Sharing Information and Providing Feedback using MISP

CIRCL
Computer Incident
Response Center
Luxembourg

MISP
Threat Sharing

Andras Iklody @iglocska

TLP:WHITE

Suricon 2016-11-09

Quick MISP introduction

- During a malware analysis workgroup in 2012, we discovered that we worked on the analysis of the same malware.
- We wanted to share information in an easy and automated way **to avoid duplication of work**.
- Christophe Vandeplas (then working at the CERT for the Belgian MoD) showed us his work on a platform that later became MISP.
- Over time, user feedback helped to improve the tool.
- Today, MISP[1] is a community-driven development, used by Governments, Financial Institutions, Critical Infrastructure and private sector.

[1] https://github.com/MISP/MISP

Development based on practical user feedback

- There are many different types of users of an information sharing platform like MISP:
  - **Malware reversers** willing to share indicators of analysis with respective colleagues.
  - **Security analysts** searching, validating and using indicators in operational security.
  - **Intelligence analysts** gathering information about specific adversary groups.
  - **Law-enforcement** relying on indicators to support or bootstrap their DFIR cases.
  - **Risk analysis teams** willing to know about the new threats, likelyhood and occurences.
  - **Fraud analysts** willing to share financial indicators to detect financial frauds.

Many objectives from different user-groups

- Sharing indicators for **detection**.
  - 'Do I have infected systems in my infrastructure or the ones I operate?'
- Sharing indicators to **block**.
  - 'I use these attributes to block, sinkhole or divert traffic.'
- Sharing indicators to **perform intelligence**.
  - 'Gathering information about campaigns and attacks. Are they related? Who is targeting me? Who are the adversaries?'
- $\rightarrow$ These objectives can be conflicting (e.g. False-positives have different impacts)

