# **MISP-STIX**

## THE HOLY GRAIL FOR MISP AND STIX FORMATS

MISP core team - Christian Studer TLP:WHITE

MISP PROJECT https://www.misp-project.org/



CTI SUMMIT (CTIS-2022)

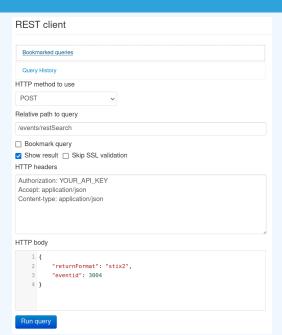
#### **SUMMARY**

- Past & current status
- Recent changes
- Continuous improvement & future roadmap
- Organisational & philosophical aspects
- Demo (?)

### MISP & STIX

- **■** Built-in integration
- Export & Import features
  - ► Export MISP Events collections
  - ► Import STIX files
- Supported version
  - ► STIX 1.1.1
  - ► STIX 2.0
- Accessible via restSearch

#### STIX CONVERSION USAGE IN MISP



#### STIX CONVERSION USAGE IN MISP

#### Response

Queried URL: https://iglocska.eu/events/restSearch Response code: 200

Request duration: 3714.93 ms

Response headers

Date: Wed, 12 Oct 2022 11:30:55 GMT

Server: Apache/2.4.29 (Ubuntu)

Content-Length: 20803

X-Result-Count: 1

X-Export-Module-Used: stb2 X-Beanonse-Format: ison

Content-Disposition: attachment: filename, "misp.event.3004.ison"

