MISP

Malware Information Sharing Platform

Picture by Sybren A. Stüvel

Situation 1

- We detect targeted malware
- Maybe directed towards other institutions
- Let’s share it with them
- How? What?

Situation 2

- Question: Can you help us analyze?
- Sure, send us the malware
- Analysis = IOCs to recognize it
  - Checksum, Registry key, Domain name, IP address, ….
- Search in our own network / logs
- ! We are also infected !

don’t share with people?

TOP SECRET

Secrecy

- No secure medium
- (over) Classified information
- No trust

Takes too much time

- Whom should I contact?
- How should I inform them?
- How do I share?

Picture by Dave Pearson

Solutions
NEXT EXIT ↗

Malware Information Sharing Platform

- Sharing with humans
  - Internally / Colleagues / Constituents
  - Partners and trust-groups
- Sharing with machines
- Collaborative analysis and correlation

Sharing with Humans

- Data you store is immediately available to your **colleagues** and **partners** via an **easy to use** webinterface
- Store the event id in your ticketing system or be
- informed by the **signed and encrypted email** notifications.

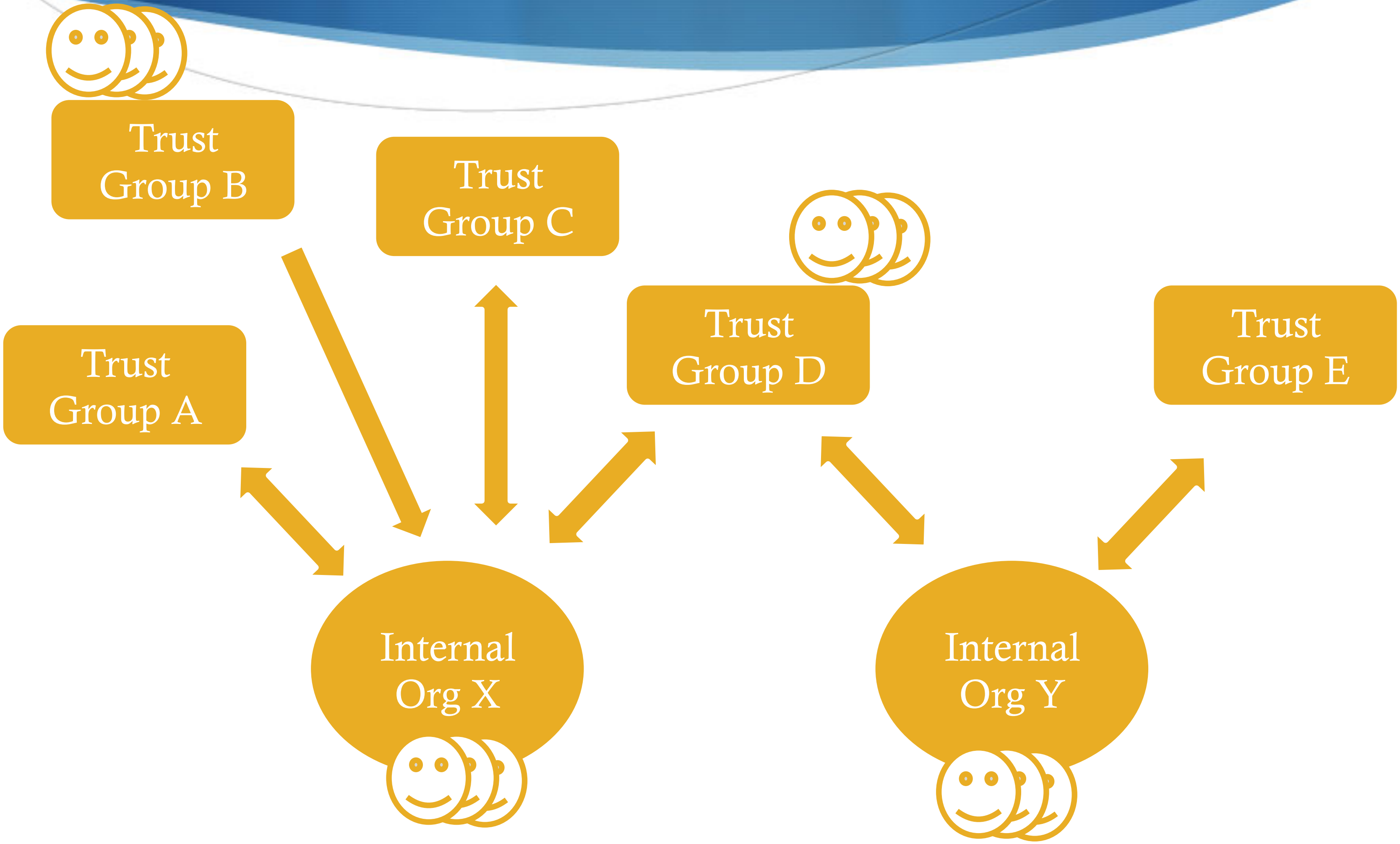
Sharing with Machines

- Generating **Snort/Suricata IDS** rules, **STIX**, **OpenIOC**, **text** or **csv** exports MISP allows you to automatically import data in your detection systems resulting in better and faster detection of intrusions.

