevel option. Define the log level.
- Added --logconsole option. Suppress log messages to the console's *STDOUT*.
- Added --version option. Show the library version.
- Improved apiosintDS.request method according new available options.
- New MISP Module plugin version

- Documentation updated

### **1.6.3 1.8.2 (2019-10-25)**

- Bug fix for cache management of latesthashes.txt list

### **1.6.4 1.8 (2019-10-22)**

- Added MD5/SHA1/SHA256 strings as entity to search
- Added lookup to hash files for hash entities
- Added support su hash lookup for related urls detected
- Minor bug fixes
- New schema json for response

### **1.6.5 1.7 (2019-10-20)**

- Added support to be used as standard python library
- Added docs
- Minor bug fixes

### **1.6.6 1.6 (2019-10-13)**

- Not a real new release. Just added support to pip.

### **1.6.7 1.6 (2019-10-13)**

- First release for python library version usable as CLI tool.
- Added Cache support
- Multiple IoCs submission via text file
- Output management
- New schema response

### **1.6.8 1.0 (2019-10-07)**

- Released version 1.0 published on [DigitalSide Threat-Intel](#) repository.

## 1.7 License

MIT License

Copyright (c) 2019 Davide Baglieri

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the “Software”), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED “AS IS”, WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

## Symbols

-c, --cache (*configuration value*), 5  
 -cc, --clearcache (*configuration value*), 6  
 -cd, --cachedirectory (*configuration value*), 5  
 -ct, --cachetimeout (*configuration value*), 6  
 -e, --entity (*configuration value*), 4  
 -f, --file (*configuration value*), 4  
 -h, --help (*configuration value*), 4  
 -i, --info (*configuration value*), 7  
 -l, --logfile (*configuration value*), 7  
 -lc, --logconsole (*configuration value*), 7  
 -ld, --localdirectory (*configuration value*), 6  
 -ll, --loglevel (*configuration value*), 7  
 -nc, --nocolor (*configuration value*), 5  
 -o, --output (*configuration value*), 5  
 -p, --pretty (*configuration value*), 5  
 -s, --schema (*configuration value*), 7  
 -st, --stix (*configuration value*), 4  
 -v, --verbose (*configuration value*), 5  
 -vv, --version (*configuration value*), 7

## C

cache (*configuration value*), 16  
 cachedirectory (*configuration value*), 16  
 cachetimeout (*configuration value*), 16  
 clearcache (*configuration value*), 16

## E

entities (*configuration value*), 15

## I

Input (*configuration value*), 18

## L

localdirectory (*configuration value*), 17  
 logconsole (*configuration value*), 17  
 logfile (*configuration value*), 17  
 loglevel (*configuration value*), 17

## M

Module type (*configuration value*), 18

## O

Output (*configuration value*), 18

## P

Plugin.Enrichment\_apiosintds\_cache (*configuration value*), 20  
 Plugin.Enrichment\_apiosintds\_cache\_directory (*configuration value*), 20  
 Plugin.Enrichment\_apiosintds\_cache\_timeout\_h (*configuration value*), 20  
 Plugin.Enrichment\_apiosintds\_enabled (*configuration value*), 19  
 Plugin.Enrichment\_apiosintds\_import\_related (*configuration value*), 19  
 Plugin.Enrichment\_apiosintds\_local\_directory (*configuration value*), 20  
 Plugin.Enrichment\_apiosintds\_restrict (*configuration value*), 19  
 Plugin.Enrichment\_apiosintds\_STIX2\_details (*configuration value*), 19

## S

stix (*configuration value*), 15

## V

verbose (*configuration value*), 16