Connection: close

#### Content-Type: application/json; charset=UTF-8 Raw JSON HTML Download

("type": "bundle", "spec\_version": "2.8", "id": "bundle - e86f9cb3 -757a-4799-8775-968cd843dfb7", "objects": [{"type": "identity - 566d3b39-9db9-44b9-8869-7f56a5e38e14", "created": "2022-19-11711:34:13.090Z", "modified" vpe": "report", "id": "report--a2df99c2-4b96-4d24-9000-49acd1855e22", "created by ref": "identity--5db63b38-9db0-44b9-8869-7f56a5e38e14", "created": "2022-10-11711:34:13.0002", "modified": "2022-10-11711:34:13.0002", "name": "Flubot m sp-object-263c2e72-80f6-492f-994f-fa25795d5e6b", "course-of-action-ec42d8be-f762-4127-80f4-f079ea6d7135", "indicator--1fa8ba4e-dcd7-497f-aa6b-bcd276e65ff0", "malware--ef91833f-3334-4955-9218-f196494e9fc0", "indicator--24600ccd-8f43ty--0740119a-7941-4ab1-81d7-1e2098bfbfc3", "x-misp-object--7fbd8f19-3fb4-4a7f-b362-59d883b59d84", "x-misp-object--6a8d3fbf-3f9d-48c7-8366-29da37f3cd92", "x-misp-object--102d8d6d-dedd-4d33-bb43-c73727a646e1", "observed-data--337c0935-a 1". "relationship--e8608d8-038a-4656-881e-ff62088732d3", "relationship--04d18fef-c917-48ca-bedd-2d9ac64ba04e", "relationship--06135d9e-dd61-4282-9509-45bd0426682b", "relationship--2ccc388f-33a3-4201-9b35-96017c4bdff8", "relationship--06135d9e-dd61-4282-9509-45bd0426682b", "relationship--2ccc388f-33a3-4201-9b35-96017c4bdff8", "relationship--06135d9e-dd61-4282-9509-45bd0426682b", "relationship--2ccc388f-33a3-4201-9b35-96017c4bdff8", "relationship--2ccc388f-33a3-4201-9b35-96017c4bdff8", "relationship--2ccc388f-33a3-4201-9b35-96017c4bdff8", "relationship--36135d9e-dd61-4282-9509-45bd0426682b", "relationship--2ccc388f-33a3-4201-9b35-96017c4bdff8", "relationship--36135d9e-dd61-4282-9509-45bd0426682b", "relationship--3ccc388f-33a3-4201-9b35-96017c4bdff8", "relationship--3ccc388f-33a3-4201-9b35-96017c4bdff8", "relationship--3ccc388f-33a3-4201-9b35-96017c4bdff8", "relationship--3ccc388f-33a3-4201-9b35-96017c4bdff8", "relationship--3ccc388f-3aa-4656-8ba04-TIX.Converter\"" "nsint'lifetime\"nernetual\"" "osint'certaintya\"50\"" "PAD'MHITF" "enisa:mefarious.activity.abusea\"mobile.malware\"" "circl'incident.classificationa\"malware\"" "euronol.incident malware\"" "euronol.i lassification=\"vulnerability\""\. "object marking refs": ["marking-definition--613f2e26-497d-48c7-9eca-b8e91df99dc9"\), ("type": "x-misp-object", "id": "x-misp-object--263c2e72-89f6-492f-994f-fa25799d5e6b", "created by ref": "identit ed": \*2022-10-11T10:51:55.0002", "labels": ["miso:name"\"short-message-service\"", "miso:meta-category=\"misc\""], "x miso attributes": [["type": "text", "object relation": "body", "value": "Missed Call: You have a missed call.\r\nCall uuid": "97f2cbee-e14f-4145-bf8f-01376719303d"), ("type": "phone-number", "object\_relation": "from", "value": "+352131575", "category": "Person", "uuid": "18b5bffb-ffb3-4841-9714-94b6ccb7d6377"]], "x\_misp\_comment": "malicious sms", "x\_m -action", "id": "course-of-action--ec42d8be-f762-4127-88f4-f879ea6d7135", "created": "2822-19-11711:16:48,0982", "modified": "2822-19-11711:16:48,0992", "name": "Indicator Blocking Mitigation - T1854", "description": "ATTACK Mitigation s, and other associated mechanisms are secured with appropriate permissions and access controls. Consider automatically relaunching forwarding mechanisms at recurring intervals (ex: temporal, on-logge, etc.) as well as applying appropriate permissions. bels": ["misp:qalaxy-name=\"Course of Action\"", "misp:qalaxy-type=\"mitre-course-of-action\"", "misp-qalaxy:mitre-course-of-action\"| Mitigation - Ti054\""], "external\_references": [{"source\_name": "mitre-attack", " b-bcd276e55ff9", "created by ref": "identity-5d6d3b38-9db0-4409-8869-7f56a5e38e14", "created": "2822-10-i1711:16:40.0082", "modified": "2822-10-i1711:16:40.0082", "description": "malicious sms url", "pattern": "furl; value = 'https:// without tld = 'evilorovider' AND url:x miso in = '8.231.77.176' AND url:x miso opery string = 'e1525c9f']", "valid from": "2922-93-12713:27:997", "kill chain phases": [{"kill chain name": "miso-category", "phase name": "network"], " e\""]}, {"type": "malware", "id": "malware-ef918337-3334-4955-9218-f106494e9fc0", "created": "2022-10-11711:08:28.000Z", "name": "FluBot", "description": "Malware galaxy based on Malpedia archi ce the first quarter of 2021 it has been targeting many other European countries as well as Japan. It uses a DGA for it's CGC and relies on both DMS and DMS-over-HTTPS for name resolution. Despite arrests of multiple people suspected ce.". "kill chain phases": [("kill chain phases": "misp-category". "phase name": "misp-category". "phase name": "misp-category". "misp-calaxy-names\"Malgedia\"". "misp-galaxy-types\"malgedia\"". "mi 0.9db0.44b9.8869.7f56a5x38e14", "created": "2022-10-11T11:08:28:000Z", "modified": "2022-10-11T11:08:28:000Z", "description": "malicious