# Building instantly exploitable protection for yourself and your partners against targeted cyber threats using MISP

***by Andras Iklody***

# What is MISP?

MISP is:

- a repository of malware, IOCs and cyber threat related technical information
- a sharing platform that enables partners to instantly share the above mentioned data
- A collaboration system,
- that converts your and your partners' information into protection for its entire user community
- that helps you identify links between your incidents and the collective threat intelligence of all your interconnected partners

# History of MISP

- Originally developed by Christophe Vandeplas in his free time
- Adopted by the Belgian Defense and later on by NATO
- NATO started investing into the development of MISP since summer 2012
- Since then it has gone open source
- CIRCL started developing tools and APIs around MISP
- with a rapidly growing user community, improvements and new features are being added by various 3rd parties, such as FIRST

# So what issues does MISP try to tackle?

# The situation without MISP

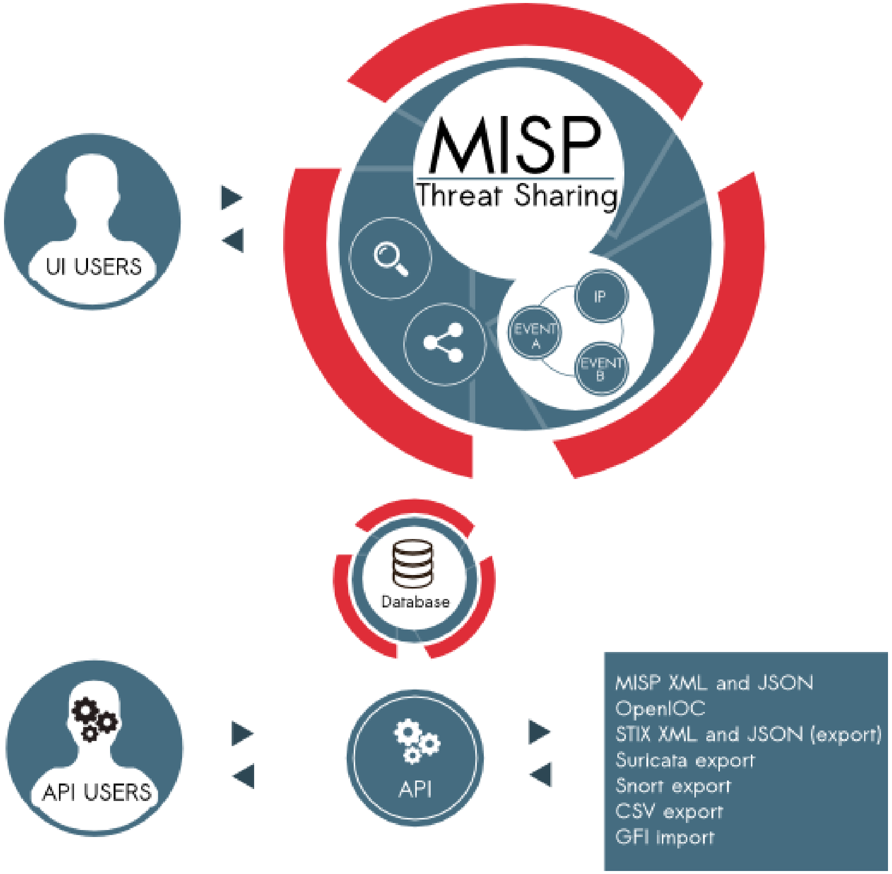
- There has always been some level of information sharing
- But most of the time it happened ad hoc:
  - Phone call
  - e-mail with a CSV with malicious IP addresses
  - Or for people we don't like: PDFs with indicators in the text

# The situation without MISP

- Data doesn't reach target audience
- recipients end up with something they can't really use
- or even worse, something that they already have – meaning they could have maybe prevented an incident, had they shared the information
- a lot of duplication of effort
- Information sharing in this old fashioned way happens at the expense of interrupting your analyst's workflow
- You end up with a lot of information that you cannot really exploit which, again, leads to attacks being successful that could have been prevented

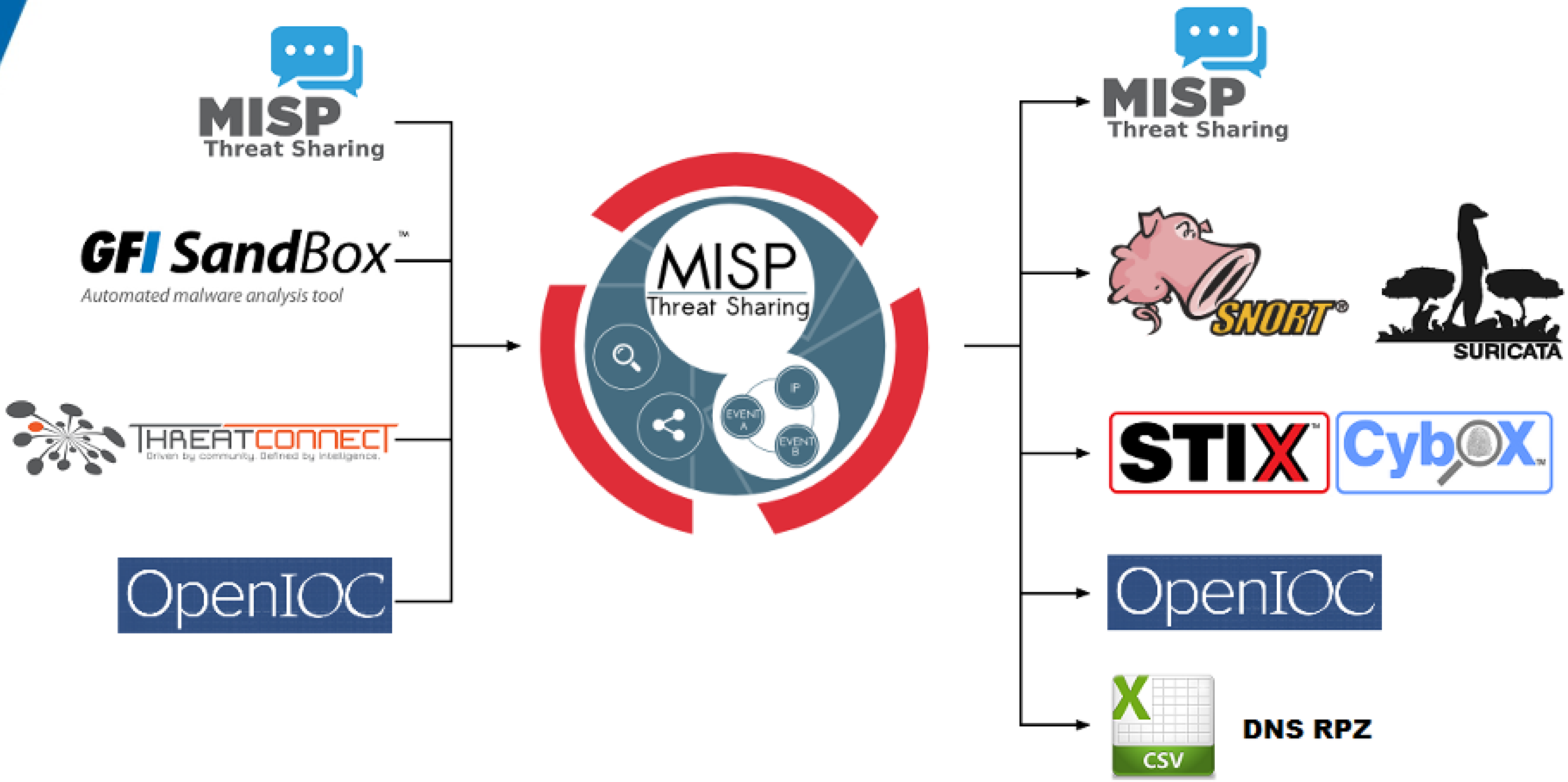
# How does MISP work?

- Various ways to interact with the data in MISP:
  - Web interface
  - API
  - Indirectly through systems ingesting MISP's exports / producing data for MISP
- will provide the same benefits either way



# Inter-connectivity

supporting a wide range of connectivity options

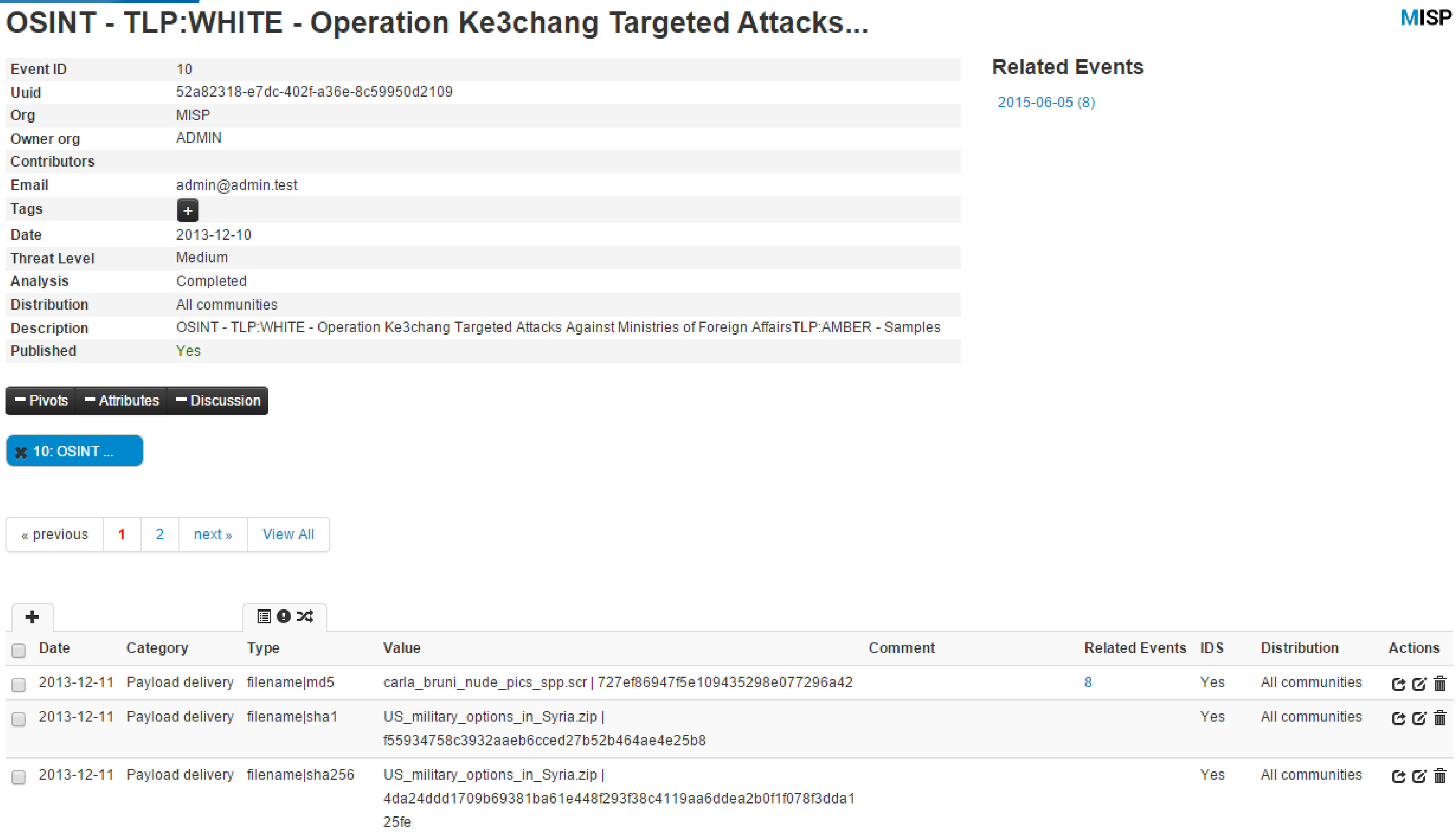


# *The data structure at a glance*

- Simplistic data structure that can easily be converted to other formats
- Designed not to overwhelm users
- The main design concept: Capture what is actually important
- Community driven evolution

