cyber threat

threat **landscape**

threat **intellll**ligence

threat indicator

bon**A**ay**P**ee**T**eet

THE **cloud**

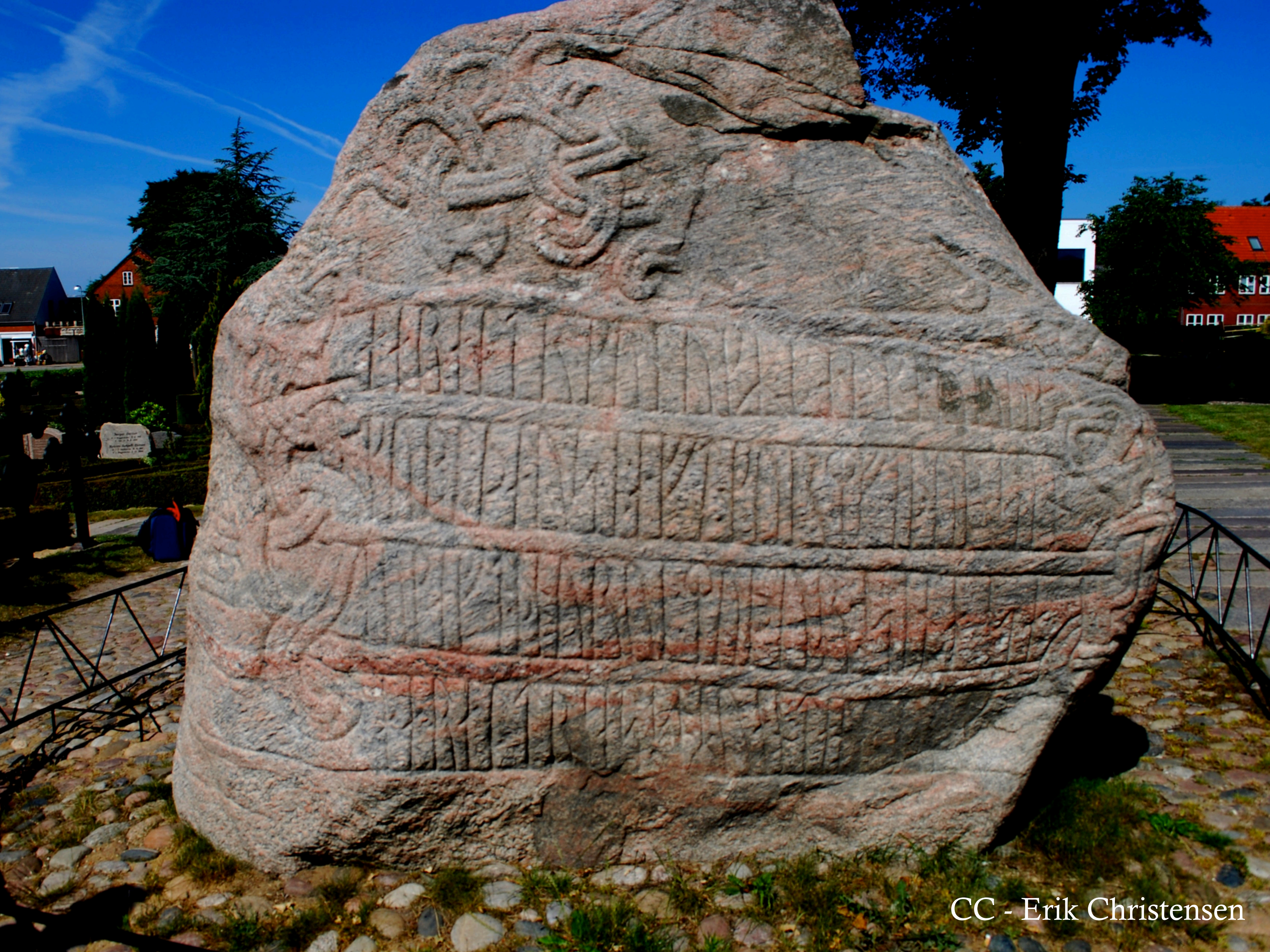
data **feed**

CC - Elisa Azzali

CC - Tim Morgan

CC - Quinn Dombrowski

Public domain - Theodore C. Marceau



CC - Erik Christensen

MISP
Threat Sharing

Damn-fast and effective malware info sharing with MISP

by Christophe Vandeplas

http://misp-project.org

MISP is…

- a repository of malware, IOCs and 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 from your interconnected partners

MISP
Threat Sharing

History

- 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
- Open source - AGPL
- CIRCL : added tools and APIs around MISP
- Today Andras Iklody is the main developer
- Rapidly growing user community, improvements and new features are being added by various 3rd parties

What issues does MISP try to tackle?

The situation without MISP

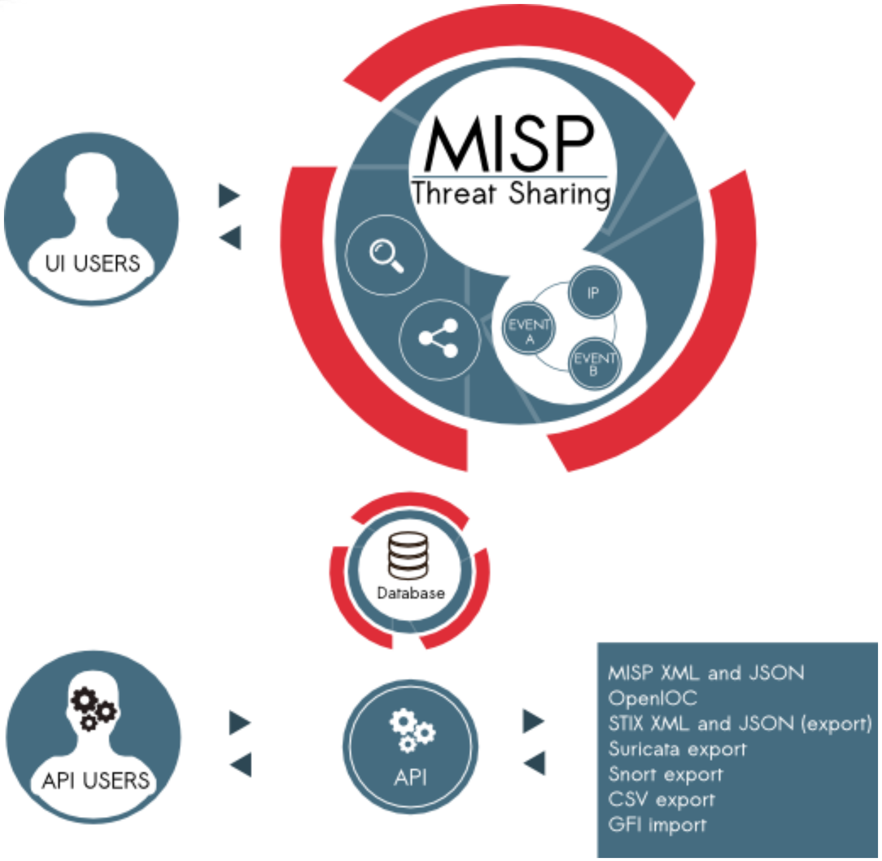
- There has always been some level of information sharing
- But most of the time it happened ad hoc:
  - Phone call
  - e-mail with a CSV with malicious IP addresses
  - Or for people we don't like: PDFs with indicators in the text

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
- 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?