apk from malicious url", "pattern": "[file:hashes.MD5 = 'fia3x62de12faecee82bf4599ccifdcd' AND fi 9481429988dbb4b3488a396457e8fffc57577c9d5eee015578ff6a3ada12e' AND file:name = 'samole.apk.exe' AND file:size = '751328' AND (file:content ref.x miso filename = 'samole.apk.exe' AND file:content ref.hashes.MD5 = 'fia3e62de12faecee82b -10-11711:08:282", "kill\_chain\_phases": [{"kill\_chain\_name": "misp-category", "phase\_name": "file"}], "labels": ["misp:name-\"file\"", "misp:meta-category-\"file\"", "misp:to\_ids-\"True\"", "malware\_classification:malware-category-\"\$ 6", "created by ref": "identity--5d8d3b30-9mb0-44b9-8869-7f56a5e38e14", "created: "2022-10-11T11:16:40.000Z", "modified": "2022-10-11T11:16:40.000Z", "description": "c2c server", "pattern": "[url:value = 'https://another.evil.provide x miso query string = 'aif9f536']", "valid from": "2022-10-11711:16:40Z", "kill chain phases": [f"kill chain name": "miso-category", "phase name": "network"], "labels": [fmiso:name=\"url\"", "miso:meta-category\"\"network\"", "miso:meta-category\"\"network\"", "miso:meta-category\"\"network\"", "miso:meta-category\"\"network\"", "miso:meta-category\"\"network\"", "miso:meta-category\"\"network\"", "miso:meta-category\"\"network\"", "miso:meta-category\"\"network\"", "miso:meta-category\"\"network\"", "miso:meta-category\"\", "miso:meta-cate 7-ie2d98bfbfc3", "created\_by\_ref": "identity--5d633b39-9d80-44b9-8869-7f56a5e38e14", "created": "2022-19-i1719:36:34.0002", "modified": "2022-19-i1719:36:34.0002", "name": "CVE-2022-27835", "labels": ["misp:name=\"vulnerability\"", "m [{"source name": "cve", "external id": "CVE-2022-27835"}]}, {"type": "x-misp-object", "id": "x-misp-object--7fbd8f19-3fb4-4a7f-b182-503893b59494", "created by ref": "identity--5d63b30-9d00-44b9-8889-7f58a5e38e14", "created": "2022-19 a\"", "misp:meta-category=\"misc\""1, "x misp attributes": [("type": "comment", "object relation": "comment", "value": "vara rule to detect CVE-2922-27835", "category": "Other", "uuid": "bi5c809a-6878-4166-b94f-9879dddidbi8"), ("type" "c76b6bd3-2ba5-46f5-8f35-52ad12ba8288"), {"type": "text", "object\_relation": "version", "value": "3.7.1", "category": "Other", "uuid": "5568dfd7-67e7-487f-bde2-c36645841894"), {"type": "yara", "object\_relation": "yara", "value": "rule description = \"matches on dumped, decrypted V/DEX files of Flubot version > 4.2\"\r\n sample = \"37be18494cd03ea70affdd6270cef6e3\"\r\n\r\n strings:\r\n Ss2 = \"iava/net/HttpURLConnection:\"\r\n (Sdex at 0 or Sydex at 0)\r\n 817824c6de"), {"type": "text", "object\_relation": "yara-rule-name", "value": "android\_flubot", "category": "Other", "uuid": "8da65be2-18b4-428c-8ddf-438ic378e38b"}], "x\_misp\_comment": "yara-rule to detect CVE-2822-27835", "x\_misp\_meta ct-6a9d3fbf-3f9d-49c7-8366-29da37f3cs92", "created by ref": "identity--5d6d3b39-9db6-44b9-8869-7f56a5c38e14", "created": "2822-19-11711;34:13.0902", "modified": "2922-19-11711;34:13.0902", "labels": ["miso:name=\"queolocation\"", "miso:name=\"queolocation\"", "miso:name=\"queolocation\", "miso:name=\"queolo ountry", "value": "United States", "category": "Other", "comment": "8.231,77.176; enriched via the mmdb lookup module,", "uuid": "328b624d-8ddb-4579-98bc-ee75fc71665b"), ("type": "text", "object relation": "countrycode", "value": "US" "uuid": "a5397d9a.3461-42f1-be85-fc33ad7625fb"], {"type": "float", "object\_relation": "latitude", "value": "38", "category": "Other", "comment": "8.231.77.176: enriched via the mmdb\_lookup module.", "uuid": "337a8523-481c-48d6-ba30-a7 v": "Other", "comment": "8,231,77,176; enriched via the mmdb lookup module,", "uuid": "86284fe-2636-496d-bdf1-d821d9bda715"}, ("type": "text", "object relation": "text", "value": "db source: GeoOpen-Country, build db: 2822-97-89 67:1 31.77.176; enriched via the mmdb lookup module.". "wuid": "277fb8ac-a0b9-4473-bd55-89c2635d3d82"\lambda. "x misp comment": "8.231.77.176; enriched via the mmdb lookup module.". "x misp meta category": "misc". "x misp name": "geolocation"\lambda. "created\_by\_ref": "identity--5d6d3b30-9db0-44b9-8869-7f56a5e38ei4", "created: "2022-10-11Ti1:34:13.000Z", "modified": "2022-10-11Ti1:34:13.000Z", "labels": ["misp:name=\"qeolocation\"", "misp:meta-category=\"misc\""], "x\_misp\_attribu v": "Other", "comment": "8,231,77,176; enriched via the mmdb lookup module,", "puid": "f13c9364-da6c-4292-8ic8-793495e8253d"), ("type": "text", "object relation": "countrycode", "value": "US", "category": "Other", "comment": "8,231,77 b4"), {"type": "float", "object\_relation": "latitude", "value": "38", "category": "Other", "comment": "8.231.77.176: enriched via the mmdb\_lookup module.", "uuid": "053e1a9b-0565-4a52-ba72-07c4f9c29079"}, {"type": "float", "object\_rel