- Importing data can also be done in various ways: **free-text** import, **OpenIOC**, **batch import**, or using the **preconfigured or custom templates**.

- If you run MISP internally, data can also be **uploaded and downloaded automagically from and to externally hosted MISP** instances.

MISP – MISP communication

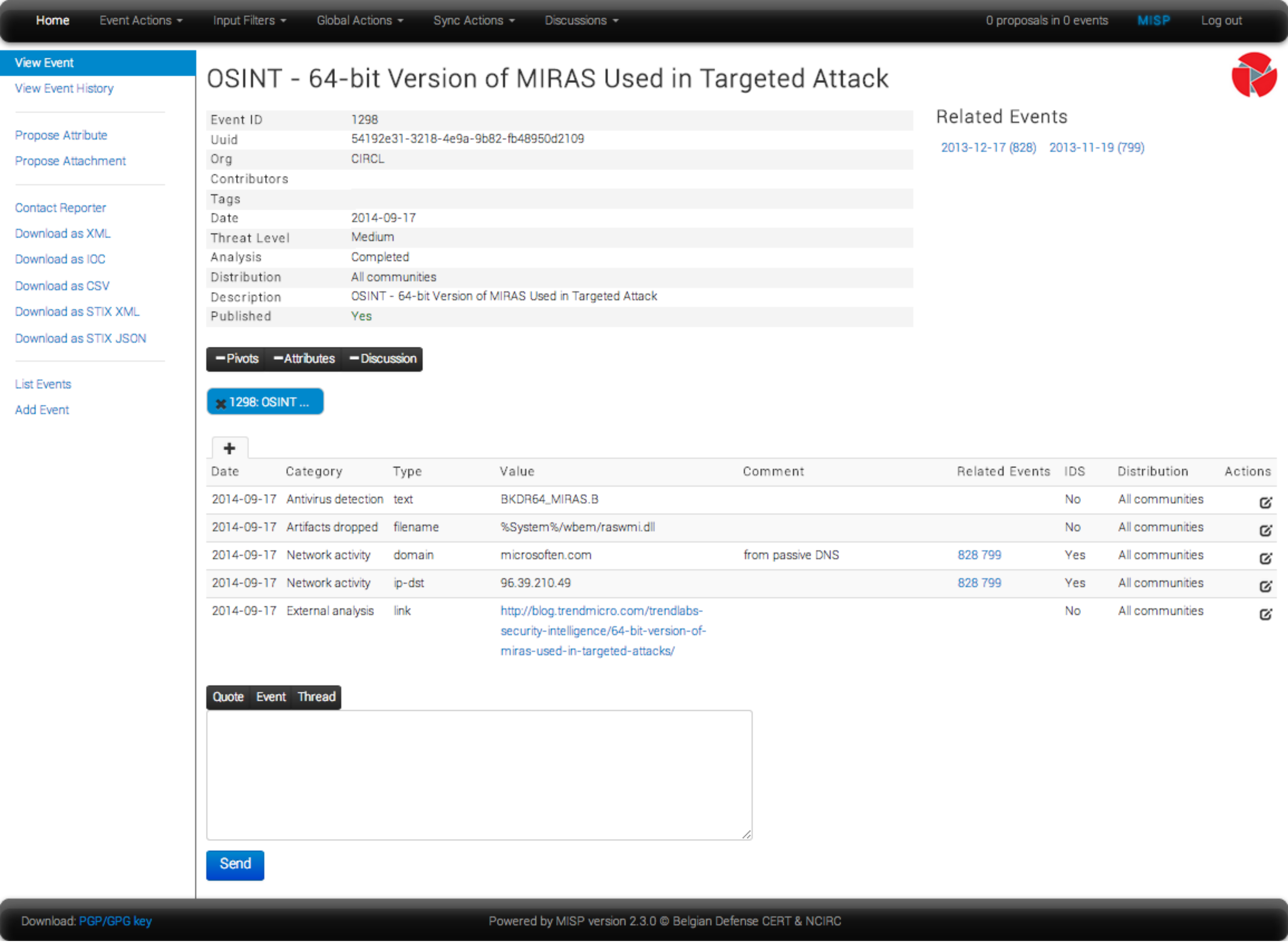

Trust Group B
Trust Group C
Trust Group D
Trust Group E
Trust Group A
Internal Org X
Internal Org Y

Collaborative analysis and correlation

- How often has your team analyzed to realize at the end that a **colleague had already worked** on another, **similar, sample**? Or that an external report has already been made?

- When new data is added MISP will immediately **show relations** with other **observables and indicators**. This results in more efficient analysis, but also allows you to have a better picture of the TTPs, related campaigns and attribution.

- The **discussion feature** will also enable conversations between multiple analysts.