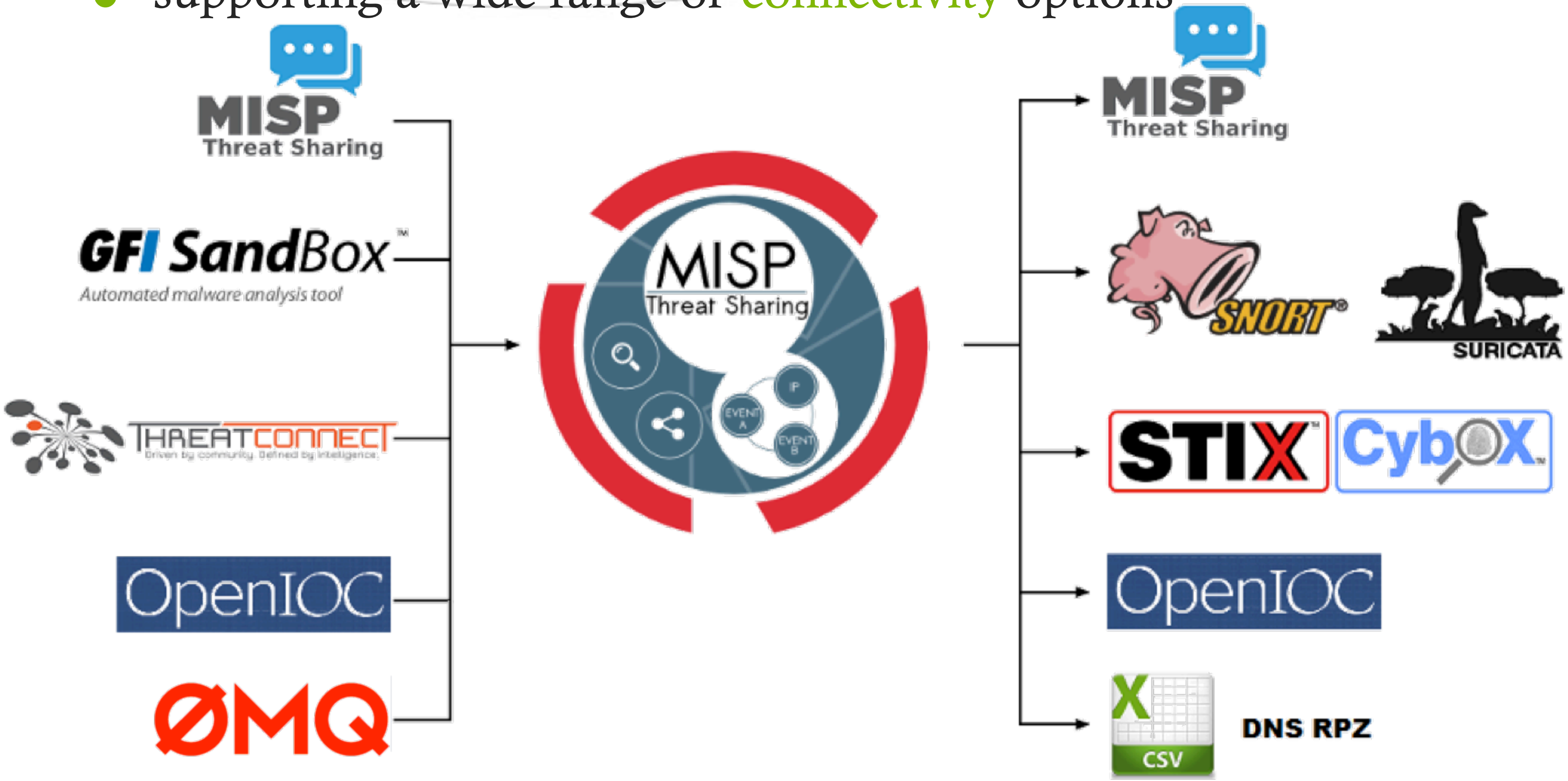
- Various ways to interact with the data in MISP:
  - Web interface
  - API
  - Indirectly (exports / imports)



MISP XML and JSON
OpenIOC
STIX XML and JSON (export)
Suricata export
Snort export
CSV export
GFI import

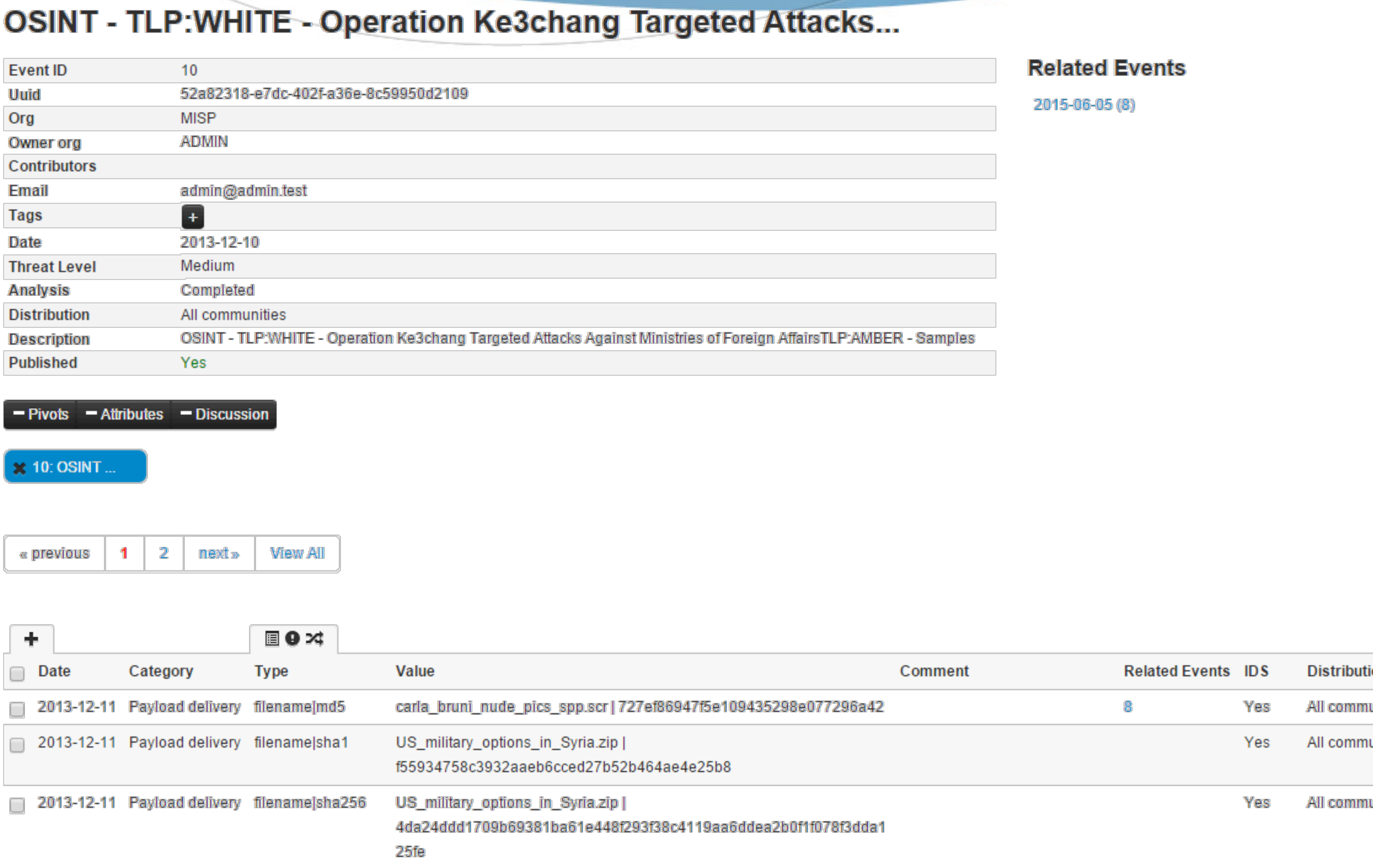
Inter connectivity

- supporting a wide range of connectivity options



The data structure at a glance

- Designed not to overwhelm users
- The main design concept: Capture what is actually important
- An Event contains Attributes
- Attributes: 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

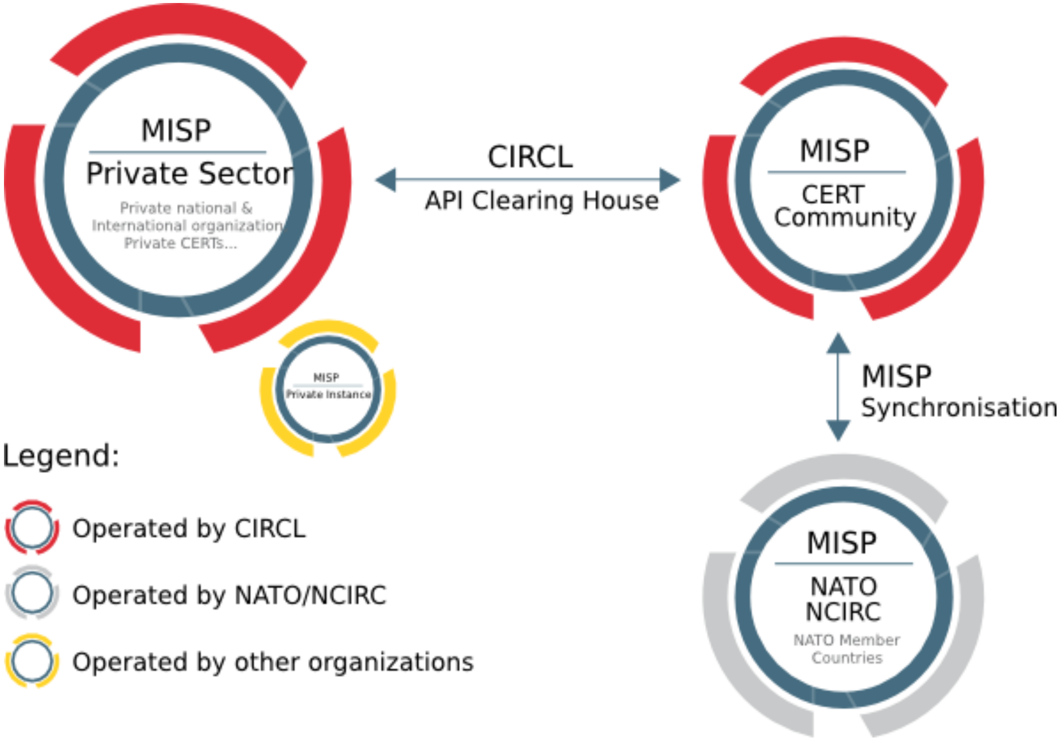
Related Events

2015-06-05 (8)