# *The data structure at a glance*

- Each package of information is called an “Event”
- Events are made up of “Attributes”
- Attributes can describe several things (IOCs, Context, CVEs external resources, malware samples)
  - Attributes have a category and a type
  - They can be marked to be included in the IDS exports
  - They can have contextual comments



# OSINT - TLP:WHITE - Operation Ke3chang Targeted Attacks...

| | |
|---|---|
| Event ID | 10 |
| Uuid | 52a82318-e7dc-402f-a36e-8c59950d2109 |
| Org | MISP |
| Owner org | ADMIN |
| Contributors | |
| Email | admin@admin.test |
| Tags | + |
| Date | 2013-12-10 |
| Threat Level | Medium |
| Analysis | Completed |
| Distribution | All communities |
| Description | OSINT - TLP:WHITE - Operation Ke3chang Targeted Attacks Against Ministries of Foreign AffairsTLP:AMBER - Samples |
| Published | Yes |

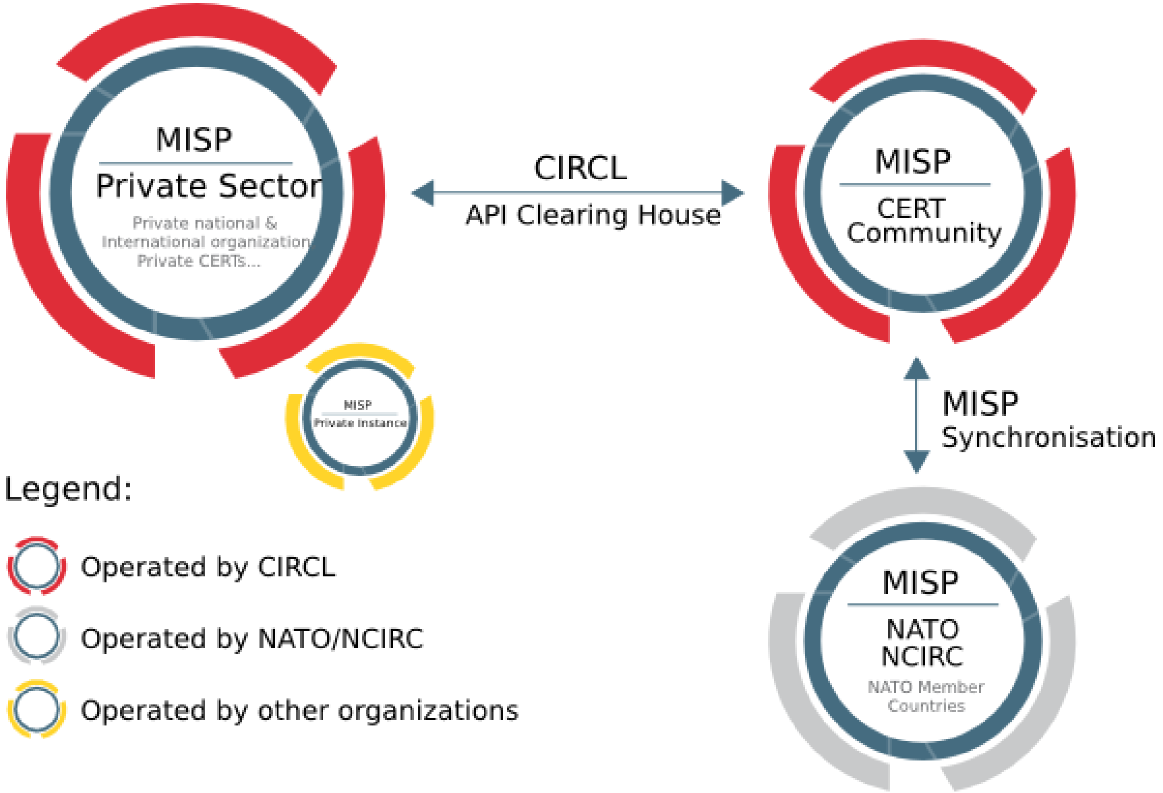
## Related Events

2015-06-05 (8)

| □ | Date | Category | Type | Value | Comment | Related Events | IDS | Distribution | Actions |
|---|---|---|---|---|---|---|---|---|---|
| □ | 2013-12-11 | Payload delivery | filename\|md5 | carla_bruni_nude_pics_spp.scr \| 727ef86947f5e109435298e077296a42 | | 8 | Yes | All communities | |
| □ | 2013-12-11 | Payload delivery | filename\|sha1 | US_military_options_in_Syria.zip \| f55934758c3932aaeb6cced27b52b464ae4e25b8 | | | Yes | All communities | |
| □ | 2013-12-11 | Payload delivery | filename\|sha256 | US_military_options_in_Syria.zip \| 4da24ddd1709b69381ba61e448f293f38c4119aa6ddea2b0f1f078f3dda125fe | | | Yes | All communities | |

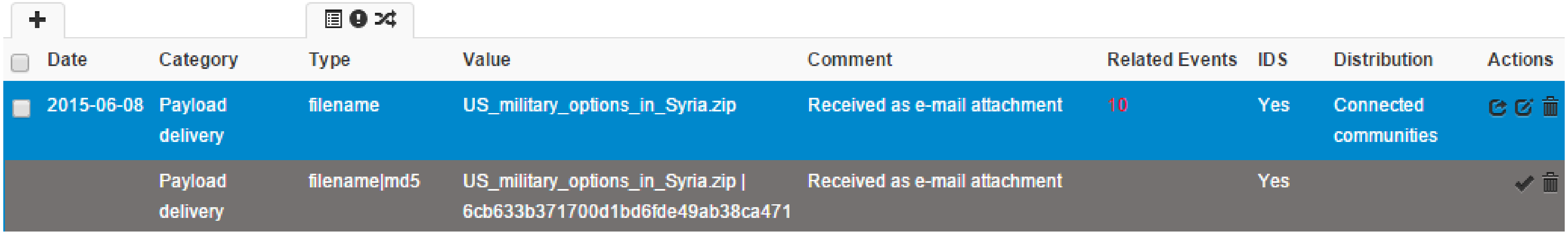
# Sharing and collaboration

- Share your data with other users of the same instance
- Share your data with users of interconnected instances
  - Distribution settings
  - Sharing groups in upcoming version
- MISP topology example (CIRCL)



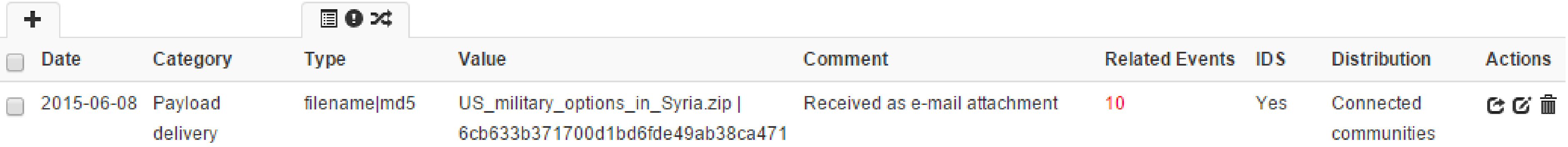
# Sharing and collaboration

- Collaborate using Proposals
  - Create a proposal to an event that you do not own
  - The creating organization will get notified
  - They can accept / discard your proposal



+

| □ | Date | Category | Type | Value | Comment | Related Events | IDS | Distribution | Actions |
|---|---|---|---|---|---|---|---|---|---|
| □ | 2015-06-08 | Payload delivery | filename | US_military_options_in_Syria.zip | Received as e-mail attachment | 10 | Yes | Connected communities | |
| | | Payload delivery | filename\|md5 | US_military_options_in_Syria.zip \| 6cb633b371700d1bd6fde49ab38ca471 | Received as e-mail attachment | | Yes | | ✓ |

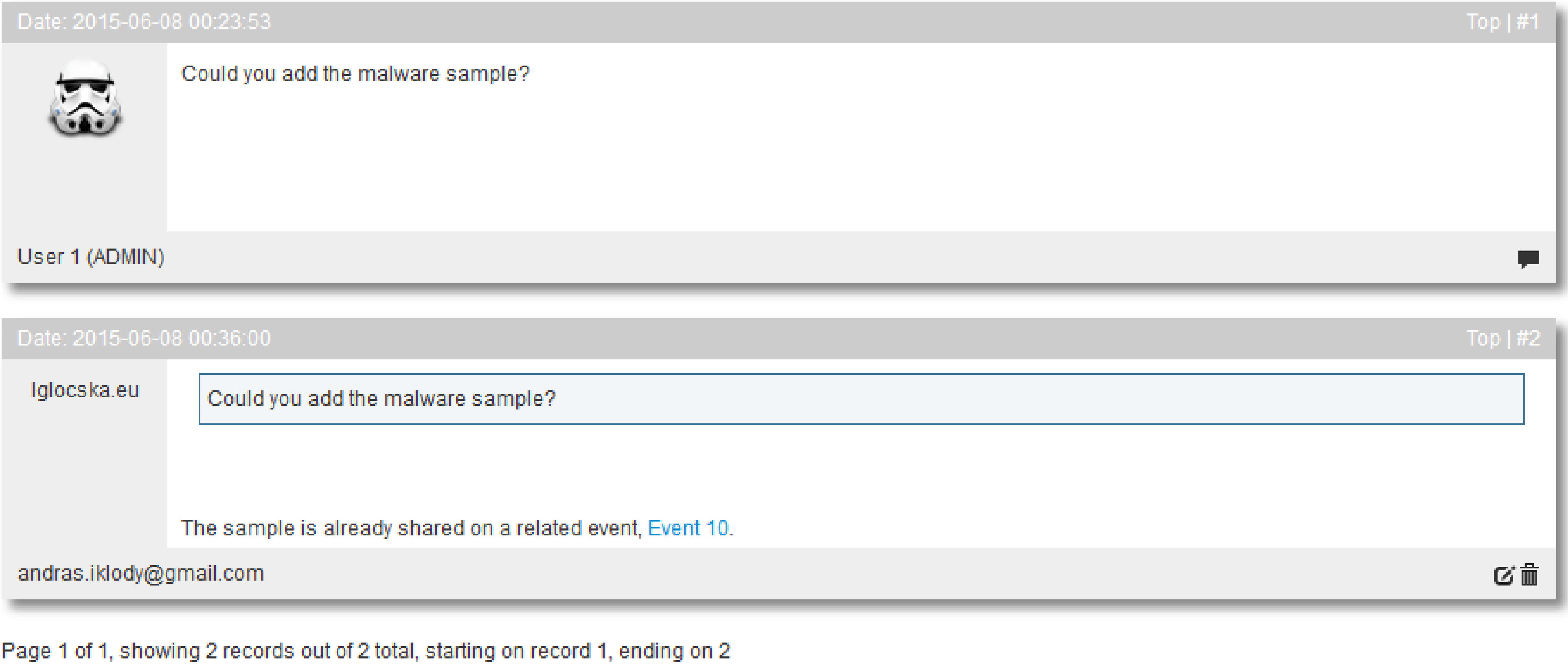


+

| □ | Date | Category | Type | Value | Comment | Related Events | IDS | Distribution | Actions |
|---|---|---|---|---|---|---|---|---|---|
| □ | 2015-06-08 | Payload delivery | filename\|md5 | US_military_options_in_Syria.zip \| 6cb633b371700d1bd6fde49ab38ca471 | Received as e-mail attachment | 10 | Yes | Connected communities | |