#### STIX CONVERSION USAGE IN MISP

```
cURL
        PvMISP
curl \
 -d '{"returnFormat":"stix2", "eventid":3004}' \
 -H "Authorization: YOUR_API_KEY
 -H "Accept: application/json" \
 -H "Content-type: application/json" \
 -X POST https://iglocska.eu/events/restSearch
cURI
        PyMISP
misp_url = 'https://iglocska.eu'
misp_key = YOUR API KEY
misp_verifycert = True
relative path = 'events/restSearch'
body = {
    "returnFormat": "stix2",
    "eventid": 3004
from pymisp import ExpandedPyMISP
misp = ExpandedPyMISP(misp_url, misp_key, misp_verifycert)
misp.direct_call(relative_path, body)
```

5 | 24

#### FORMER FEATURE LIMITATIONS

- **Supported versions** 
  - ► 1.1.1 XML (& JSON)
  - ▶ 2.0
- Data type support



### FORMER FEATURE LIMITATIONS

- Supported versions
  - ► 1.1.1 XML (& JSON)
  - ▶ 2.0
- Data type support

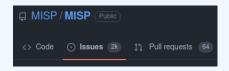


### FORMER PRACTICAL & ORGANISATIONAL LIMITATIONS

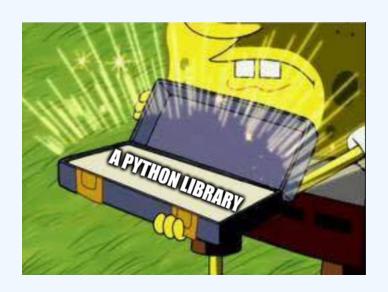
- Export and import features only available via MISP
  - ► Need an automation key (and/or to deal with the UI)
- **Github**: STIX issues lost within the MISP core issues

### FORMER PRACTICAL & ORGANISATIONAL LIMITATIONS

- Export and import features only available via MISP
  - ► Need an automation key (and/or to deal with the UI)
- Github: STIX issues lost within the MISP core issues



# THE SOLUTION



#### **KEY FEATURES**

- Support all the STIX versions
  - ► STIX 2.1 Support
  - ► 1.1.1, 1.2, 2.0 Support enhanced
- Various MISP data collection supported
- **■** Mapping documentation

#### HANDLING THE CONVERSION WITH A PYTHON LIBRARY

- Used in MISP built-in export modules
- Enable a **stand-alone** use of the python code<sup>1</sup>
  - Pass filenames & get the converted content written in 1 or more result file(s)
- Possible integration within python code
  - Give it a list of filenames
  - MISP standard format <-> STIX
    - JSON or PyMISP

<sup>&</sup>lt;sup>1</sup>i.e command line

#### LIBRARY USAGE - COMMAND LINE

```
post_chistod -/qLLT/MISP-MISP-STIX-Converter () (q1::dev) postry run mays sixt converter :h usage: misp_stix_converter [-h] [-v (1.1.1.1.2,2.0,2.1]] [-f FILE [FILE ...]] [-s] [-t] [--feature {attribute,event}] [--format ()son,xml)] [-n NAMESPACE] [-o ORG] convert MISP <> STIX potentials of the state of
```

#### LIBRARY USAGE - PYTHON INTEGRATION

```
ui chrisr3d ~/git/MISP/MISP-STIX-Converter
                        , id='identity--5a8e935e-5484-488c-852c-776f7c7cf985', created='2020-06-17T11:36:58.000Z', modified='2020-06-17T11:36'
  000Z', name='ORGNAME 387', identity class='organization', revoked=False), Identity(type='identity', spec version='2.1', id='identity', i
 ator--5abb8534-4368-4bb2-adf1-02480a00020f'. 'indicator--5abb8534-123c-4ed4-8e80-02480a00020f'. 'indicator--5abb8534-1014-4283
alfc-02480a00020f', 'indicator--5abb8534-d930-4139-8263-02480a00020f', 'indicator--5abb8534-4840-4087-al6a-02480a00020f', 'sigh
    ing--5d7a49a7-8f8c-42a1-8f7b-72e9a964451a'. 'indicator--5abb8534-a8d0-4956-812f-02480a00020f'. 'indicator--5abb8534-1ab4-
```

#### MAPPING DOCUMENTATION

- Mapping overview
  - Quick overview on how MISP data structures are mapped with STIX objects
- Detailed mapping
  - Extended explanation on how each granular data is mapped with STIX objects fields

2.