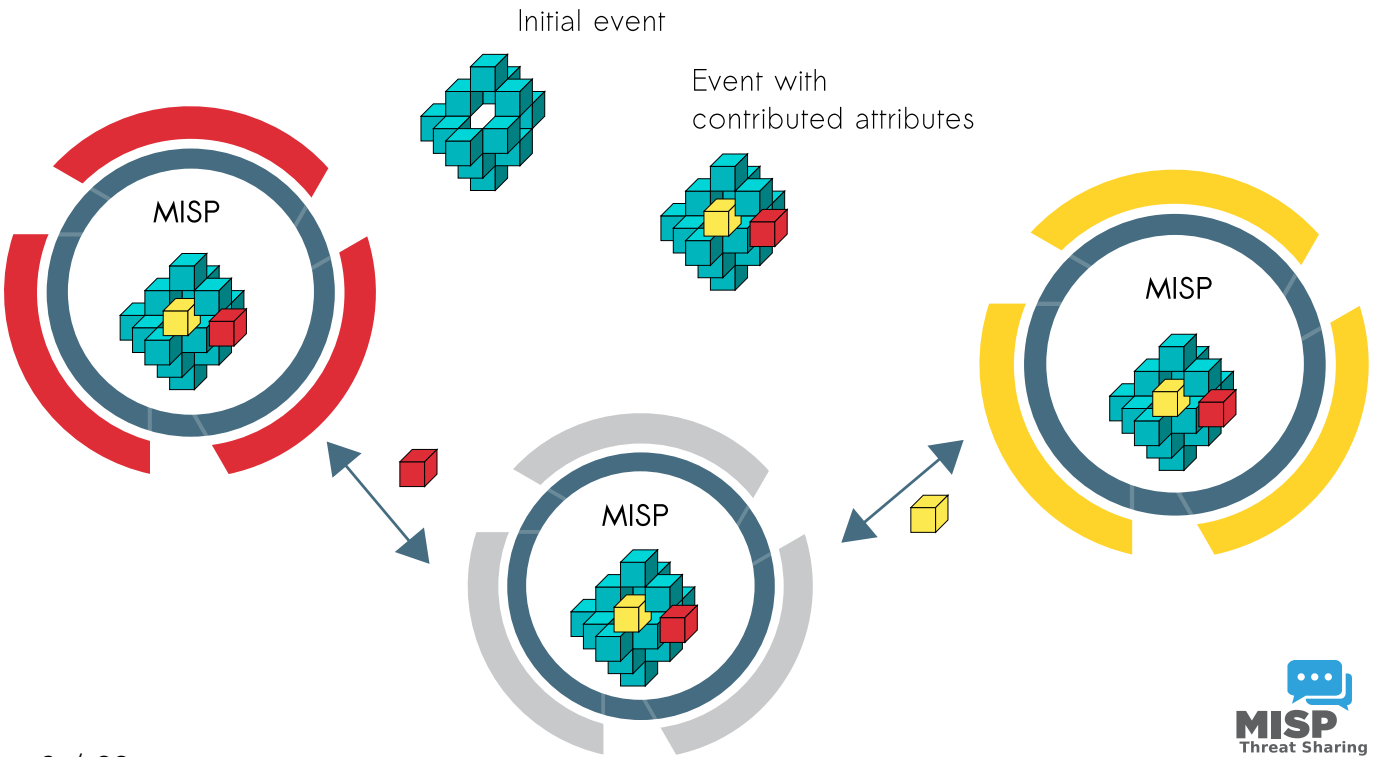
Quick MISP introduction

- MISP[2] is an IOC and threat indicators sharing free software.
- MISP has **many functionalities** e.g. flexible sharing groups, automatic correlation, free-text import helper, event distribution and collaboration.
- MISP project recently grown into multiple sub-projects to support information sharing practices.
- CIRCL operates multiple MISP instances with a significant user base (more than 600 organizations with more than 1300 users).
- After some years of trial-and-error, we explain the background behind current and new **MISP features**.

[2] https://github.com/MISP/MISP

MISP core distributed sharing functionality

- MISP's core functionality is sharing where everyone can be a consumer and/or a contributor/producer.
- Quick benefit without the obligation to contribute.
- Low barrier access to get acquainted to the system.



MISP feed system and external feed consolidation

- Easy way of building filtered subsets of the data repository for feed creation
- Allows out of bound sharing and simple hosting of MISP feeds
- MISP can easily ingest other MISP feeds directly or via cherry picking
- For existing non-MISP format feeds, MISP uses various parsing algorithms to convert feed data on the fly
- Preview and correlate feed data directly for evaluation

Events and Attributes in MISP

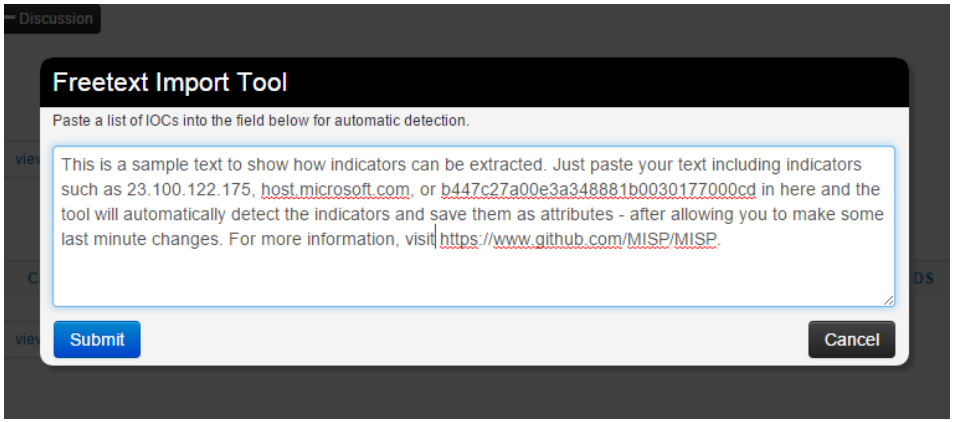
- MISP attributes[3] initially started with a standard set of "cyber security" indicators.
- MISP attributes are purely **based on usage** (what people and organizations use daily).
- Evolution of MISP attributes is based on practical usage and users (e.g. recent addition of the **financial indicators** in 2.4).
- In next release, MISP galaxy will be added to give the freedom to the **community to create new and combined attributes** and share them.