# Sharing and collaboration

- Discuss ongoing events using the forums
  - Add comments to events (keeping the releasability)
  - Create threads not related to specific events



Date: 2015-06-08 00:23:53 | Top | #1

Could you add the malware sample?

User 1 (ADMIN)

Date: 2015-06-08 00:36:00 | Top | #2

Iglocska.eu

> Could you add the malware sample?

The sample is already shared on a related event, Event 10.

andras.iklody@gmail.com

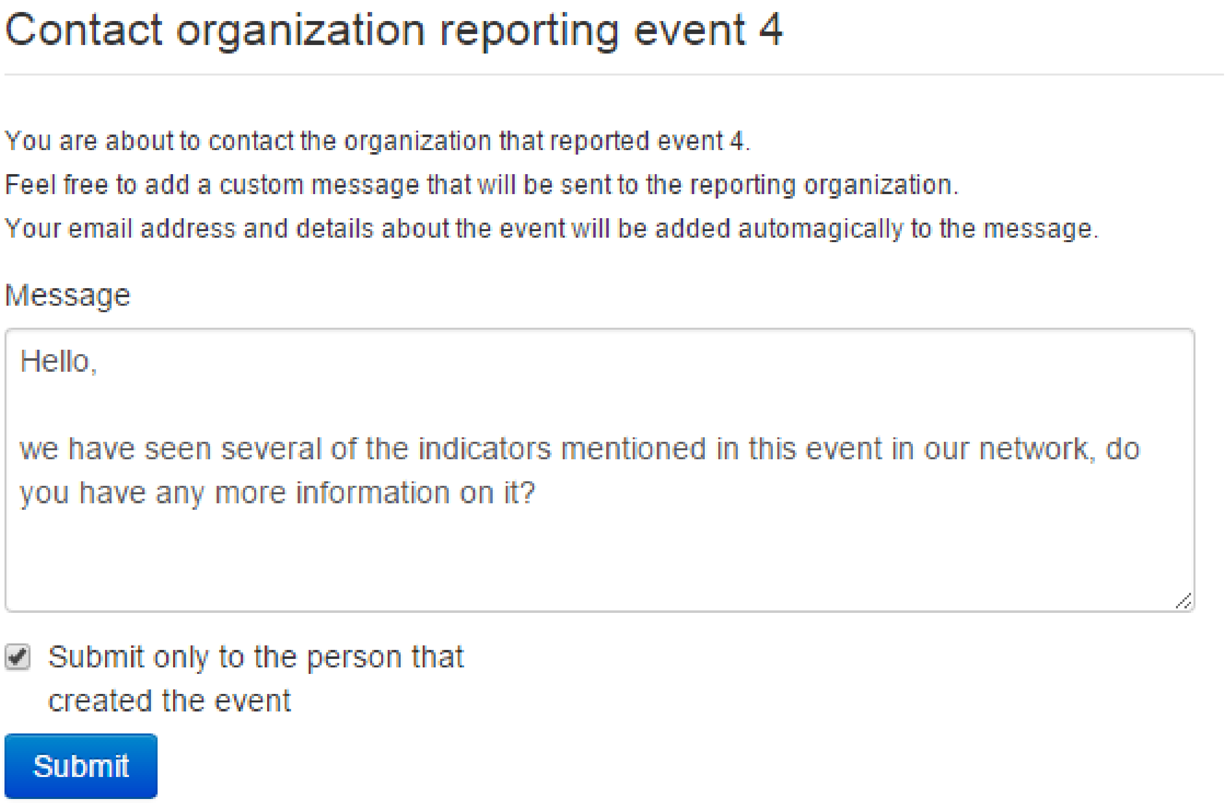
Page 1 of 1, showing 2 records out of 2 total, starting on record 1, ending on 2

# Sharing and collaboration

- Receive alerts of other users publishing events
  - Encrypted e-mails each time an event is published
  - Or when event is pushed to your instance / pulled by your instance
  - The e-mail alerts are an opt-in feature

# Sharing and collaboration

- Contact reporter of an event
  - Choose to only contact the person that has created the event or his entire organisation
  - All e-mailing can be enforced to be encrypted



## Contact organization reporting event 4

You are about to contact the organization that reported event 4.
Feel free to add a custom message that will be sent to the reporting organization.
Your email address and details about the event will be added automagically to the message.

Message

Hello,

we have seen several of the indicators mentioned in this event in our network, do you have any more information on it?

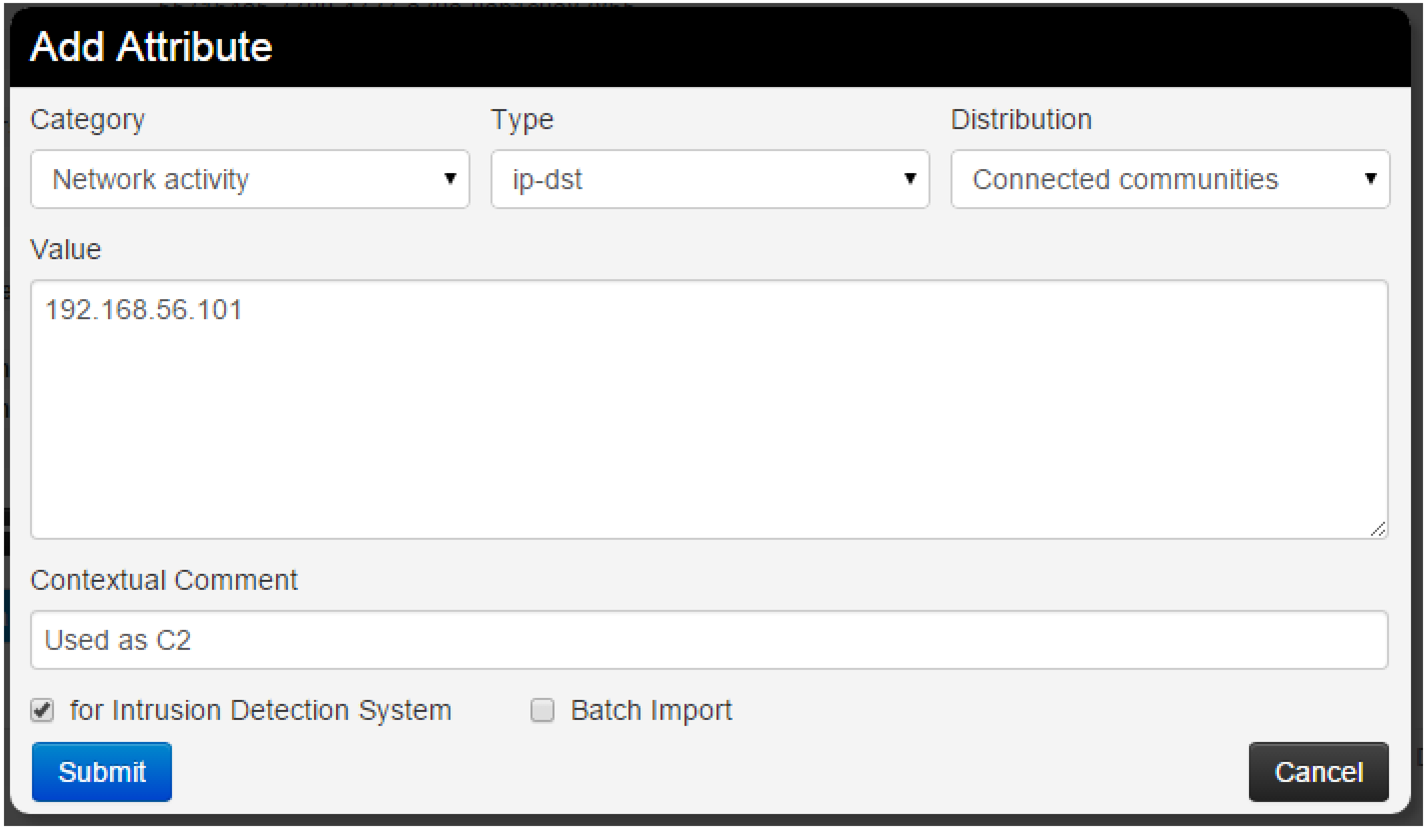
☑ Submit only to the person that created the event

# *Feeding MISP with data*

- Overview
- Manual input
  - Enter data via the interface
  - Use the free-text import tool
  - Use a template
- Feed MISP via the APIs / upload tools
  - Import from sandbox (GFI)
  - Use the REST API
  - Upload MISP XML / OpenIOC / Threatconnect export