#### **WORK IN PROGRESS & CONTINUOUS DEVELOPMENT**

#### ■ STIX 2 -> MISP import feature

- Current mapping improvement
  - Support for Custom Galaxy clusters
  - ► Better support of existing STIX objects libraries²
  - ► Support custom STIX format<sup>3</sup>

<sup>&</sup>lt;sup>2</sup>e.g: https://github.com/mitre/cti

<sup>&</sup>lt;sup>3</sup>e.g: ACS custom markings

#### **WORK IN PROGRESS & CONTINUOUS DEVELOPMENT**

- STIX 2 -> MISP import feature
- Current mapping improvement
  - Support for Custom Galaxy clusters
  - ► Better support of existing STIX objects libraries²
  - ► Support custom STIX format<sup>3</sup>

#### **■ TAXII integration**



<sup>&</sup>lt;sup>2</sup>e.g: https://github.com/mitre/cti

<sup>&</sup>lt;sup>3</sup>e.g: ACS custom markings

### WHAT COMES NEXT?

- Extend the export feature to any kind of data collection
- Add notes on any data structure
- Sightings on context layers
- Port the STIX 1 -> MISP import feature

# HANDLING DIFFERENT STIX CONTENT CREATION DESIGNS

- Impossible to control the content created by external parties
- We want to keep UUIDs

# HANDLING DIFFERENT STIX CONTENT CREATION DESIGNS

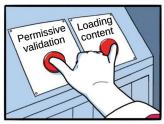
- Impossible to control the content created by external parties
- We want to keep UUIDs
- Facing UUIDs validation issues
  - Loading error





### AN EASY FIX: A STIX 2 PYTHON LIBRARY FORK4

- No change on the content validation
  - Differs only on the UUIDs validation process
- MISP has now the same UUIDs requirements
  - We keep a reference to the initial UUID
  - ► A UUID v5 is generated





"https://github.com/MISP/cti-python-stix2 &
https://pypi.org/project/misp-lib-stix2/

#### MINDING THE GAP BETWEEN FORMATS

- From a sharing platform to an threat intelligence exchange format
  - Custom STIX objects
  - Custom fields in existing objects
  - ► STIX extensions
- Handling the infinite possibilities of a patterning language
  - ► Importing STIX 2 patterns in separate MISP objects

#### MINDING THE GAP BETWEEN FORMATS

- From a sharing platform to an threat intelligence exchange format
  - Custom STIX objects
  - Custom fields in existing objects
  - STIX extensions
- Handling the infinite possibilities of a patterning language
  - ► Importing STIX 2 patterns in separate MISP objects

#### MAPPING CHALLENGES

- Attack Pattern (Cluster)
- Campaign (Cluster)
- Course of Action (Cluster / Object depends on context action taken vs action to be taken)
- Grouping (Event)
- Identity (Cluster / Attribute / Object)
- Indicator (Object/Attribute)
- Intrusion Set (Cluster)
- Location (Object/Attribute)
- Malware (Cluster / Object)
- Note (Neither To be defined)
- Observed Data (Object / Attribute)
- Report (Event / Event Report)
- Threat Actor (Cluster)
- Tool (Cluster + Object (Concept of a tool + file attachment))
- Vulnerability (??? if known vulnerability -> cluster / if in progress -> object) ???

#### **EVOLUTION PERSPECTIVES**



- Members of the Oasis CTI TC
  - Our involvement
    - Participating to the development process
  - Our proposal: Go for the open source way
    - Make the contribution process more accessible=> Bring more contributers / contributions
    - Easier access to the resources
      - => More visibility

## How to report bugs/issues

- Github issues
  - ► https://github.com/MISP/misp-stix/issues
  - ► https://github.com/MISP/MISP/issues
- Please provide details
  - ► How did the issue happen
  - ► **Recommendation**: provide samples
- Any feedback welcome

### USEFUL LINKS

- https://github.com/MISP/misp-stix
- https://github.com/MISP/misp-stix/tree/main/ documentation
- https://github.com/MISP
- https://www.misp-project.org/
- https://twitter.com/MISPProject
- https://twitter.com/chrisred 68

#### **DEMO TIME**