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

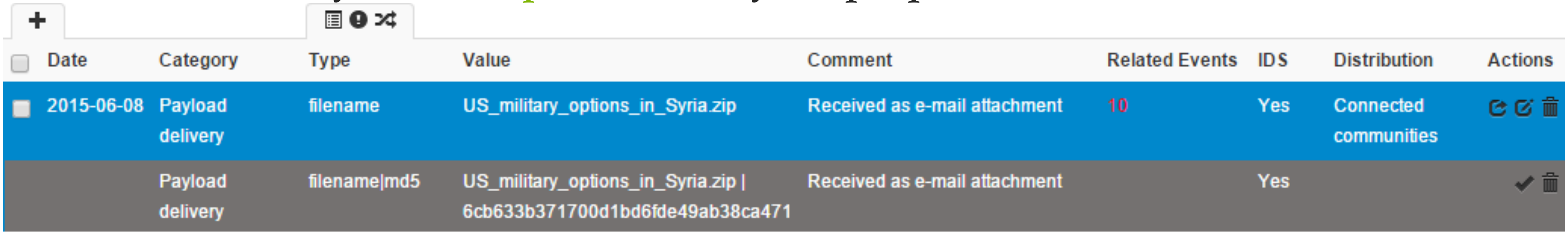
Sharing and collaboration

- 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
- Topology example at CIRCL
- Email alert on publish (PGP encrypted/signed)

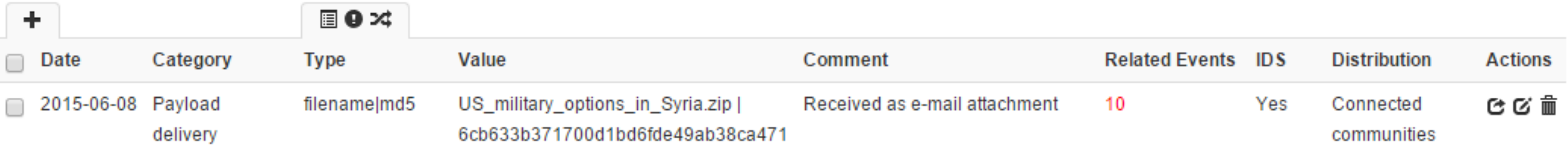


Sharing and collaboration

- 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



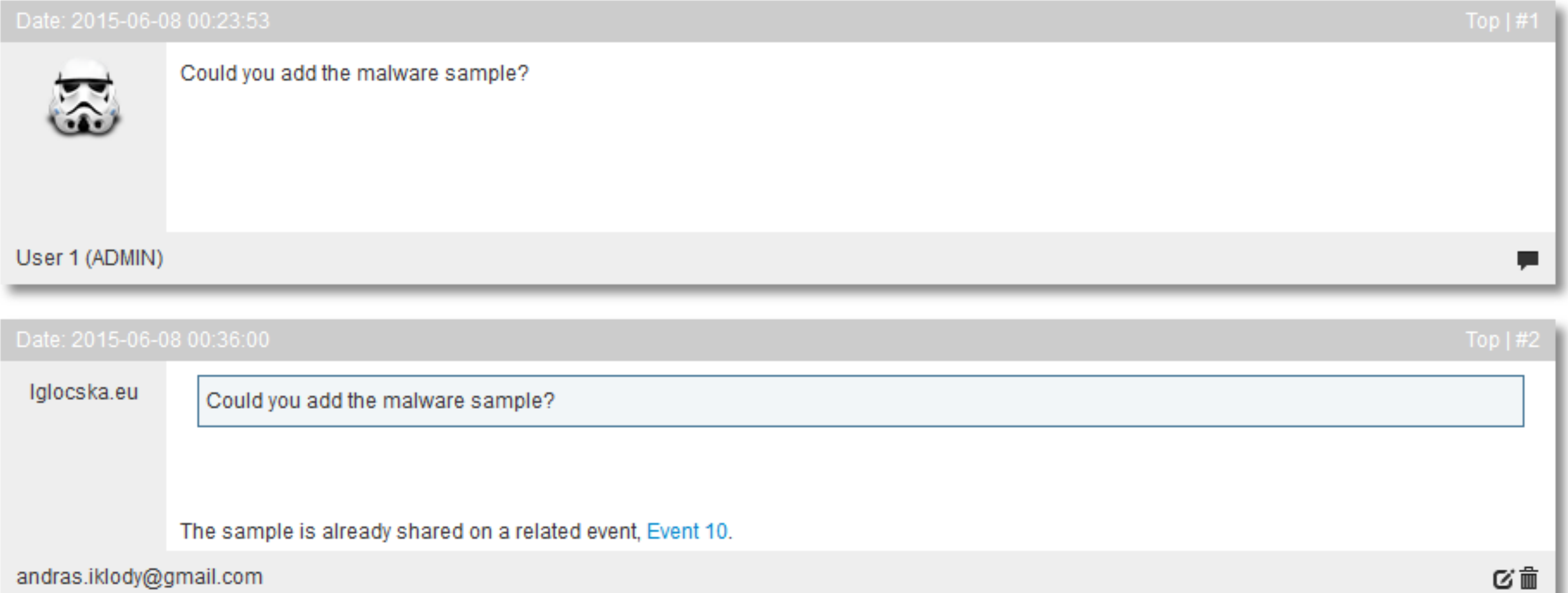
□	Date	Category	Type	Value	Comment	Related Events	IDS	Distribution	Actions
□	2015-06-08	Payload delivery	filename	US_military_options_in_Syria.zip	Received as e-mail attachment	10	Yes	Connected communities	
		Payload delivery	filename|md5	US_military_options_in_Syria.zip | 6cb633b371700d1bd6fde49ab38ca471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