# Entering data via the interface

- Simple interface to create attributes



Add Attribute

Category: Network activity

Type: ip-dst

Distribution: Connected communities

Value: 192.168.56.101

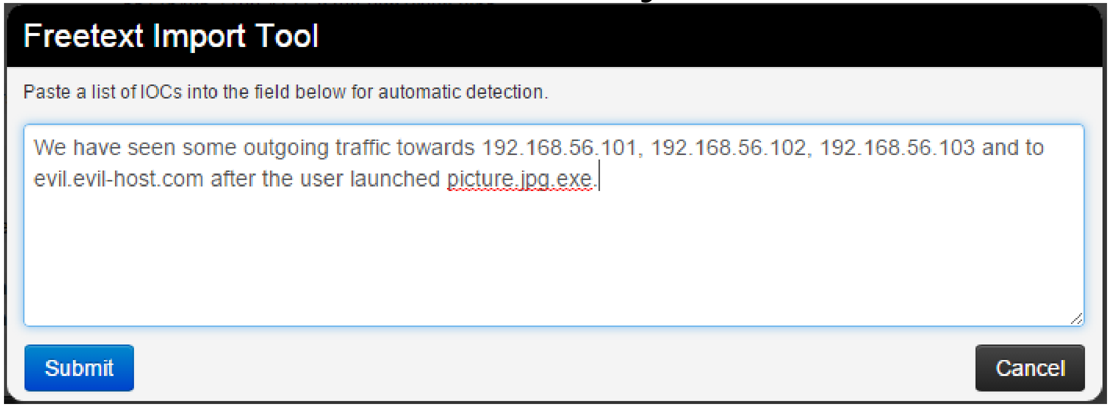
Contextual Comment: Used as C2

☑ for Intrusion Detection System

□ Batch Import

# Using the freetext import

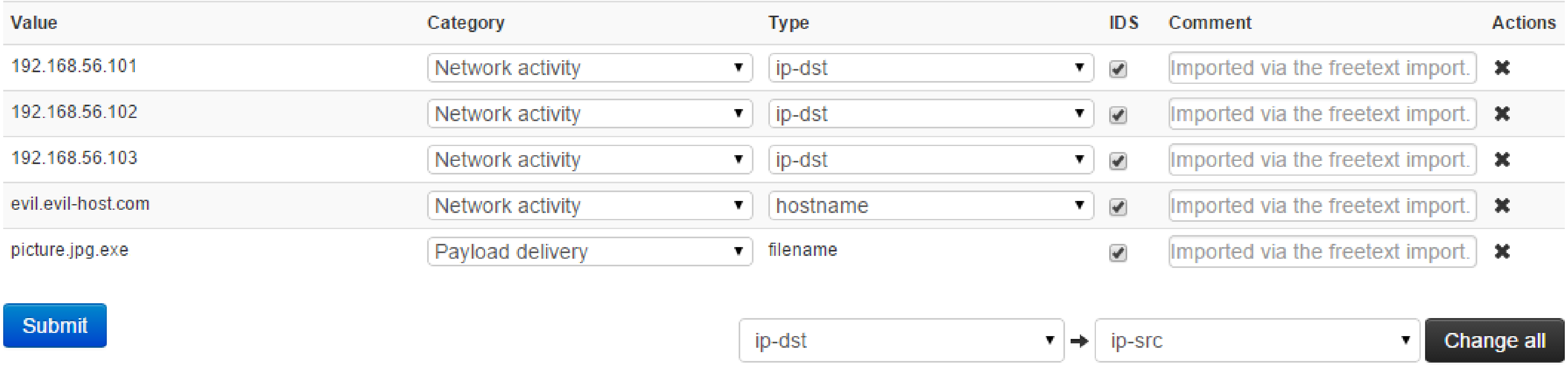
Simply paste text from any document and let MISP find the indicators for you.



**Freetext Import Tool**

Paste a list of IOCs into the field below for automatic detection.

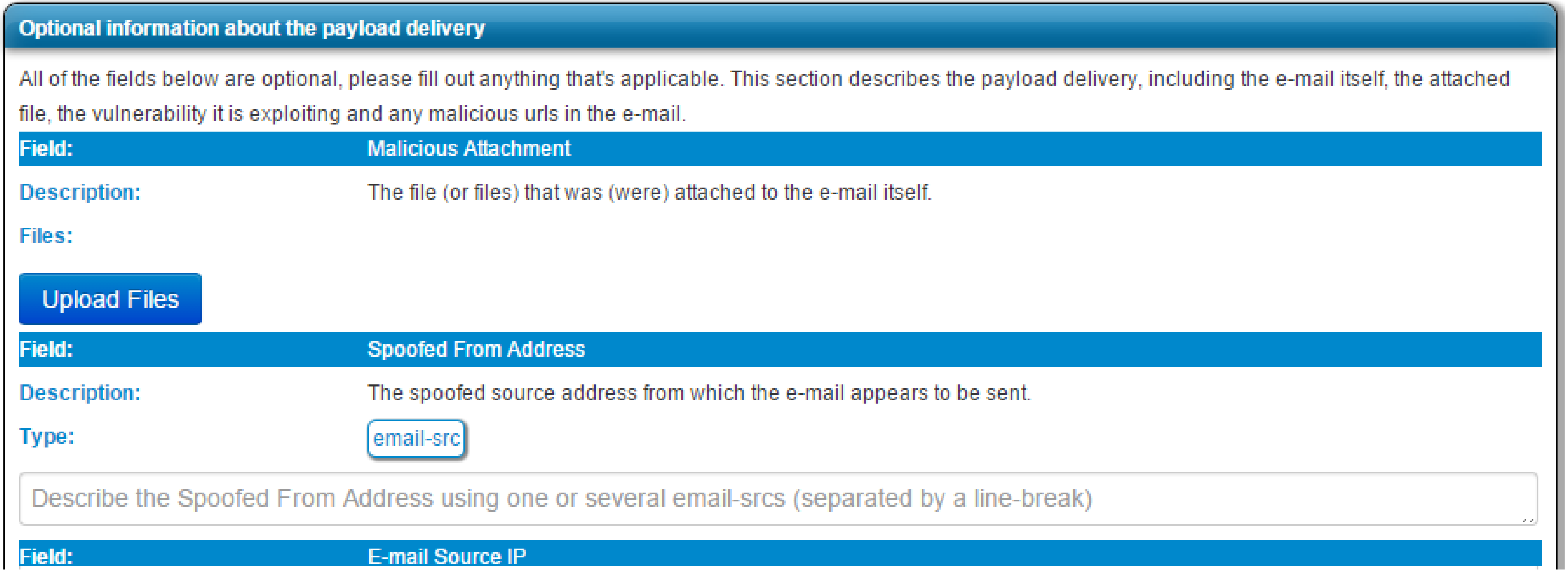
We have seen some outgoing traffic towards 192.168.56.101, 192.168.56.102, 192.168.56.103 and to evil.evil-host.com after the user launched picture.jpg.exe.



| Value | Category | Type | IDS | Comment | Actions |
|---|---|---|---|---|---|
| 192.168.56.101 | Network activity | ip-dst | ☑ | Imported via the freetext import. | ✖ |
| 192.168.56.102 | Network activity | ip-dst | ☑ | Imported via the freetext import. | ✖ |
| 192.168.56.103 | Network activity | ip-dst | ☑ | Imported via the freetext import. | ✖ |
| evil.evil-host.com | Network activity | hostname | ☑ | Imported via the freetext import. | ✖ |
| picture.jpg.exe | Payload delivery | filename | ☑ | Imported via the freetext import. | ✖ |

# Using templates

- Create templates to make life easier for your users
- Less experienced users will get a simple form to fill out that caters to your expectations



**Optional information about the payload delivery**

All of the fields below are optional, please fill out anything that's applicable. This section describes the payload delivery, including the e-mail itself, the attached file, the vulnerability it is exploiting and any malicious urls in the e-mail.

| | |
|---|---|
| **Field:** | Malicious Attachment |
| **Description:** | The file (or files) that was (were) attached to the e-mail itself. |
| **Files:** | |

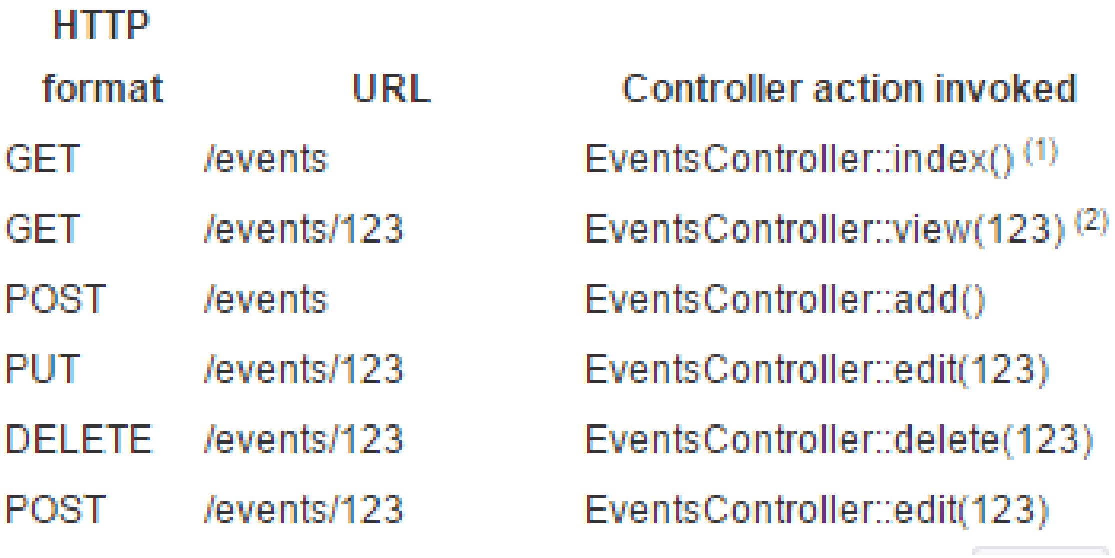
| | |
|---|---|
| **Field:** | Spoofed From Address |
| **Description:** | The spoofed source address from which the e-mail appears to be sent. |
| **Type:** | email-src |