[3] attributes can be anything that helps describe the intent of the event package from indicators, vulnerabilities or any relevant information

Contributing data to MISP

- Offering a wide range of data creation possibilities
  - Various ways of contributing data via the MISP UI including a freetext parser and a dynamic templating system
  - Flexible APIs that ease automation
  - PyMISP Python library
  - Import tools and Python Import/Enrichment module system
  - Integration with external tools such as Viper, sandboxes such as Cuckoo, etc
- Contribution can be direct by creating an event but **users can propose attributes updates** to the event owner or simply indicate a sighting.
- **Users should not be forced to use a single interface to contribute**.

Example: Freetext import in MISP



Freetext Import 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.

Value	Category	Type	IDS	Comment	Actions
23.100.122.175	Network activity	ip-dst	☑	Imported via the freetext import.	✖
host.microsoft.com	Network activity	hostname	☑	Imported via the freetext import.	✖
b447c27a00e3a348881b0030177000cd	Payload delivery	md5	☑	Imported via the freetext import.	✖
https://www.github.com/MISP/MISP	Network activity	url	☑	Imported via the freetext import.	✖

Submit

ip-dst → ip-src Change all

Update all comment fields Change all

Filters: All | File | Network | Financial | Proposal | Correlation

Date	Org	Category	Type	Value	Comment	Related Events	IDS	Distribution	Actions
2016-02-24		Network activity	hostname	host.microsoft.com	Imported via the freetext import.		Yes	Inherit	
2016-02-24		Network activity	ip-dst	23.100.122.175	Imported via the freetext import.	298	Yes	Inherit	
2016-02-24		Network activity	url	https://www.github.com/MISP/MISP	Imported via the freetext import.		Yes	Inherit	
2016-02-24		Payload delivery	md5	b447c27a00e3a348881b0030177000cd	Imported via the freetext import.		Yes	Inherit	