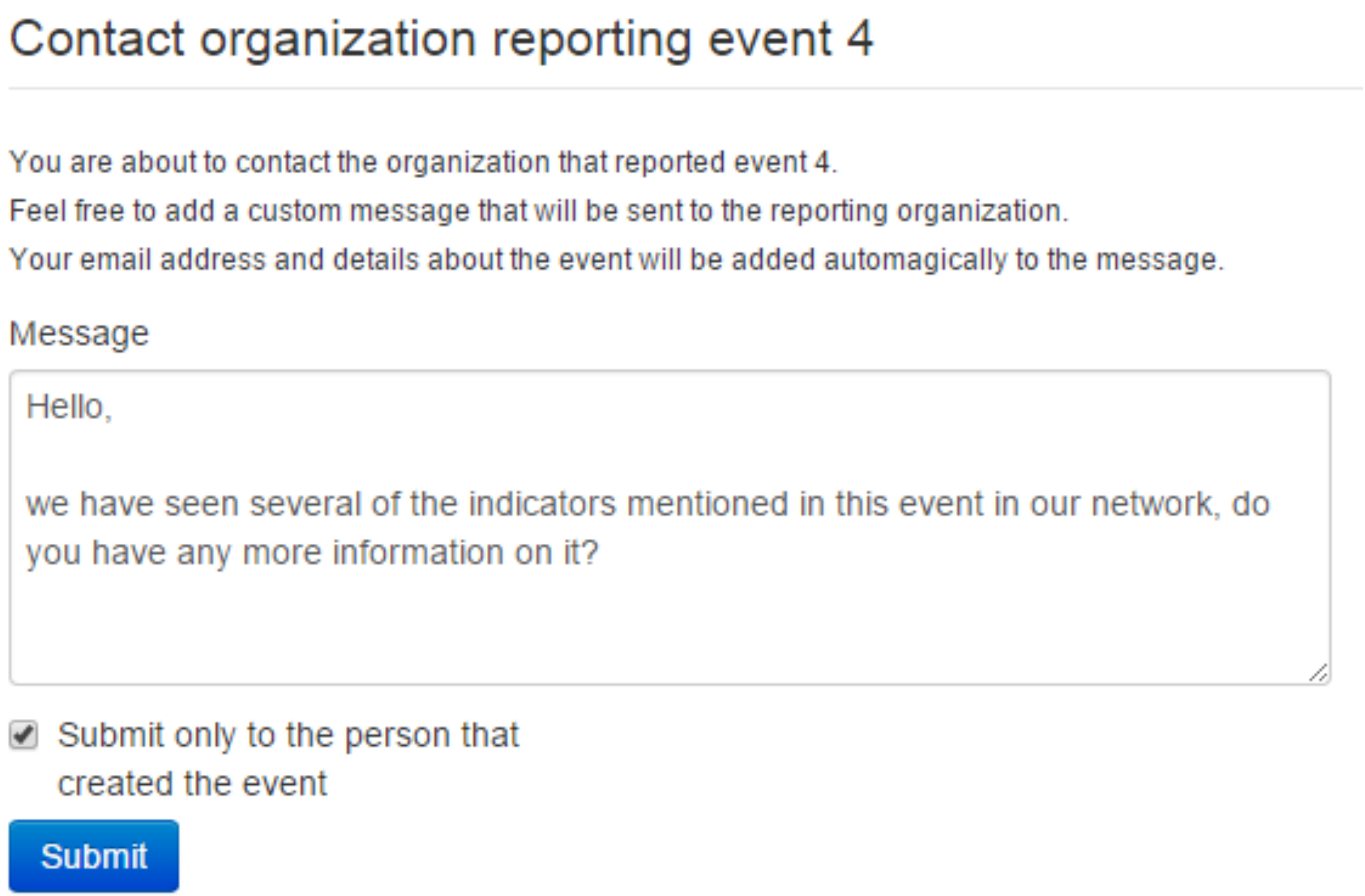
> Could you add the malware sample?

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

andras.iklody@gmail.com

MISP
Threat Sharing

Sharing and collaboration



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?

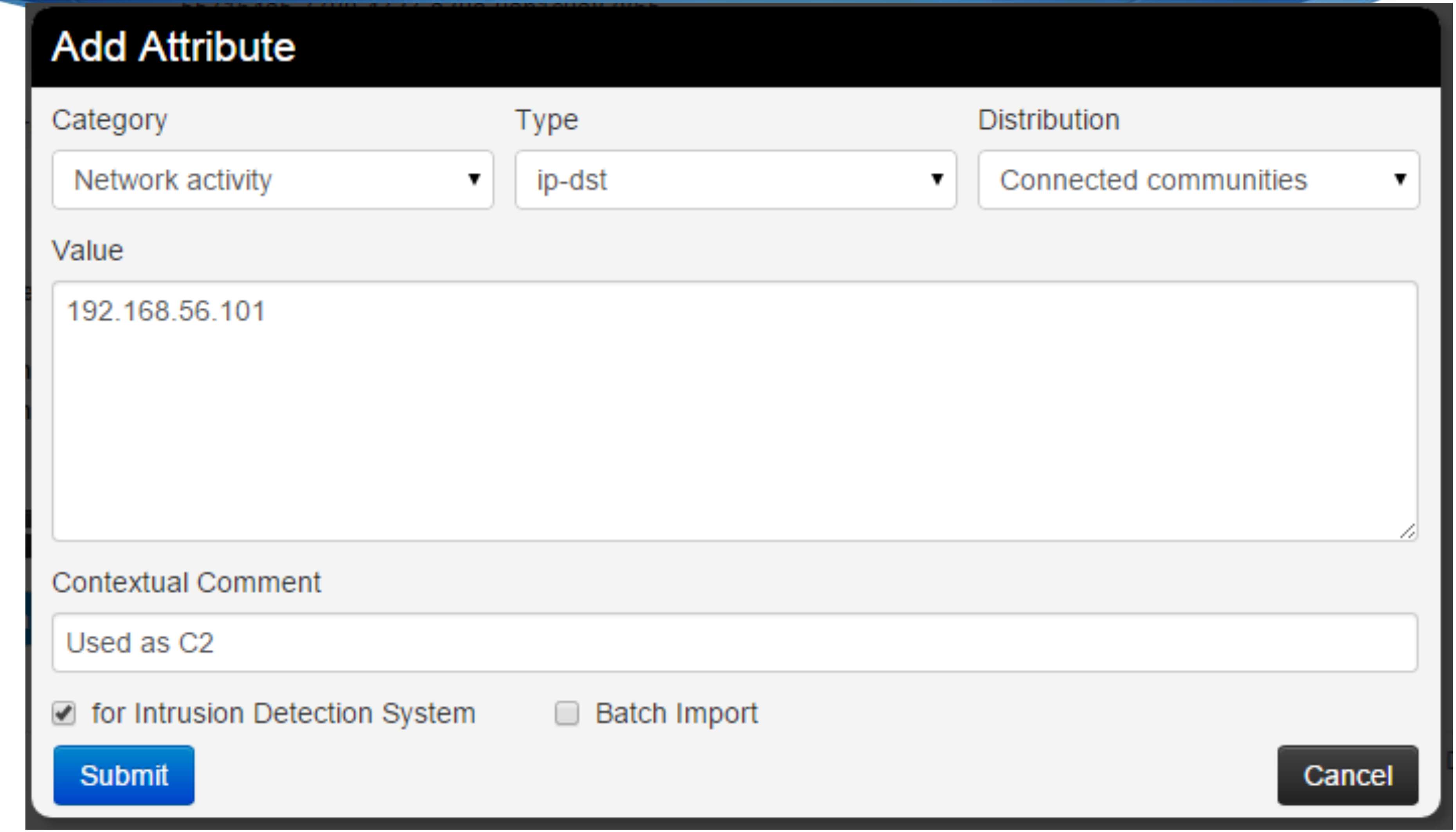
☑ Submit only to the person that created the event