Describe the Spoofed From Address using one or several email-srcs (separated by a line-break)

| | |
|---|---|
| **Field:** | E-mail Source IP |

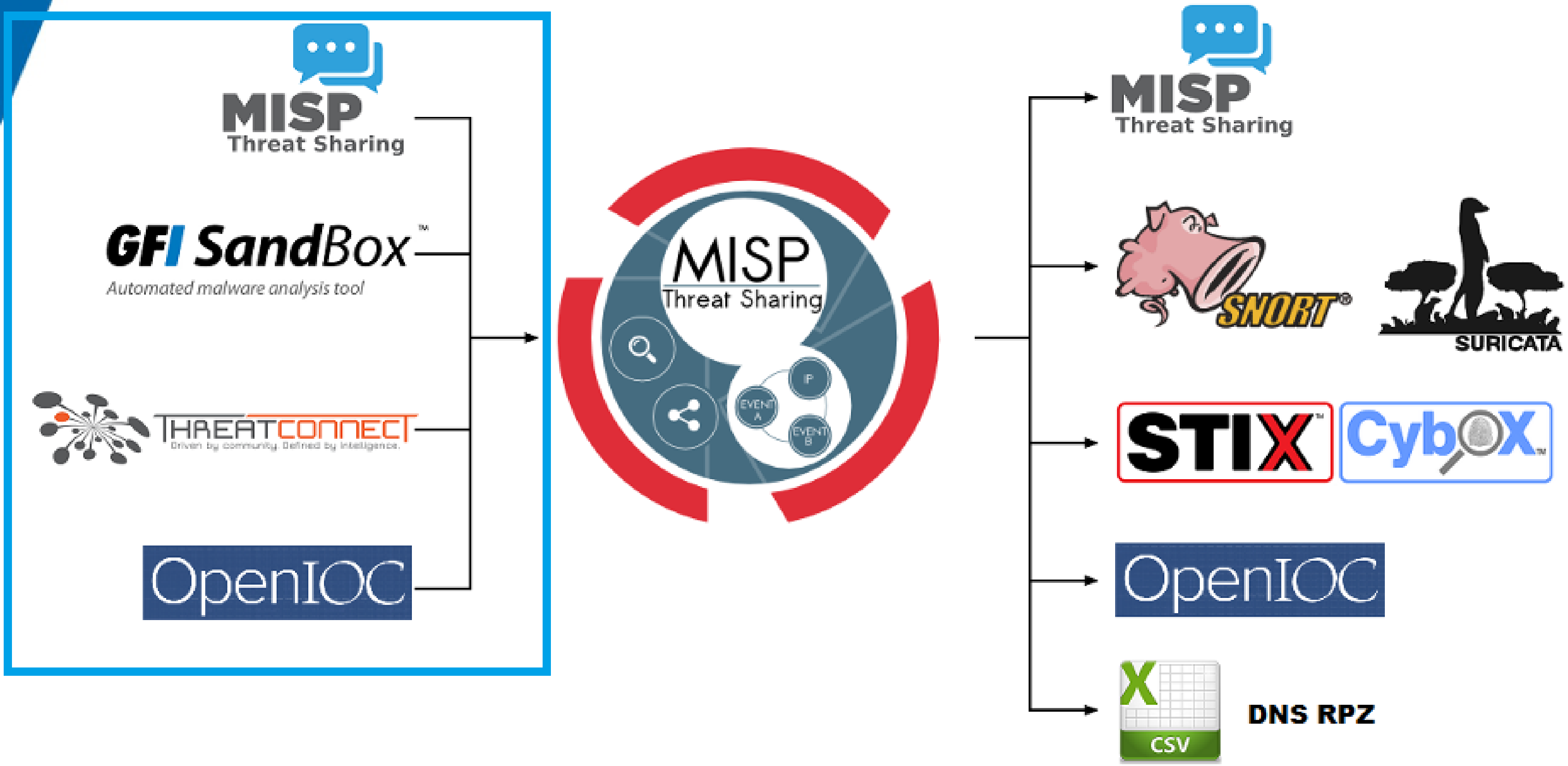
# *Using the REST API*

- MISP has a REST interface that allows you to interact with events and attributes
- Build scripts that modify data to MISP in a simple XML/JSON format using the REST API
- MISP will take care of the rest (access control, synchronisation, notifications, correlation, etc)



| HTTP format | URL | Controller action invoked |
|---|---|---|
| GET | /events | EventsController::index() (1) |
| GET | /events/123 | EventsController::view(123) (2) |
| POST | /events | EventsController::add() |
| PUT | /events/123 | EventsController::edit(123) |
| DELETE | /events/123 | EventsController::delete(123) |
| POST | /events/123 | EventsController::edit(123) |

# Importing data into MISP

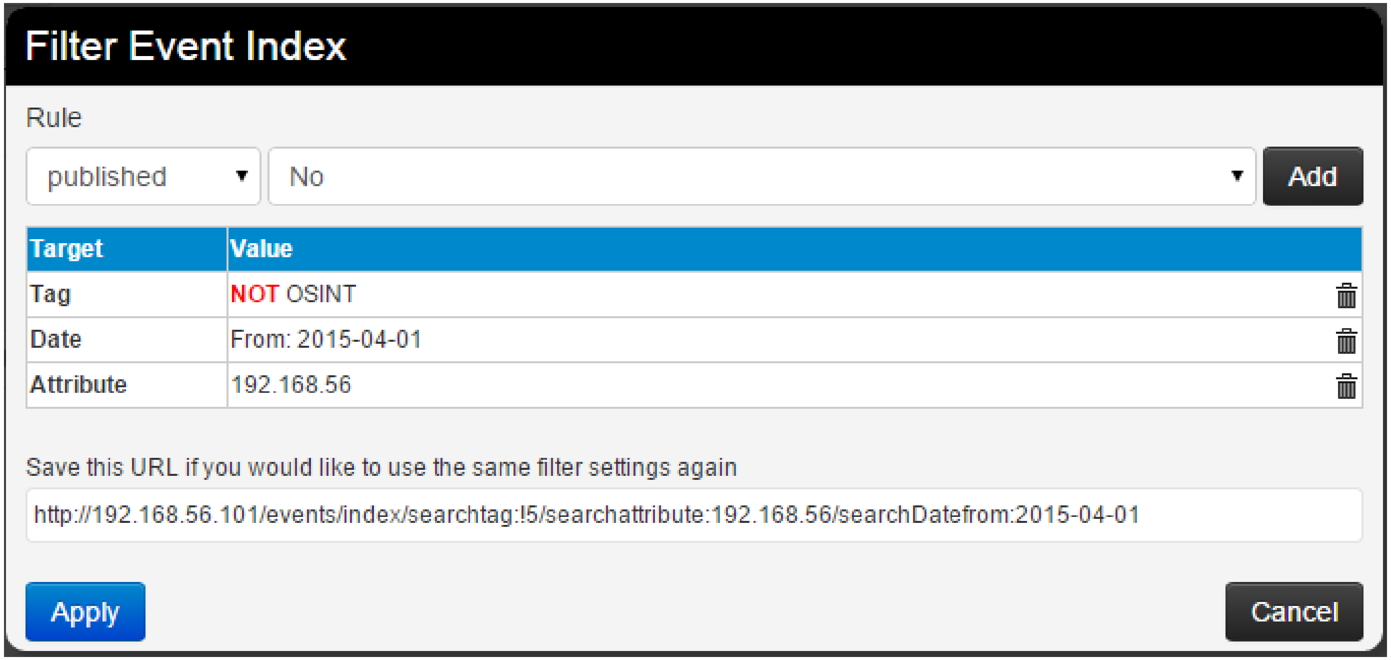


# *Exploiting the data in MISP and supporting the analysis*

- Overview
- Finding data in MISP
- Correlation and pivoting
- Giving data context by tagging
- Visualisation and building tools that leverage MISP data

# Finding data in MISP

Various tools for finding data in MISP



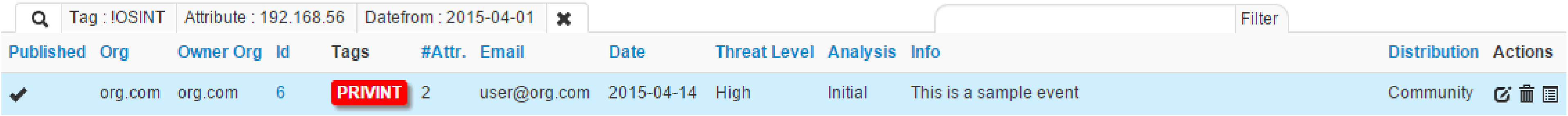
Rule

published ▾ No ▾

| Target | Value |
|---|---|
| Tag | NOT OSINT |
| Date | From: 2015-04-01 |
| Attribute | 192.168.56 |

Save this URL if you would like to use the same filter settings again

```
http://192.168.56.101/events/index/searchtag:!5/searchattribute:192.168.56/searchDatefrom:2015-04-01
```



Tag : !OSINT | Attribute : 192.168.56 | Datefrom : 2015-04-01 ✖

| Published | Org | Owner Org | Id | Tags | #Attr. | Email | Date | Threat Level | Analysis | Info | Distribution | Actions |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ✓ | org.com | org.com | 6 | PRIVINT | 2 | user@org.com | 2015-04-14 | High | Initial | This is a sample event | Community | |

# Correlation and pivoting

- Detecting similarities between events can be crucial
  - Helps analysts find similarities between attacks
  - Discover an ongoing campaign
  - Same threat actors behind a series of attacks
  - See trends in ongoing attacks
- Correlation happens each time you enter data into MISP

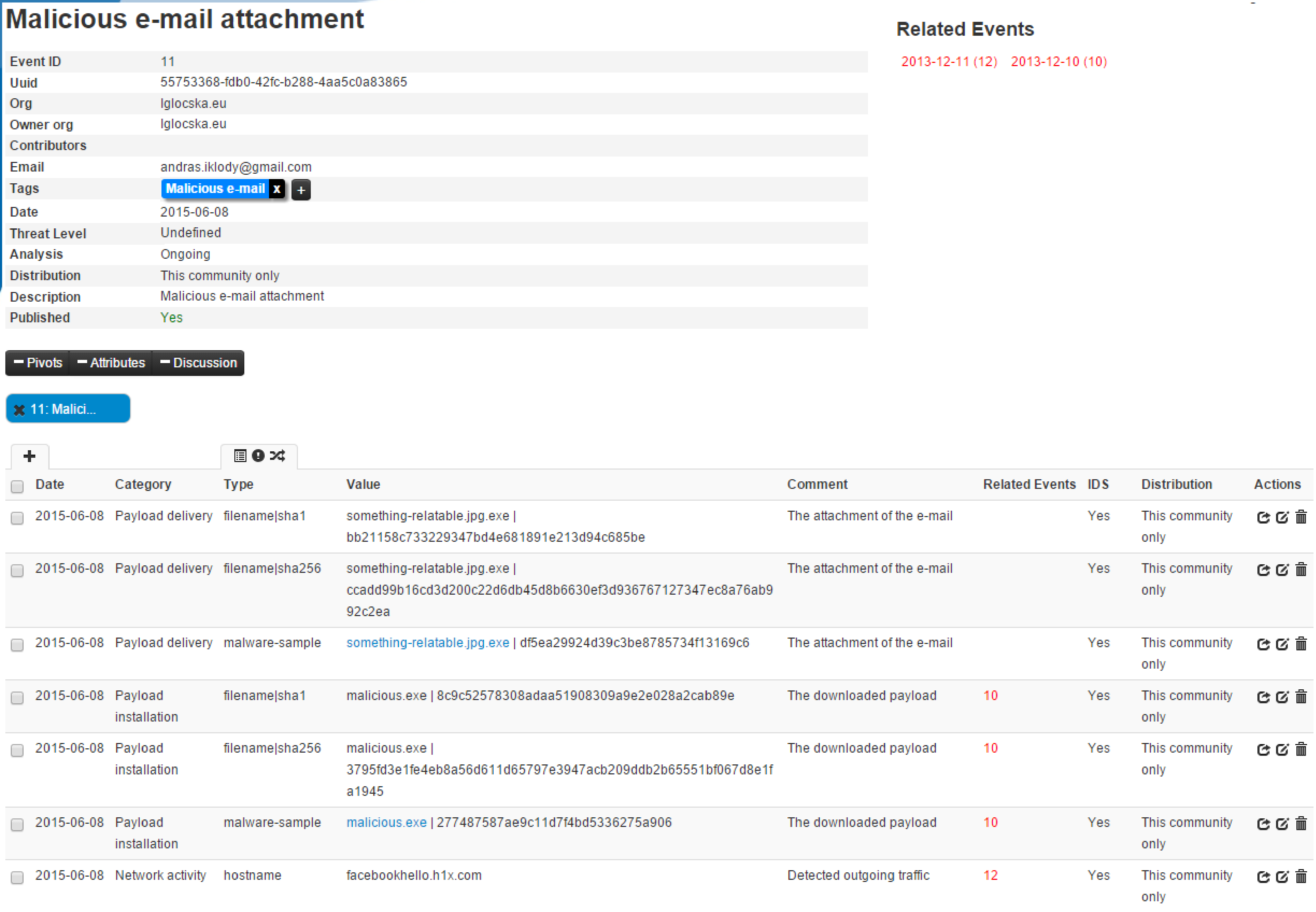
# *Correlating data example*

- Let's assume the following situation:
  - You are user of a MISP populated with data by yourself and your partners
  - You receive an e-mail that has an executable as attachment
  - The attachment has a name that is obviously meant to fool someone in your organization
  - You run it through your sandbox and put the resulting indicators into MISP