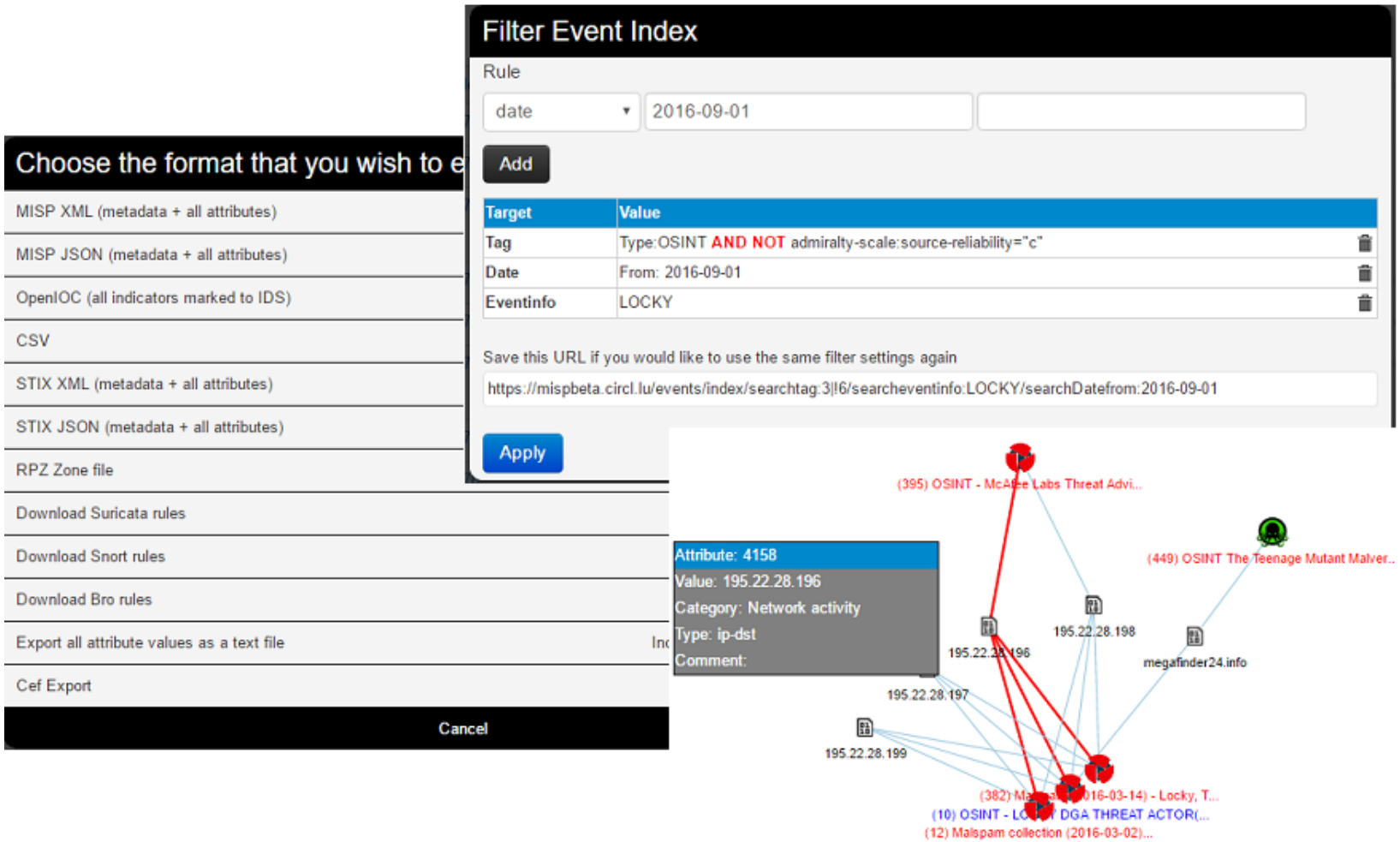
Supporting Sharing in MISP

- Delegate events publication to another organization.
  - The other organization can take over the ownership of an event and provide **pseudo-anonymity to initial organization**.
- Sharing groups allow custom sharing per event or even at attribute level.
  - Sharing communities can be used locally or even cross MISP instances.
  - **Sharing groups** can be done at the **event level or the attribute level** (e.g. financial indicators shared to a financial sharing group and cyber security indicators to CSIRT community).

Using the data in MISP

- Various ways for analysts of interacting with the data directly
  - Viewing,
  - Searching and filtering the data-set
  - Correlating data using correlation graphs
  - Downloading the viewed data in various formats
  - Use one of the many tools in the MISP eco-system (MISP Workbench, Viper, MISPego, etc)

Various ways of viewing the data in MISP



Connecting devices and tools to MISP

- One of the main goals of MISP is to feed protective tools with data
  - IDSes / IPSes (examples: Suricata, Bro, Snort)
  - SIEMs (examples: CEF, CSV)
  - Host scanners (examples: OpenIOC, STIX, CSV)
  - Various analysis tools (example: Maltego)
  - DNS policies (example: RPZ)
- Various ways of exporting this data (downloads of selected data, full exports, APIs)
- The idea was to leave the selection of the subset of data pushed to these to the user using APIs

Exporting data using the API

- Flexible, highly parametrised APIs
- Filter data by tags
- The dillema of time to live vs on-demand parametrisation
- Home in on the most sane data-set for each use-case
- Simple post a JSON containing parameters to the relevant API

Suricata in MISP

- Exported attribute types: ip-dst, ip-src, email-src, email-dst, email-subject, email-attachment, domain, hostname, url, user-agent, snort
- Rewriting of existing snort rules (sid, reference, etc)
- Try to be conscious about the number of rules (culling of duplicates, use optimisations)