That was the theory, now the practical part

Adding stuff in MISP

- 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

Simple interface to create attributes



Add Attribute

Category: Network activity

Type: ip-dst

Distribution: Connected communities

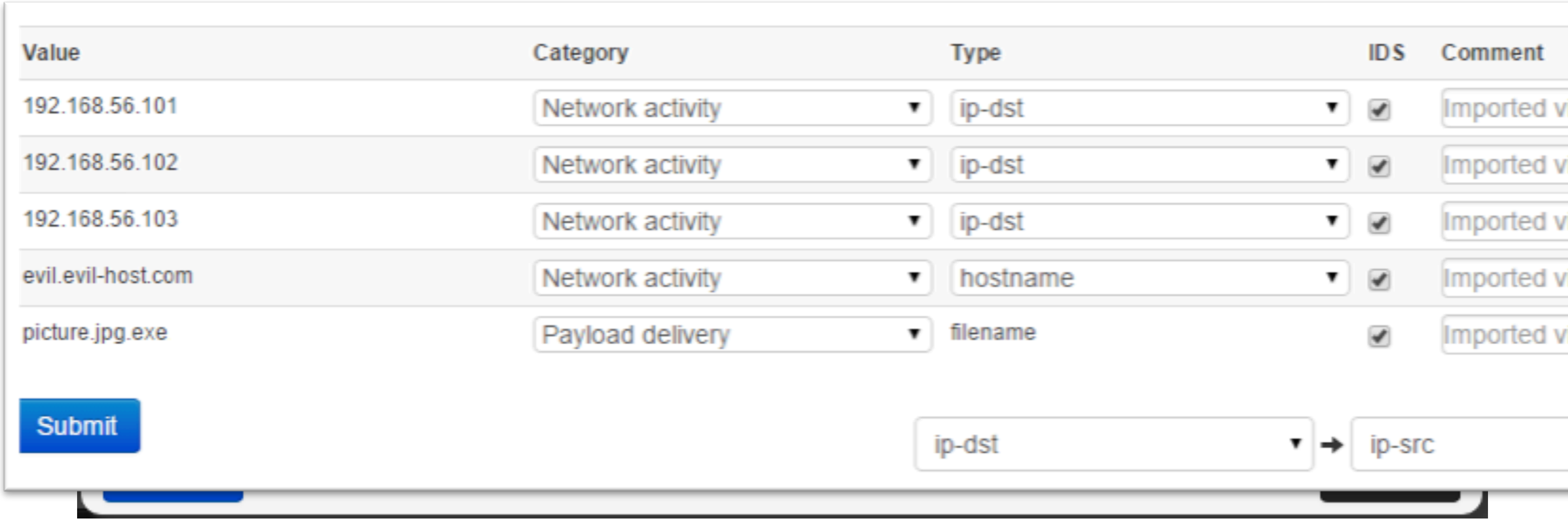
Value: 192.168.56.101

Contextual Comment: Used as C2

☑ for Intrusion Detection System

□ Batch Import

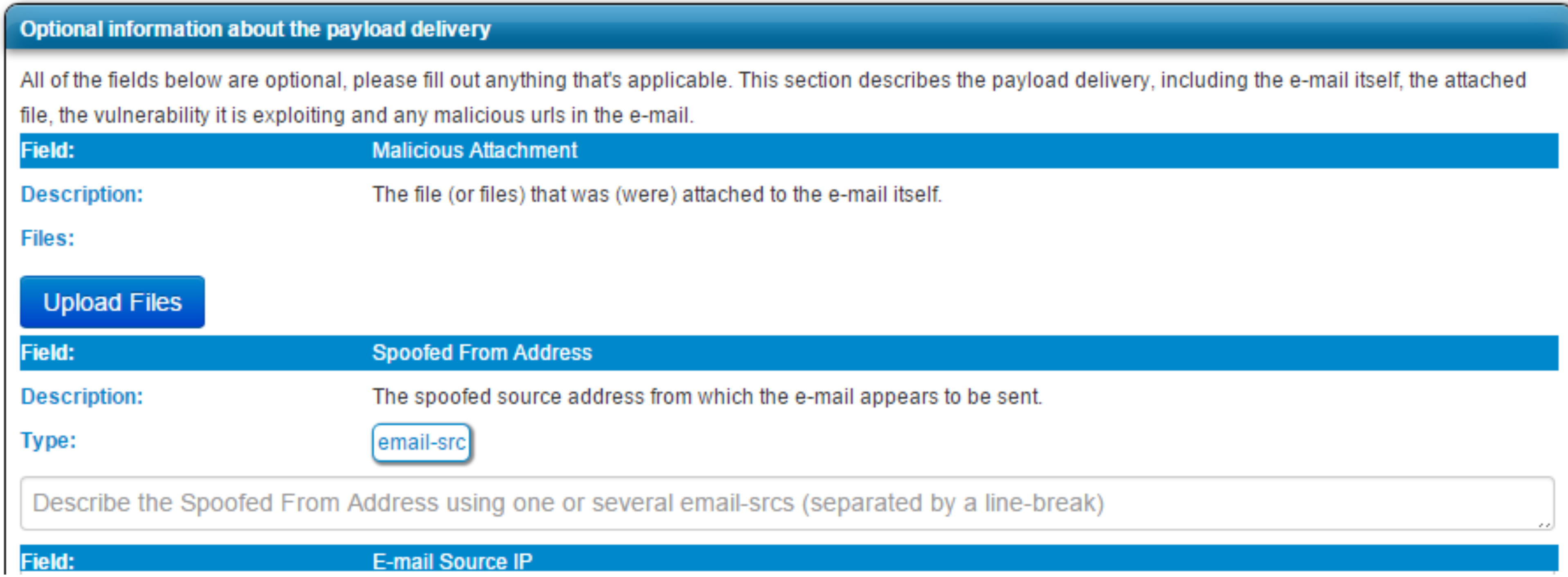
Free-text Import Tool



Value	Category	Type	IDS	Comment
192.168.56.101	Network activity ▾	ip-dst ▾	☑	Imported v
192.168.56.102	Network activity ▾	ip-dst ▾	☑	Imported v
192.168.56.103	Network activity ▾	ip-dst ▾	☑	Imported v
evil.evil-host.com	Network activity ▾	hostname ▾	☑	Imported v
picture.jpg.exe	Payload delivery ▾	filename	☑	Imported v

Templates

- 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)

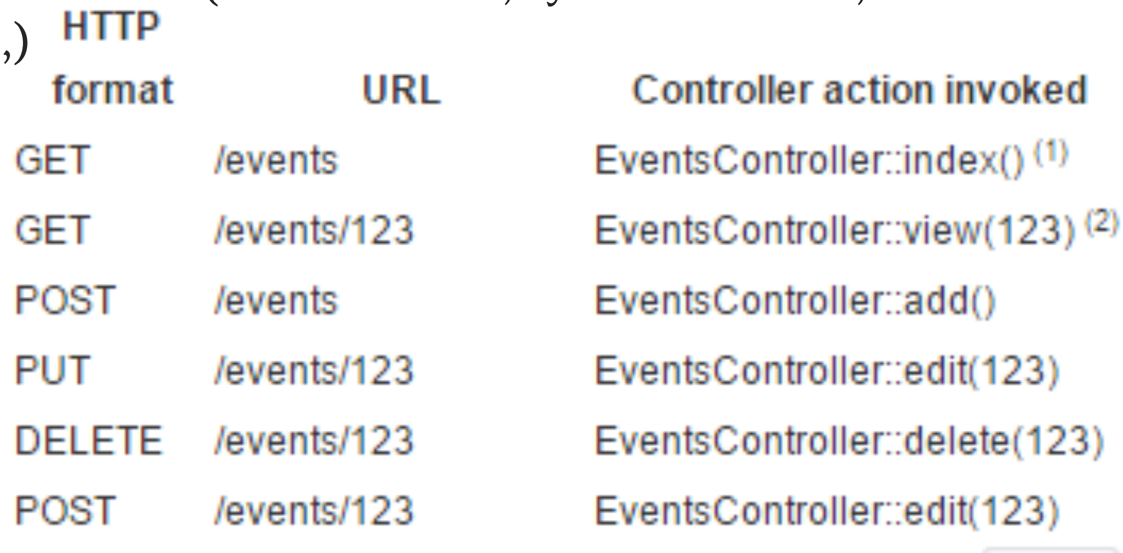
Field:	**E-mail Source IP**

REST API

- Allows you to interact with events and attributes

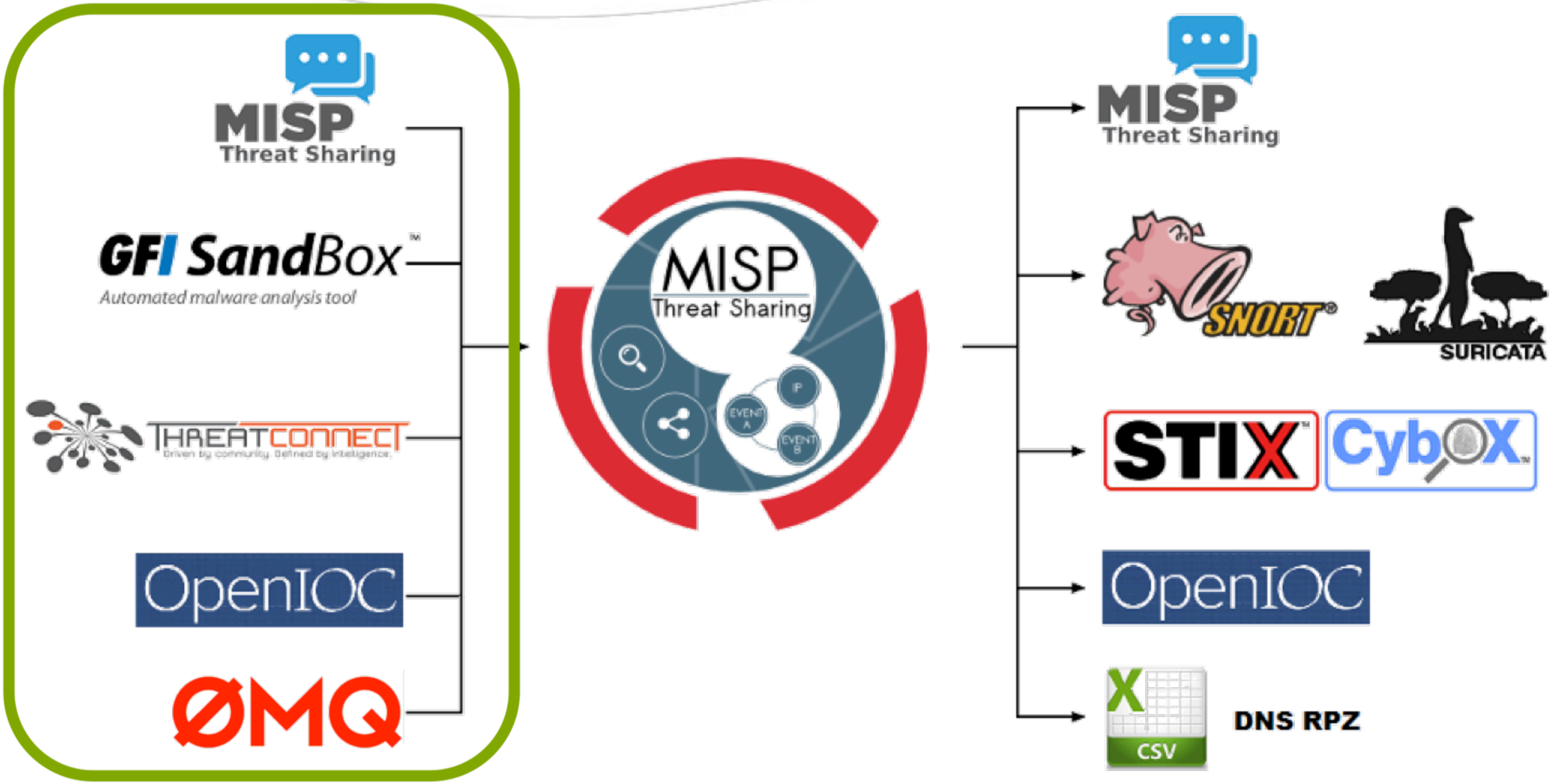
- You build scripts that modify data to MISP in a simple XML/JSON format using the REST API