# Correlating data example

- We create an event and add our indicators as attributes:
  - The attachment itself (something-relatable.jpg.exe)
  - An executable downloaded and run by the attachment (malicious.exe)
  - Network activity to facebookhello.h1x.com
- MISP will automatically get the MD5/Sha1/Sha256 hashes of any uploaded sample
- So we end up with a total of 7 attributes

# Correlating data example



## Malicious e-mail attachment

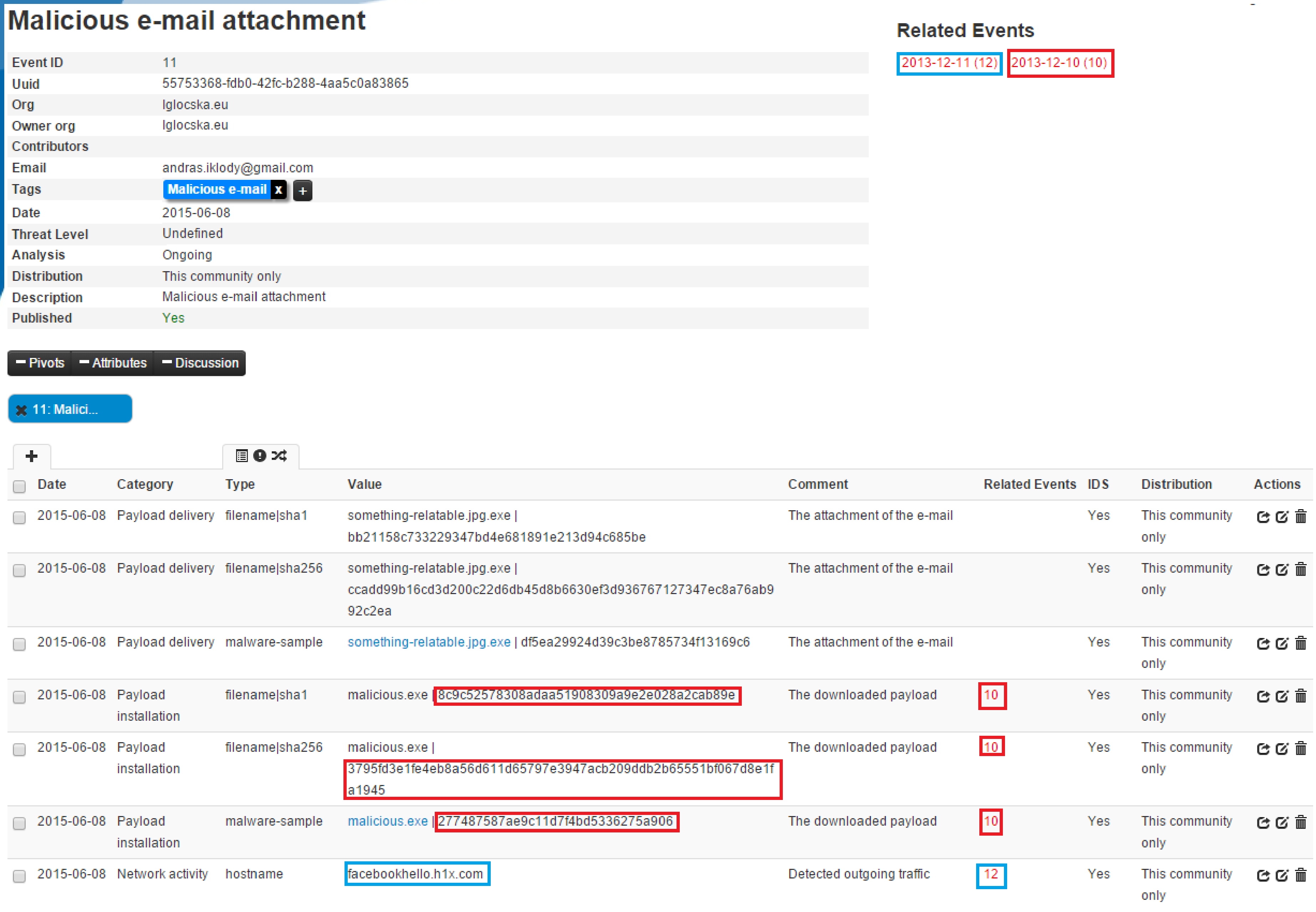
| | |
|---|---|
| Event ID | 11 |
| Uuid | 55753368-fdb0-42fc-b288-4aa5c0a83865 |
| Org | lglocska.eu |
| Owner org | lglocska.eu |
| Contributors | |
| Email | andras.iklody@gmail.com |
| Tags | Malicious e-mail x + |
| Date | 2015-06-08 |
| Threat Level | Undefined |
| Analysis | Ongoing |
| Distribution | This community only |
| Description | Malicious e-mail attachment |
| Published | Yes |

**Related Events**

2013-12-11 (12) 2013-12-10 (10)

| ☐ | Date | Category | Type | Value | Comment | Related Events | IDS | Distribution | Actions |
|---|---|---|---|---|---|---|---|---|---|
| ☐ | 2015-06-08 | Payload delivery | filename\|sha1 | something-relatable.jpg.exe \| bb21158c733229347bd4e681891e213d94c685be | The attachment of the e-mail | | Yes | This community only | |
| ☐ | 2015-06-08 | Payload delivery | filename\|sha256 | something-relatable.jpg.exe \| ccadd99b16cd3d200c22d6db45d8b6630ef3d936767127347ec8a76ab992c2ea | The attachment of the e-mail | | Yes | This community only | |
| ☐ | 2015-06-08 | Payload delivery | malware-sample | something-relatable.jpg.exe \| df5ea29924d39c3be8785734f13169c6 | The attachment of the e-mail | | Yes | This community only | |
| ☐ | 2015-06-08 | Payload installation | filename\|sha1 | malicious.exe \| 8c9c52578308adaa51908309a9e2e028a2cab89e | The downloaded payload | 10 | Yes | This community only | |
| ☐ | 2015-06-08 | Payload installation | filename\|sha256 | malicious.exe \| 3795fd3e1fe4eb8a56d611d65797e3947acb209ddb2b65551bf067d8e1fa1945 | The downloaded payload | 10 | Yes | This community only | |
| ☐ | 2015-06-08 | Payload installation | malware-sample | malicious.exe \| 277487587ae9c11d7f4bd5336275a906 | The downloaded payload | 10 | Yes | This community only | |
| ☐ | 2015-06-08 | Network activity | hostname | facebookhello.h1x.com | Detected outgoing traffic | 12 | Yes | This community only | |

# Correlating data example



## Malicious e-mail attachment

|  |  |
|---|---|
| Event ID | 11 |
| Uuid | 55753368-fdb0-42fc-b288-4aa5c0a83865 |
| Org | lglocska.eu |
| Owner org | lglocska.eu |
| Contributors |  |
| Email | andras.iklody@gmail.com |
| Tags | Malicious e-mail x + |
| Date | 2015-06-08 |
| Threat Level | Undefined |
| Analysis | Ongoing |
| Distribution | This community only |
| Description | Malicious e-mail attachment |
| Published | Yes |

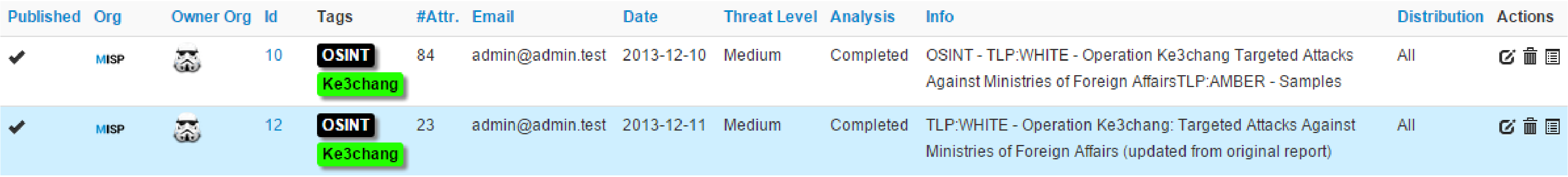
**Related Events**

2013-12-11 (12) 2013-12-10 (10)

| □ | Date | Category | Type | Value | Comment | Related Events | IDS | Distribution | Actions |
|---|---|---|---|---|---|---|---|---|---|
| □ | 2015-06-08 | Payload delivery | filename\|sha1 | something-relatable.jpg.exe \| bb21158c733229347bd4e681891e213d94c685be | The attachment of the e-mail |  | Yes | This community only |  |
| □ | 2015-06-08 | Payload delivery | filename\|sha256 | something-relatable.jpg.exe \| ccadd99b16cd3d200c22d6db45d8b6630ef3d936767127347ec8a76ab992c2ea | The attachment of the e-mail |  | Yes | This community only |  |
| □ | 2015-06-08 | Payload delivery | malware-sample | something-relatable.jpg.exe \| df5ea29924d39c3be8785734f13169c6 | The attachment of the e-mail |  | Yes | This community only |  |
| □ | 2015-06-08 | Payload installation | filename\|sha1 | malicious.exe \| 8c9c52578308adaa51908309a9e2e028a2cab89e | The downloaded payload | 10 | Yes | This community only |  |
| □ | 2015-06-08 | Payload installation | filename\|sha256 | malicious.exe \| 3795fd3e1fe4eb8a56d611d65797e3947acb209ddb2b65551bf067d8e1fa1945 | The downloaded payload | 10 | Yes | This community only |  |
| □ | 2015-06-08 | Payload installation | malware-sample | malicious.exe \| 277487587ae9c11d7f4bd5336275a906 | The downloaded payload | 10 | Yes | This community only |  |
| □ | 2015-06-08 | Network activity | hostname | facebookhello.h1x.com | Detected outgoing traffic | 12 | Yes | This community only |  |