Example Snort vs Suricata (hostname)

```
Snort
alert udp any any -> any 53 (msg: "MISP e121 Hostname: video.today-nytimes.com"; content:"|01
alert tcp any any -> any 53 (msg: "MISP e121 Hostname: video.today-nytimes.com"; content:"|01
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg: "MISP e121 Outgoing HTTP Hostname:

Suricata
alert dns any any -> any 53 (msg: "MISP e121 Hostname: video.today-nytimes.com"; dns_query; co
alert http $HOME_NET any -> $EXTERNAL_NET any (msg: "MISP e121 Outgoing HTTP Hostname: video.t
```

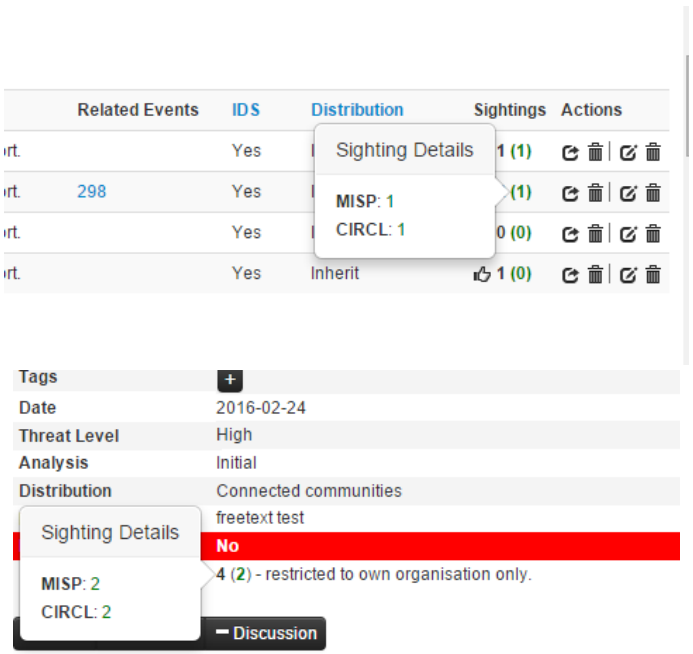
Exporting data using the API - Suricata examples

- API: https://mymisp/events/nids/suricata/download
- Attribute types used by suricata export
- filters:
  - {"type": ["domain", "hostname", "url"], "last": "30d"}
  - {"type": ["ip-src", "ip-dst"], "last": "7d"}
  - {"tags": ["admiralty-scale:information-credibility=1", "high-prio"]}
- Bad hashes for file matching extraction
  - https://mymisp/events/hids/md5/download
  - https://mymisp/events/hids/sha1/download
  - https://mymisp/events/hids/sha256/download