- MISP takes care of the rest (access control, synchronization, notifications, correlation,)



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)

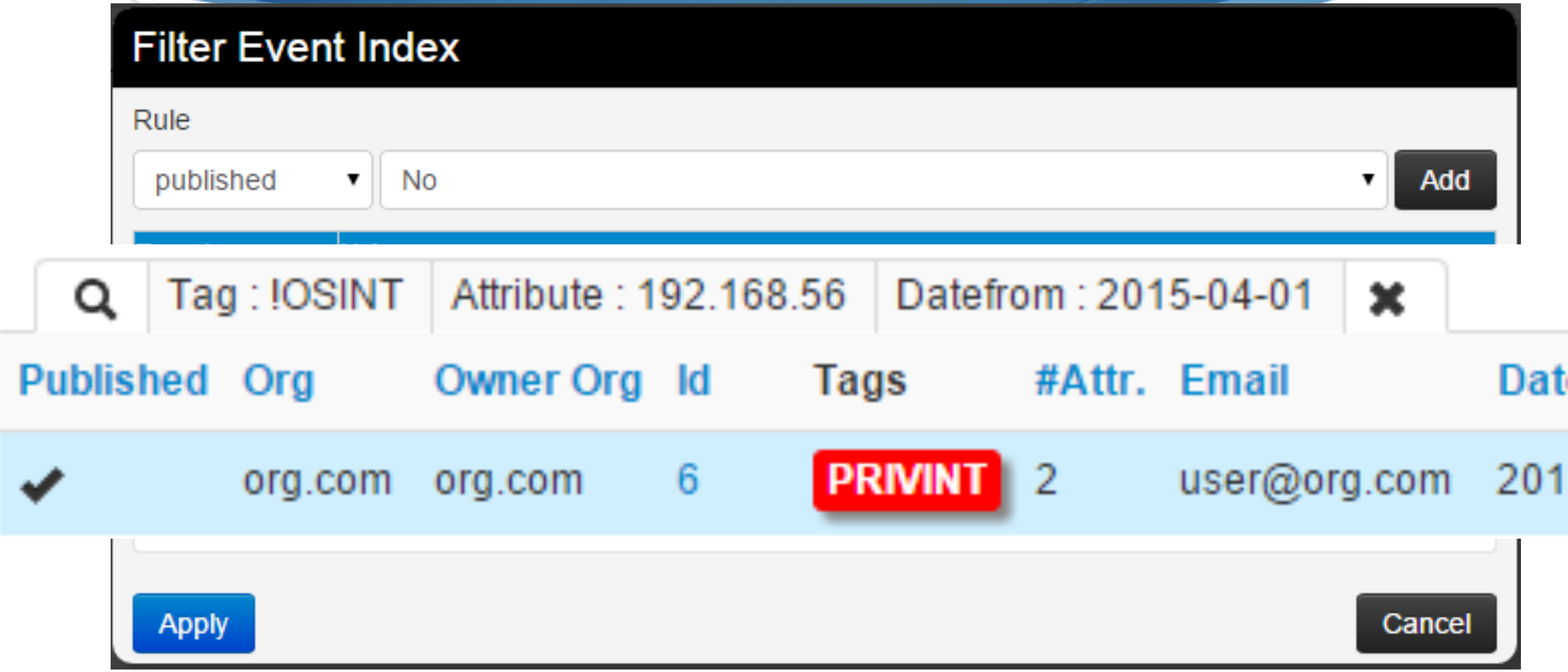
Importing options



Exploiting data within MISP

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

Finding data



Filter Event Index

Rule

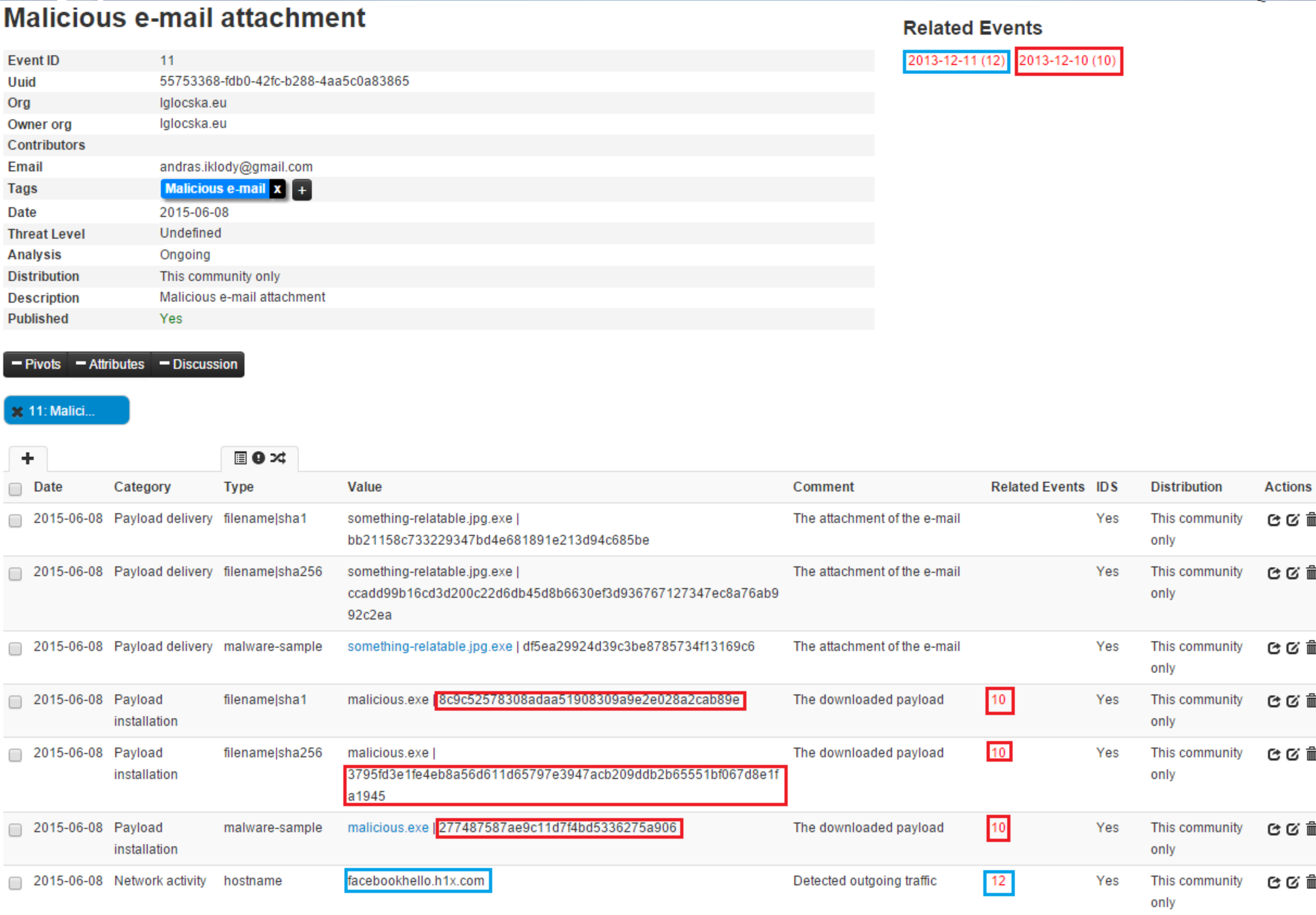
published ▾ No ▾ Add

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

Published	Org	Owner Org	Id	Tags	#Attr.	Email	Dat
✓	org.com	org.com	6	PRIVINT	2	user@org.com	201