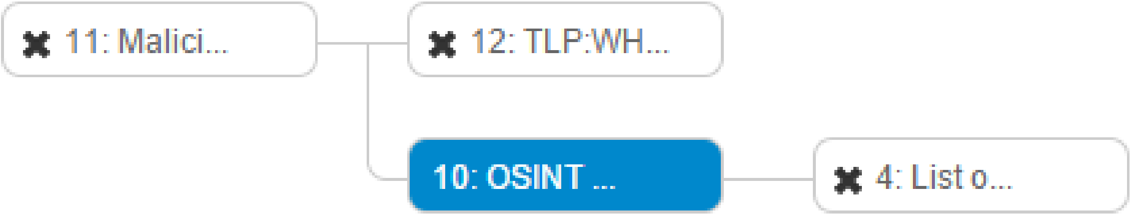
# Correlating data example

- So we found 2 correlated events, both of which are OSINT reports about Operation Ke3chang



| Published | Org | Owner Org | Id | Tags | #Attr. | Email | Date | Threat Level | Analysis | Info | Distribution | Actions |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ✓ | MISP | | 10 | OSINT<br>Ke3chang | 84 | admin@admin.test | 2013-12-10 | Medium | Completed | OSINT - TLP:WHITE - Operation Ke3chang Targeted Attacks Against Ministries of Foreign AffairsTLP:AMBER - Samples | All | |
| ✓ | MISP | | 12 | OSINT<br>Ke3chang | 23 | admin@admin.test | 2013-12-11 | Medium | Completed | TLP:WHITE - Operation Ke3chang: Targeted Attacks Against Ministries of Foreign Affairs (updated from original report) | All | |

- While pivoting through the relations, MISP built a chart showing the relations as we traversed them:

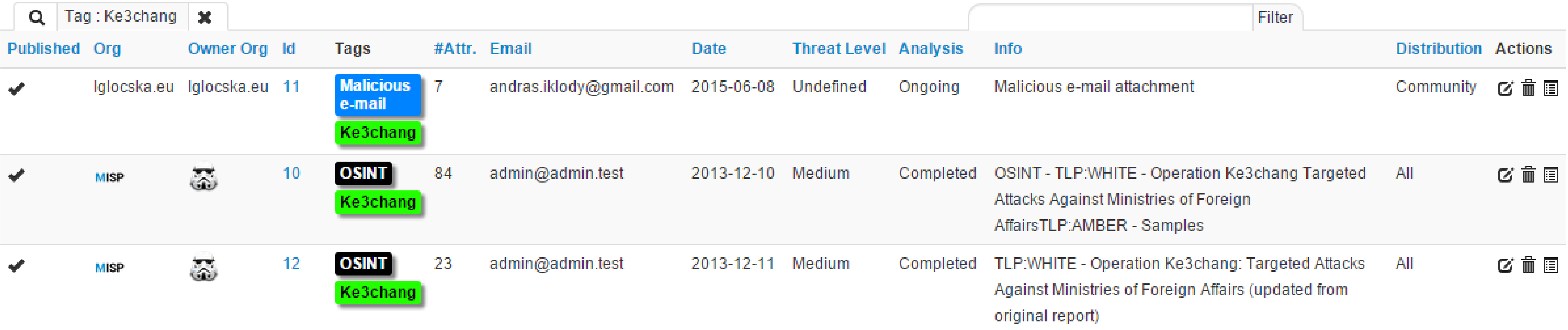


# *Tagging data*

- Tagging allows us to group events together based on arbitrary commonalities
  - Source (Privint, OSINT, etc)
  - TLP
  - Campaigns or Threat actors
  - Type of event (for example malicious attachment)
- Local to the instance
- Search-able, usable as a filter in the API
- Upcoming version: tags can be filters on the synchronization (similar to subscribing to feeds / restricting outgoing data based on tags)

# Tagging example

- So in this case, we found an event that should be tagged Ke3chang too
- Using Ke3chang as a filter option we get the following result now:



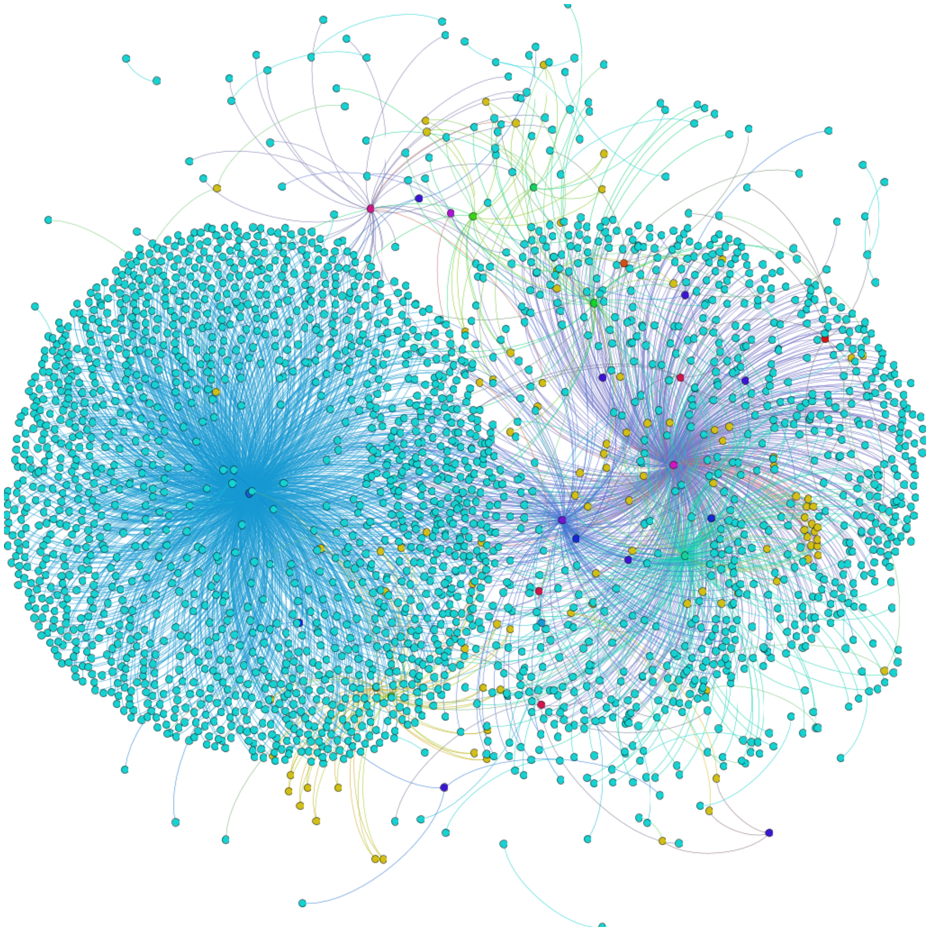
Tag : Ke3chang ✖

Filter

| Published | Org | Owner Org | Id | Tags | #Attr. | Email | Date | Threat Level | Analysis | Info | Distribution | Actions |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ✓ | Iglocska.eu | Iglocska.eu | 11 | Malicious e-mail<br>Ke3chang | 7 | andras.iklody@gmail.com | 2015-06-08 | Undefined | Ongoing | Malicious e-mail attachment | Community | |
| ✓ | MISP | | 10 | OSINT<br>Ke3chang | 84 | admin@admin.test | 2013-12-10 | Medium | Completed | OSINT - TLP:WHITE - Operation Ke3chang Targeted Attacks Against Ministries of Foreign AffairsTLP:AMBER - Samples | All | |
| ✓ | MISP | | 12 | OSINT<br>Ke3chang | 23 | admin@admin.test | 2013-12-11 | Medium | Completed | TLP:WHITE - Operation Ke3chang: Targeted Attacks Against Ministries of Foreign Affairs (updated from original report) | All | |

# *Visualisation of the data*

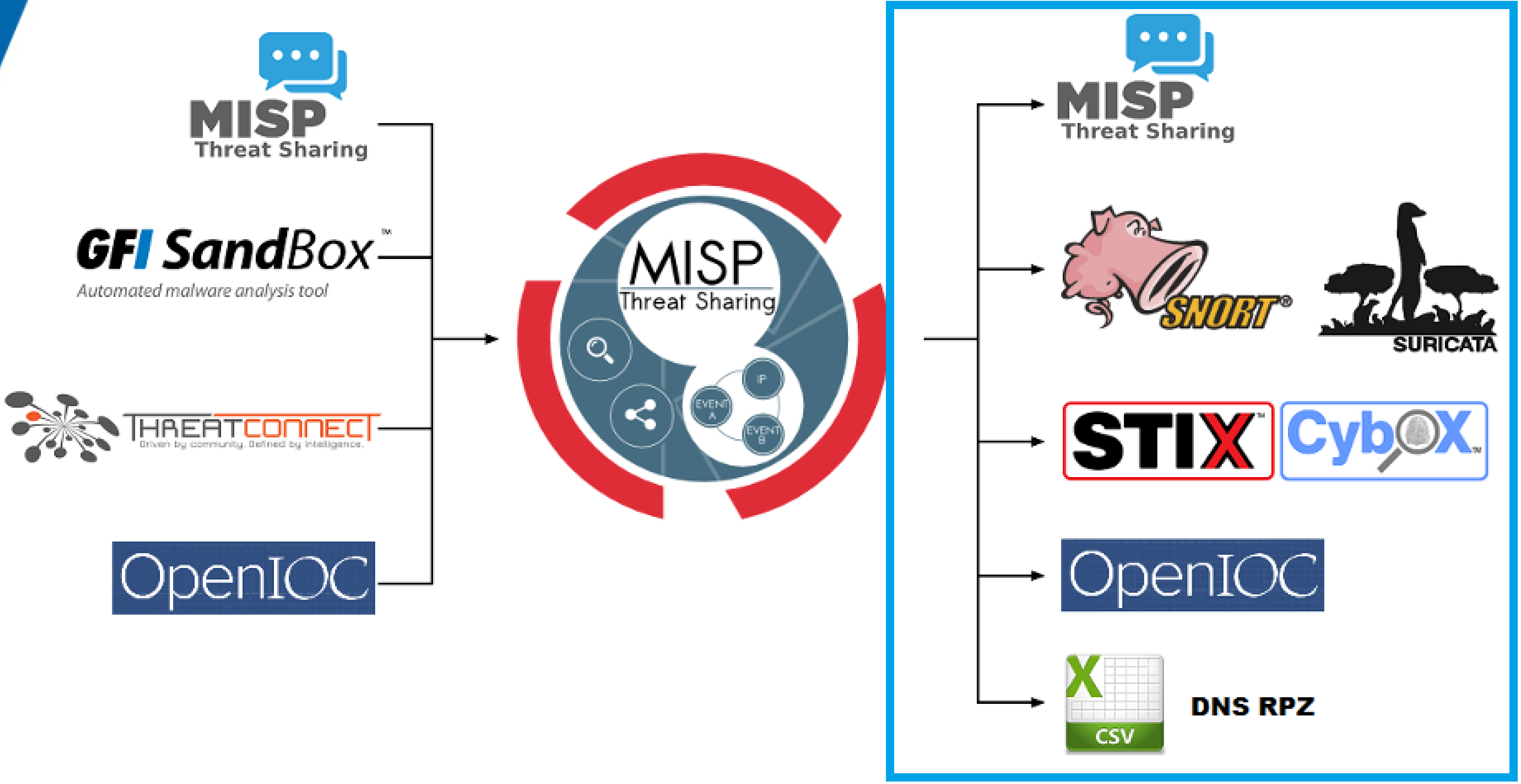
- Pivoting graph as shown before
- Using Maltego (tool developed by Andrzej Dereszowski)
- Using MISP-Graph (tool developed by Alexandre Dulaunoy from CIRCL)
- Upcoming graphing tool in the MISP UI