Result

```
#This part might still contain bugs, use and your own risk and report any issues.
#
# MISP export of IDS rules - optimized for suricata
#
# These NIDS rules contain some variables that need to exist in your configuration.
# Make sure you have set:
#
# $HOME_NET - Your internal network range
# $EXTERNAL_NET - The network considered as outside
# $SMTP_SERVERS - All your internal SMTP servers
# $HTTP_PORTS   - The ports used to contain HTTP traffic (not required with suricata export)
#
alert dns any any -> any 53 (msg: "MISP e6 Domain: retsback.com"; dns_query; content:"retsback.com"; nocase; pcre: "/(^|[^A-Za-z0-9-])retsback\.com$/i";  classtype:trojan-a
alert http $HOME_NET any -> $EXTERNAL_NET any (msg: "MISP e6 Outgoing HTTP Domain: retsback.com"; flow:to_server,established; content: "Host|3a|"; nocase; http_header; cont
alert dns any any -> any 53 (msg: "MISP e6 Domain: updconfs.com"; dns_query; content:"updconfs.com"; nocase; pcre: "/(^|[^A-Za-z0-9-])updconfs\.com$/i";  classtype:trojan-a
alert http $HOME_NET any -> $EXTERNAL_NET any (msg: "MISP e6 Outgoing HTTP Domain: updconfs.com"; flow:to_server,established; content: "Host|3a|"; nocase; http_header; cont
alert dns any any -> any 53 (msg: "MISP e6 Domain: systruster.com"; dns_query; content:"systruster.com"; nocase; pcre: "/(^|[^A-Za-z0-9-])systruster\.com$/i";  classtype:tr
alert http $HOME_NET any -> $EXTERNAL_NET any (msg: "MISP e6 Outgoing HTTP Domain: systruster.com"; flow:to_server,established; content: "Host|3a|"; nocase; http_header; co
alert dns any any -> any 53 (msg: "MISP e6 Domain: msupdcheck.com"; dns_query; content:"msupdcheck.com"; nocase; pcre: "/(^|[^A-Za-z0-9-])msupdcheck\.com$/i";  classtype:tr
alert http $HOME_NET any -> $EXTERNAL_NET any (msg: "MISP e6 Outgoing HTTP Domain: msupdcheck.com"; flow:to_server,established; content: "Host|3a|"; nocase; http_header; co
alert ip $HOME_NET any -> 91.230.211.206 any (msg: "MISP e6 Outgoing To IP: 91.230.211.206";   classtype:trojan-activity; sid:4000221; rev:1; priority:3; reference:url,http
alert ip $HOME_NET any -> 185.86.77.153 any (msg: "MISP e6 Outgoing To IP: 185.86.77.153";   classtype:trojan-activity; sid:4000231; rev:1; priority:3; reference:url,https:
alert ip $HOME_NET any -> 91.215.154.90 any (msg: "MISP e6 Outgoing To IP: 91.215.154.90";   classtype:trojan-activity; sid:4000241; rev:1; priority:3; reference:url,https:
alert ip $HOME_NET any -> 88.214.236.121 any (msg: "MISP e6 Outgoing To IP: 88.214.236.121";   classtype:trojan-activity; sid:4000251; rev:1; priority:3; reference:url,http
```

Providing feedback on any hits - Sightings support



- Sightings allow users to notify the community about the activities related to an indicator.
- Refresh time-to-live of an indicator.
- Sightings can be performed via API, and UI including import of STIX sighting documents.
- Many research opportunities in scoring indicators based on users sighting.

Providing Sightings via the API

- Simply provide a sighting by POSTing to a url
  - https://mymisp/sightings/add/[attribute_id]
  - https://mymisp/sightings/add/[attribute_uuid]
- Alternatively POST the sighted values or attribute ID in a JSON object
  - {"value": "8.8.8.8"}
  - {"id": 1337}