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



Malicious e-mail attachment

Event ID	11
Uuid	55753368-fdb0-42fc-b288-4aa5c0a83865
Org	Iglocska.eu
Owner org	Iglocska.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

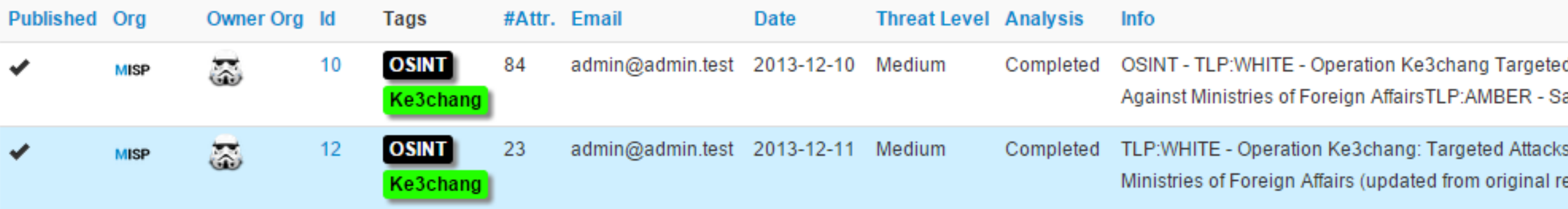
Related Events

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	

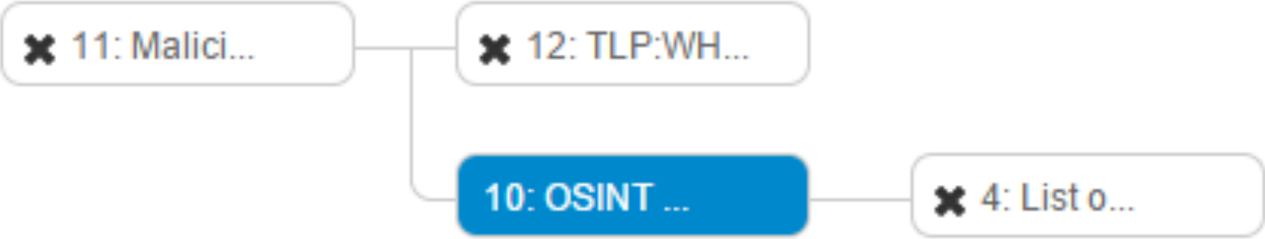
Example

- 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
✓	MISP		10	OSINT Ke3chang	84	admin@admin.test	2013-12-10	Medium	Completed	OSINT - TLP:WHITE - Operation Ke3chang Targetec Against Ministries of Foreign AffairsTLP:AMBER - Sa
✓	MISP		12	OSINT Ke3chang	23	admin@admin.test	2013-12-11	Medium	Completed	TLP:WHITE - Operation Ke3chang: Targeted Attacks Ministries of Foreign Affairs (updated from original re

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

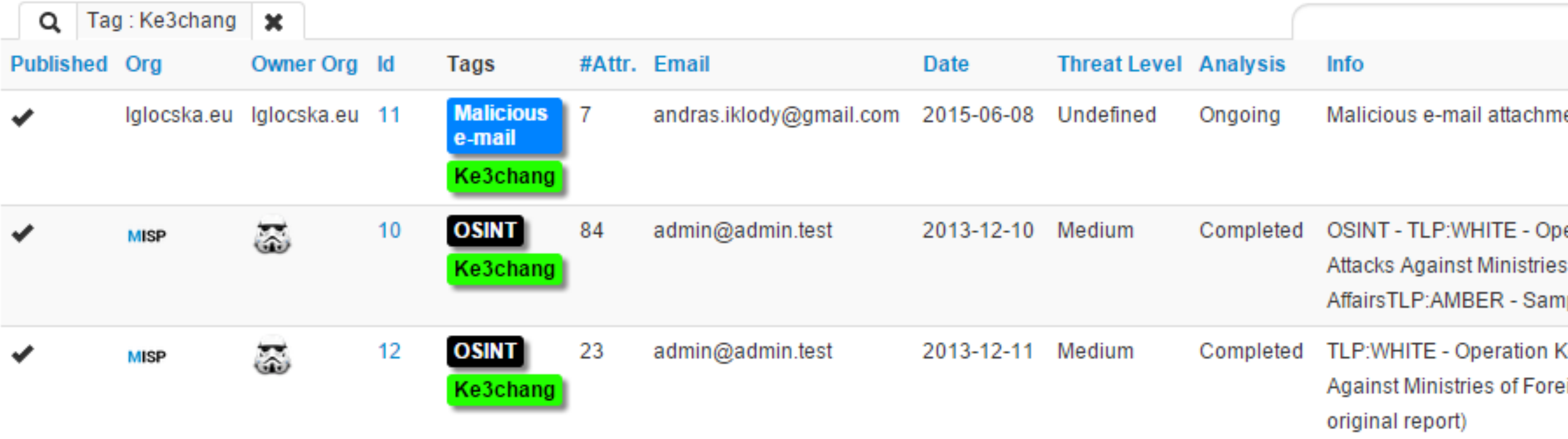


Tagging

- 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

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:

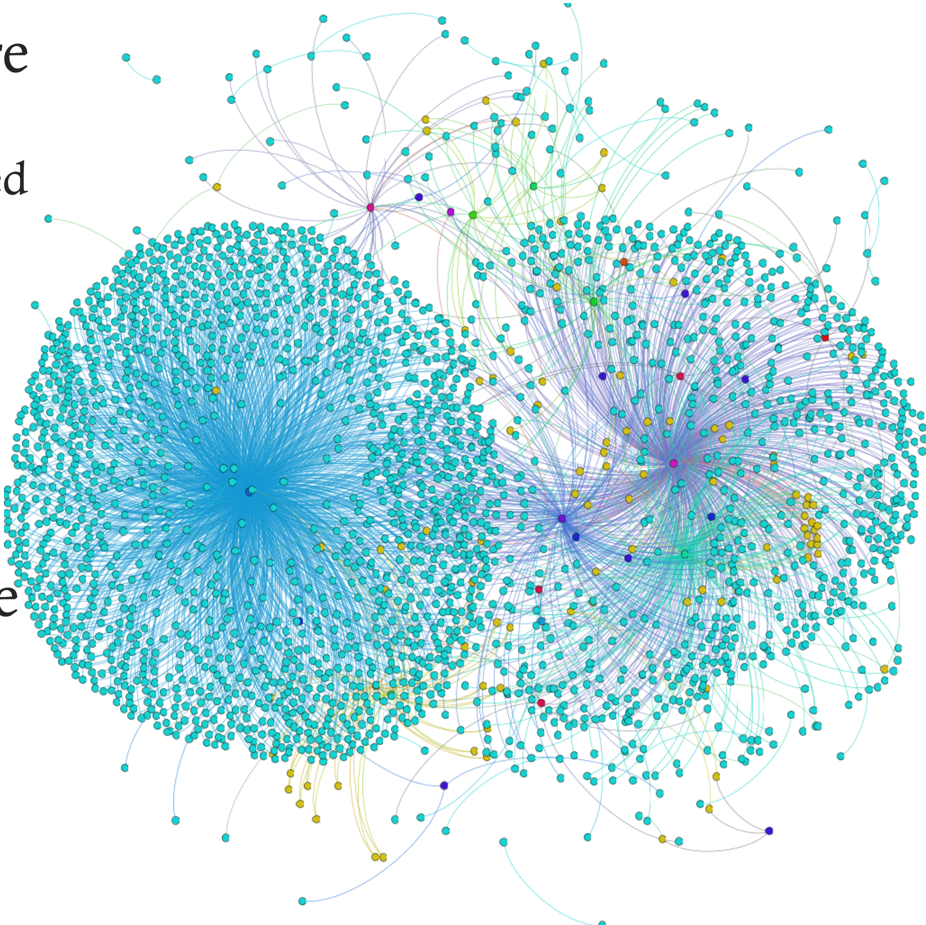


Tag : Ke3chang ✖

Published	Org	Owner Org	Id	Tags	#Attr.	Email	Date	Threat Level	Analysis	Info
✓	Iglocska.eu	Iglocska.eu	11	Malicious e-mail Ke3chang	7	andras.iklody@gmail.com	2015-06-08	Undefined	Ongoing	Malicious e-mail attachme
✓	MISP		10	OSINT Ke3chang	84	admin@admin.test	2013-12-10	Medium	Completed	OSINT - TLP:WHITE - Ope Attacks Against Ministries AffairsTLP:AMBER - Sam
✓	MISP		12	OSINT Ke3chang	23	admin@admin.test	2013-12-11	Medium	Completed	TLP:WHITE - Operation K Against Ministries of Forei original report)