# *Building automated protection*
# ***Feed your defenses***

- Overview
- Various export formats of MISP
- Feed a wide range of systems using MISP
- A flexible API
- Build and use tools that use the MISP APIs

# Exporting data from MISP



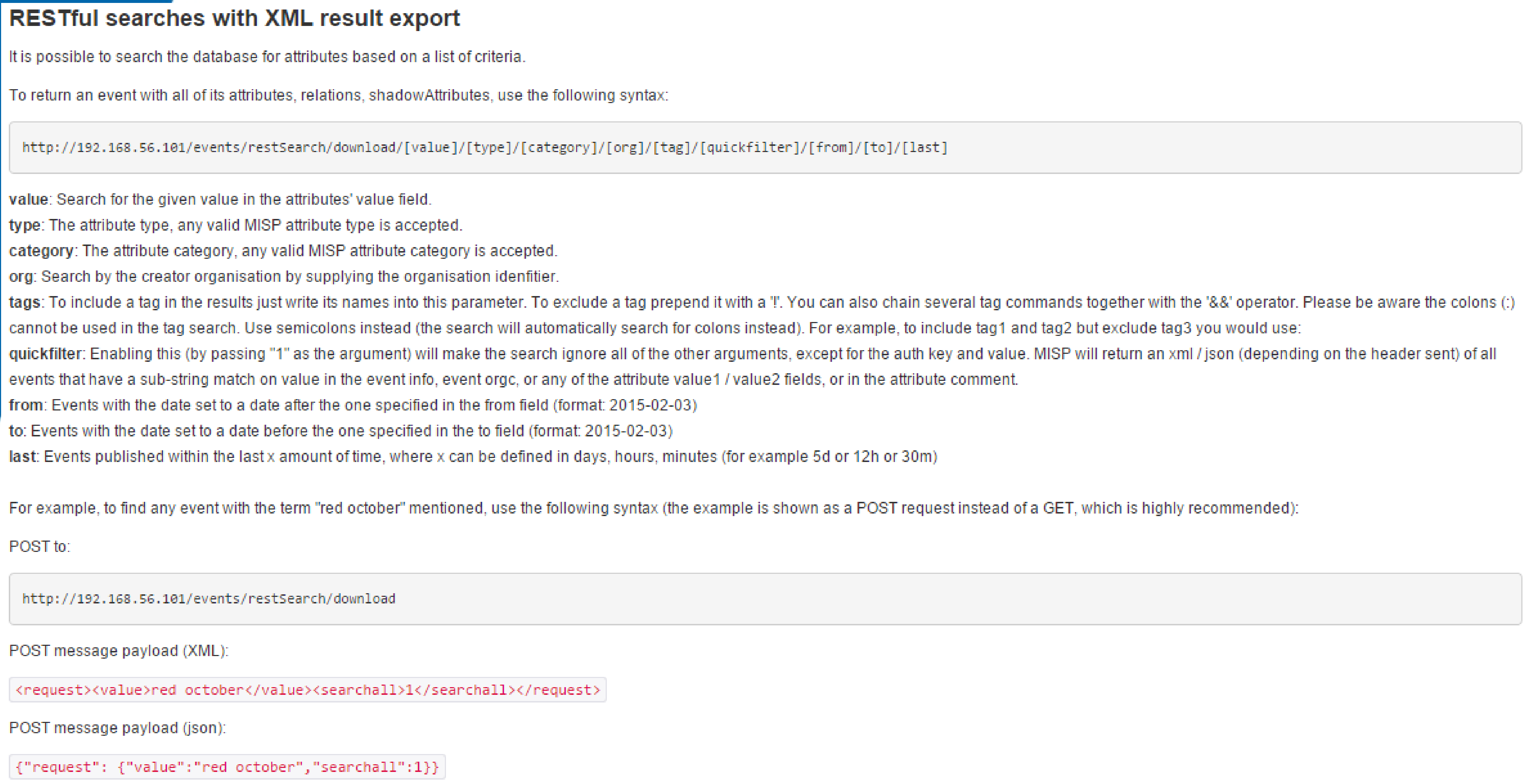
# *Feed a wide range of systems using MISP*

- NIDS (Suricata, Snort, STIX/CyBox)
- HIDS (OpenIOC, STIX/CyBox, CSV)
- SIEMs
- DNS level firewalls (DNS Responce Policy Zones)
- Forensic scanners
- Throw values obtained from CSV exports against your packet capture
- ...

# *A flexible API*

- Use the APIs to continuously retrieve the data that you are actually interested in
- Flexible filter parameters
- Build complex queries
  - Return all hostnames and domain names from events tagged Ke3chang that got published within the past 14 days
  - Return a snort rule set for all events not tagged OSINT from the past 24 hours

# A flexible API



## RESTful searches with XML result export

It is possible to search the database for attributes based on a list of criteria.

To return an event with all of its attributes, relations, shadowAttributes, use the following syntax:

```
http://192.168.56.101/events/restSearch/download/[value]/[type]/[category]/[org]/[tag]/[quickfilter]/[from]/[to]/[last]
```

**value**: Search for the given value in the attributes' value field.
**type**: The attribute type, any valid MISP attribute type is accepted.
**category**: The attribute category, any valid MISP attribute category is accepted.
**org**: Search by the creator organisation by supplying the organisation idenfitier.
**tags**: To include a tag in the results just write its names into this parameter. To exclude a tag prepend it with a '!'. You can also chain several tag commands together with the '&&' operator. Please be aware the colons (:) cannot be used in the tag search. Use semicolons instead (the search will automatically search for colons instead). For example, to include tag1 and tag2 but exclude tag3 you would use:
**quickfilter**: Enabling this (by passing "1" as the argument) will make the search ignore all of the other arguments, except for the auth key and value. MISP will return an xml / json (depending on the header sent) of all events that have a sub-string match on value in the event info, event orgc, or any of the attribute value1 / value2 fields, or in the attribute comment.
**from**: Events with the date set to a date after the one specified in the from field (format: 2015-02-03)
**to**: Events with the date set to a date before the one specified in the to field (format: 2015-02-03)
**last**: Events published within the last x amount of time, where x can be defined in days, hours, minutes (for example 5d or 12h or 30m)

For example, to find any event with the term "red october" mentioned, use the following syntax (the example is shown as a POST request instead of a GET, which is highly recommended):

POST to:

```
http://192.168.56.101/events/restSearch/download
```

POST message payload (XML):

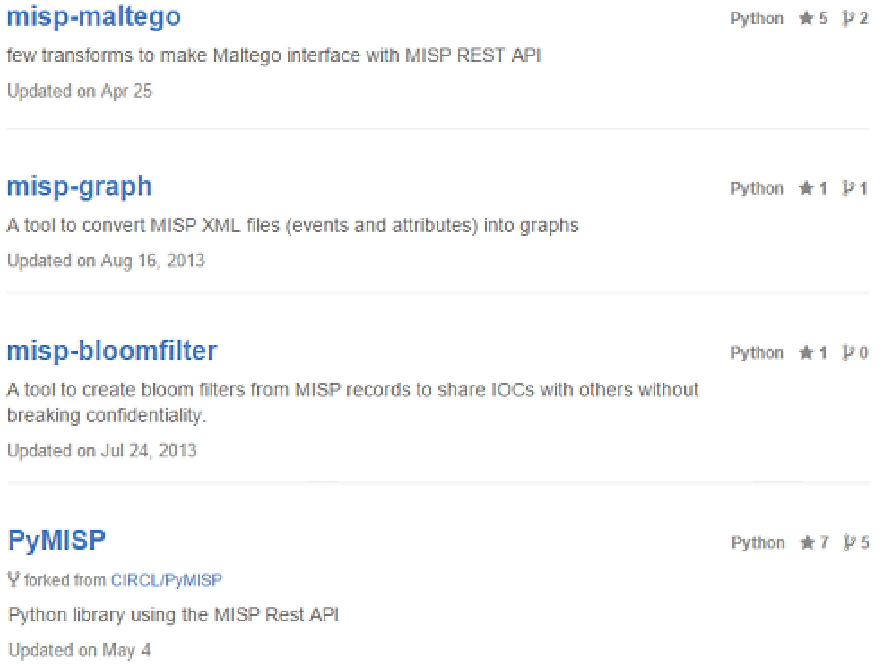
```
<request><value>red october</value><searchall>1</searchall></request>
```

POST message payload (json):

```
{"request": {"value":"red october","searchall":1}}
```

# Build and use tools that use the MISP APIs

- Tools ingesting the exports of MISP
- Built by the community and shared on the MISP github repository
- A modular import/export feature is planned that will make development for MISP easier
- We always welcome more additions!



**misp-maltego** Python ★ 5 ⑂ 2

few transforms to make Maltego interface with MISP REST API

Updated on Apr 25

**misp-graph** Python ★ 1 ⑂ 1

A tool to convert MISP XML files (events and attributes) into graphs

Updated on Aug 16, 2013

**misp-bloomfilter** Python ★ 1 ⑂ 0

A tool to create bloom filters from MISP records to share IOCs with others without breaking confidentiality.

Updated on Jul 24, 2013

**PyMISP** Python ★ 7 ⑂ 5

⑂ forked from CIRCL/PyMISP

Python library using the MISP Rest API

Updated on May 4

# *Why adopt MISP?*

- Allows you to create, ingest and share IOCs and threat intelligence without a hassle
- Building defenses out of the efforts of your partners has never been this easy
- MISP is constantly evolving
- It is widely adopted and chances are your partners are already exchanging information using MISP
- It is completely open-source and you can join the ever-growing community of organizations that share their improvements
- It is commercially supported
- Is free and developed by a non-profit

# *Questions and practical information*

- To get in touch with me: **andras.iklody@gmail.com**
- Contact the MISP Project: **info@misp-project.org**
- Website: **http://www.misp-project.org**
- Users list: **https://groups.google.com/forum/#!forum/misp-users**
- Developers list: **https://groups.google.com/forum/#!forum/misp-devel**
- Github: **http://github.com/MISP/MISP**
- Information and access request for the CIRCL MISP communities: **https://www.circl.lu/services/misp-malware-information-sharing-platform**

***Do you want to support the non-profit MISP project? Contact us for partnership !***