Same thing using STIX 1.x (warning, this can be a bit verbose)

```
<stix:STIX_Package
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xmlns:stix="http://stix.mitre.org/stix-1"
    xmlns:indicator="http://stix.mitre.org/Indicator-2"
    xmlns:stixCommon="http://stix.mitre.org/common-1"
    xmlns:cybox="http://cybox.mitre.org/cybox-2"
    xmlns:AddressObject="http://cybox.mitre.org/objects#AddressObject-2"
    xmlns:DomainNameObj="http://cybox.mitre.org/objects#DomainNameObject-1"
    xmlns:cyboxVocabs="http://cybox.mitre.org/default_vocabularies-2"
    xmlns:stixVocabs="http://stix.mitre.org/default_vocabularies-1"
    xmlns:example="http://example.com/"
    xsi:schemaLocation="
    http://stix.mitre.org/stix-1 ../stix_core.xsd
    http://stix.mitre.org/Indicator-2 ../indicator.xsd
    http://cybox.mitre.org/objects#DomainNameObject-1 http://cybox.mitre.org/XMLSchema/objects/Domain_Name/1.0/Domain_Name_Object.xsd
    http://stix.mitre.org/common-1 http://stix.mitre.org/XMLSchema/common/1.1.1/stix_common.xsd
    http://cybox.mitre.org/default_vocabularies-2 ../cybox/cybox_default_vocabularies.xsd
    http://stix.mitre.org/default_vocabularies-1 ../stix_default_vocabularies.xsd
    http://cybox.mitre.org/objects#AddressObject-2 ../cybox/objects/Address_Object.xsd"
    id="example:STIXPackage-33fe3b22-0201-47cf-85d0-97c02164528d"
    timestamp="2014-05-08T09:00:00.000000Z"
    version="1.1.1"
    >
    <stix:STIX_Header>
        <stix:Title>Example watchlist that contains IP information.</stix:Title>
        <stix:Package_Intent xsi:type="stixVocabs:PackageIntentVocab-1.0">Indicators - Watchlist</stix:Package_Intent>
    </stix:STIX_Header>
    <stix:Indicators>
        <stix:Indicator xsi:type="indicator:IndicatorType" id="example:Indicator-2e20c5b2-56fa-46cd-9662-8f199c69d2c9" timestamp="2014-05-08T09:00:00.000000Z">
          <indicator:Type xsi:type="stixVocabs:IndicatorTypeVocab-1.1">Domain Watchlist</indicator:Type>
          <indicator:Observable id="example:Observable-87c9a5bb-d005-4b3e-8081-99f720fad62b">
              <cybox:Object id="example:Object-12c760ba-cd2c-4f5d-a37d-18212eac7928">
                  <cybox:Properties xsi:type="DomainNameObj:DomainNameObjectType" type="FQDN">
                      <DomainNameObj:Value condition="Equals" apply_condition="ANY">malicious1.example.com##comma##malicious2.example.com##comma##malicious3.example.com</DomainNameObj:Value>
                  </cybox:Properties>
              </cybox:Object>
          </indicator:Observable>
          <indicator:Sightings>
            <indicator:Sighting timestamp="2014-05-08T09:00:00.000000Z">
              <indicator:Source>
                <stixCommon:Identity>
                  <stixCommon:Name>FooBar Inc.</stixCommon:Name>
                </stixCommon:Identity>
              </indicator:Source>
              <indicator:Related_Observables>
                <indicator:Related_Observable>
                  <stixCommon:Observable id="example:Observable-45b3acdf-1888-4bcc-89a9-6d9f8116fede">
                    <cybox:Object id="example:Object-a3d36250-42fa-4653-9172-87b87598390c">
                      <cybox:Properties xsi:type="DomainNameObj:DomainNameObjectType" type="FQDN">
                        <DomainNameObj:Value>malicious2.example.com</DomainNameObj:Value>
                      </cybox:Properties>
                    </cybox:Object>
                  </stixCommon:Observable>
                </indicator:Related_Observable>
              </indicator:Related_Observables>
            </indicator:Sighting>
          </indicator:Sightings>
        </stix:Indicator>
    </stix:Indicators>
</stix:STIX_Package>
```

tl;dr

- MISP allows you to
  - consolidate your threat-intel from various sources
  - Create and collaborate on your own information
  - Enrich your community's combined data set
  - Share your data granularly with your community or a subset thereof
- Using this data it allows you to
  - Support your analysts in their research
  - Find trends and commonalities between threats
  - Build protection in real time
  - Use a range of filtered subsets of your dataset for your various protective measures
  - Provide feedback on detections to your community

Q&A

- info@circl.lu (if you want to join the CIRCL MISP sharing community)
- OpenPGP fingerprint: 3B12 DCC2 82FA 2931 2F5B 709A 09E2 CD49 44E6 CBCD
- `https://github.com/MISP/` - `http://www.misp-project.org/`
- We welcome any contributions to the project, be it pull requests, ideas, github issues,...
- Join us in Zurich the 6th December for a training and/or the 7th December MISP Hackathon
- For other training opportunities feel free to get in touch with us