Visualization

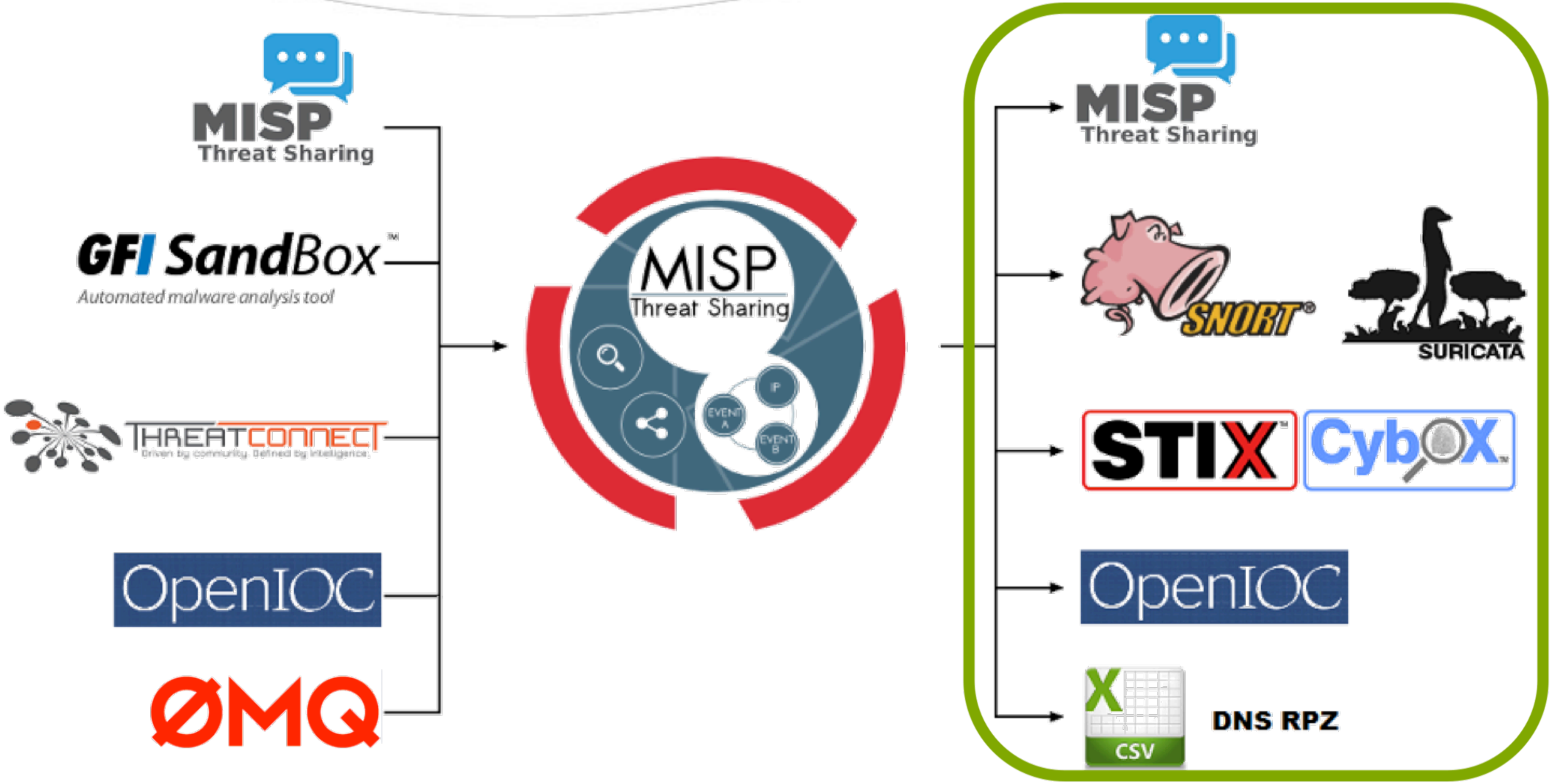
- Pivoting graph as shown before
- Using Maltego plugin (developed by Andrzej Dereszowski)
- Using MISP-Graph (tool developed by Alexandre Dulaunoy from CIRCL)
- Upcoming graphing tool in the MISP UI



Feeding your defenses

- Export formats of MISP
- Feed systems using MISP
- A flexible API
- Build and use tools that use the MISP APIs

Exporting options

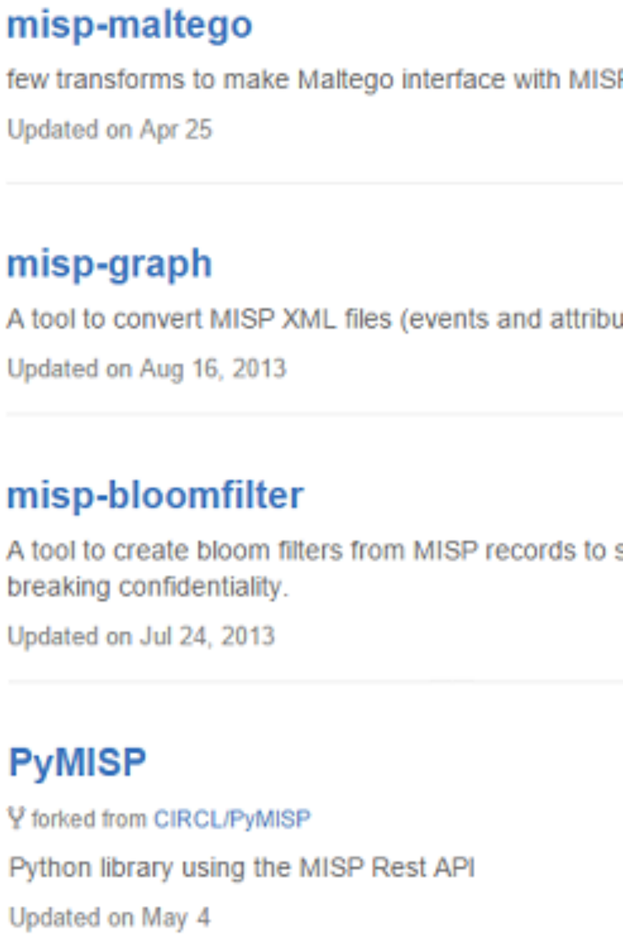


Export formats

- NIDS (Suricata, Snort, STIX/CyBox)
- HIDS (OpenIOC, STIX/CyBox, CSV)
- SIEMs
- DNS level firewalls (DNS Response Policy Zones)
- Forensic scanners
- Throw values obtained from CSV exports against your logfiles, pcaps, …
- …

API

- 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

few transforms to make Maltego interface with MISP

Updated on Apr 25

misp-graph

A tool to convert MISP XML files (events and attribu

Updated on Aug 16, 2013

misp-bloomfilter

A tool to create bloom filters from MISP records to s
breaking confidentiality.

Updated on Jul 24, 2013

PyMISP

forked from CIRCL/PyMISP

Python library using the MISP Rest API

Updated on May 4

FAQ

Why adopt MISP?

- Create, ingest and share IOCs
- Building defenses form others work
- MISP is constantly evolving
- Is already widely adopted
- It is commercially supported
- Is open-source , free and developed by a non-profit

Do you provide threat intelligence data feeds?

- **NO**
- The MISP Project takes care of software development
- We plan a public MISP with only OSINT data

Where can I find support?

- Website: http://misp-project.org
- Community Support
  - Users mailing list: https://groups.google.com/forum/#!forum/misp-users
  - Developers mailing list: https://groups.google.com/forum/#!forum/misp-devel
  - Documentation: User & Install guide
  - Source code: https://github.com/MISP
  - Issue tracking: https://github.com/MISP/MISP/issues
- Commercial Support
  - See website and ask your own vendor

Next big step !

- Bring people together
- Coordinate contributions
- Roadmap based on needs from all the users
- Guarantee long term survival

QUESTIONS?

http://misp-project.org

Contact / participate/ sponsor: info@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

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