OSINT - 64-bit Version of MIRAS Used in Targeted Attack

Event ID	1298
Uuid	54192e31-3218-4e9a-9b82-fb48950d2109
Org	CIRCL
Contributors	
Tags	
Date	2014-09-17
Threat Level	Medium
Analysis	Completed
Distribution	All communities
Description	OSINT - 64-bit Version of MIRAS Used in Targeted Attack
Published	Yes

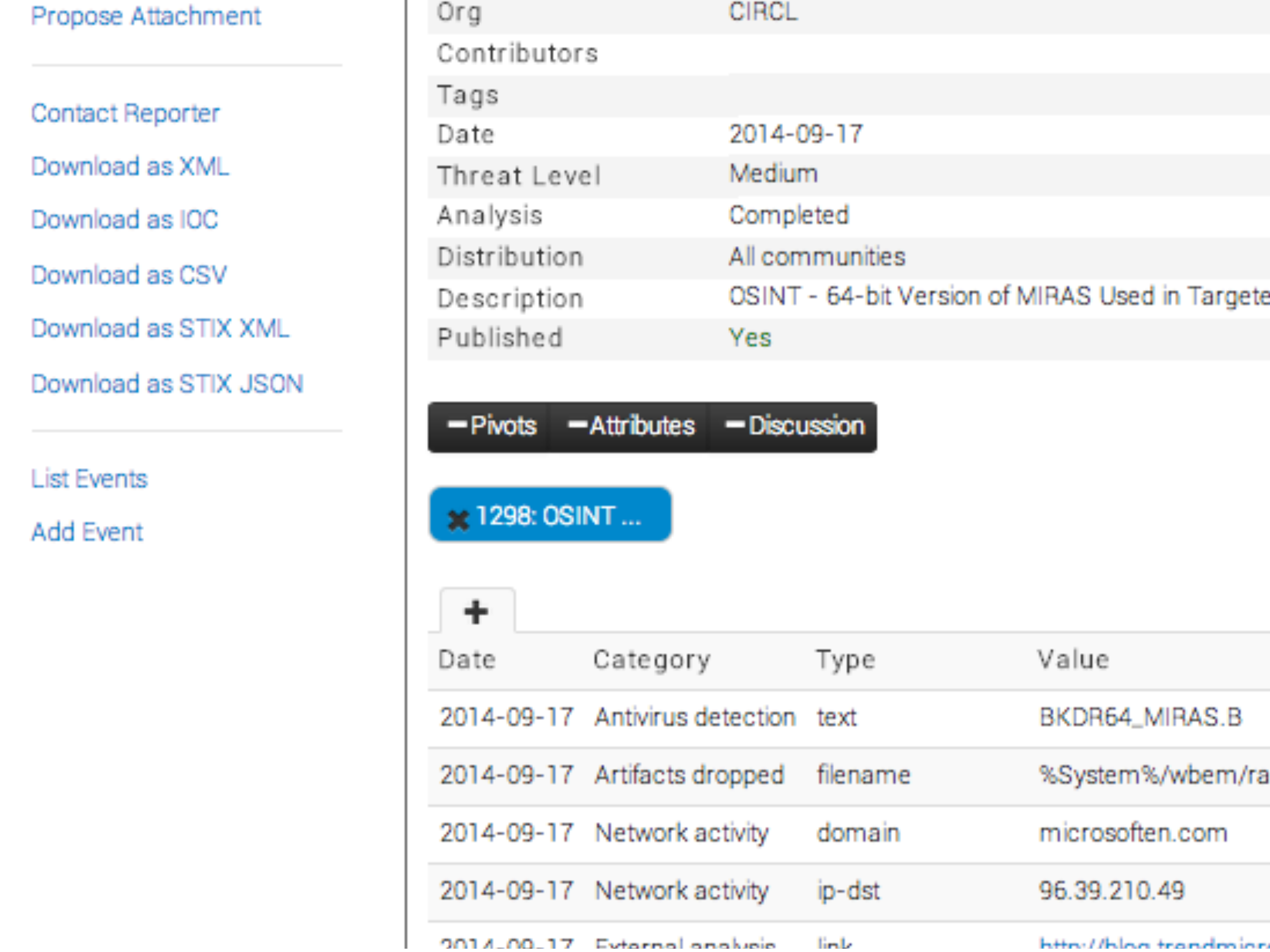
Related Events

2013-12-17 (828) 2013-11-19 (799)

Date	Category	Type	Value	Comment	Related Events	IDS	Distribution	Actions
2014-09-17	Antivirus detection	text	BKDR64_MIRAS.B			No	All communities	
2014-09-17	Artifacts dropped	filename	%System%/wbem/raswmi.dll			No	All communities	
2014-09-17	Network activity	domain	microsoften.com	from passive DNS	828 799	Yes	All communities	
2014-09-17	Network activity	ip-dst	96.39.210.49		828 799	Yes	All communities	
2014-09-17	External analysis	link	http://blog.trendmicro.com/trendlabs-security-intelligence/64-bit-version-of-miras-used-in-targeted-attacks/			No	All communities	

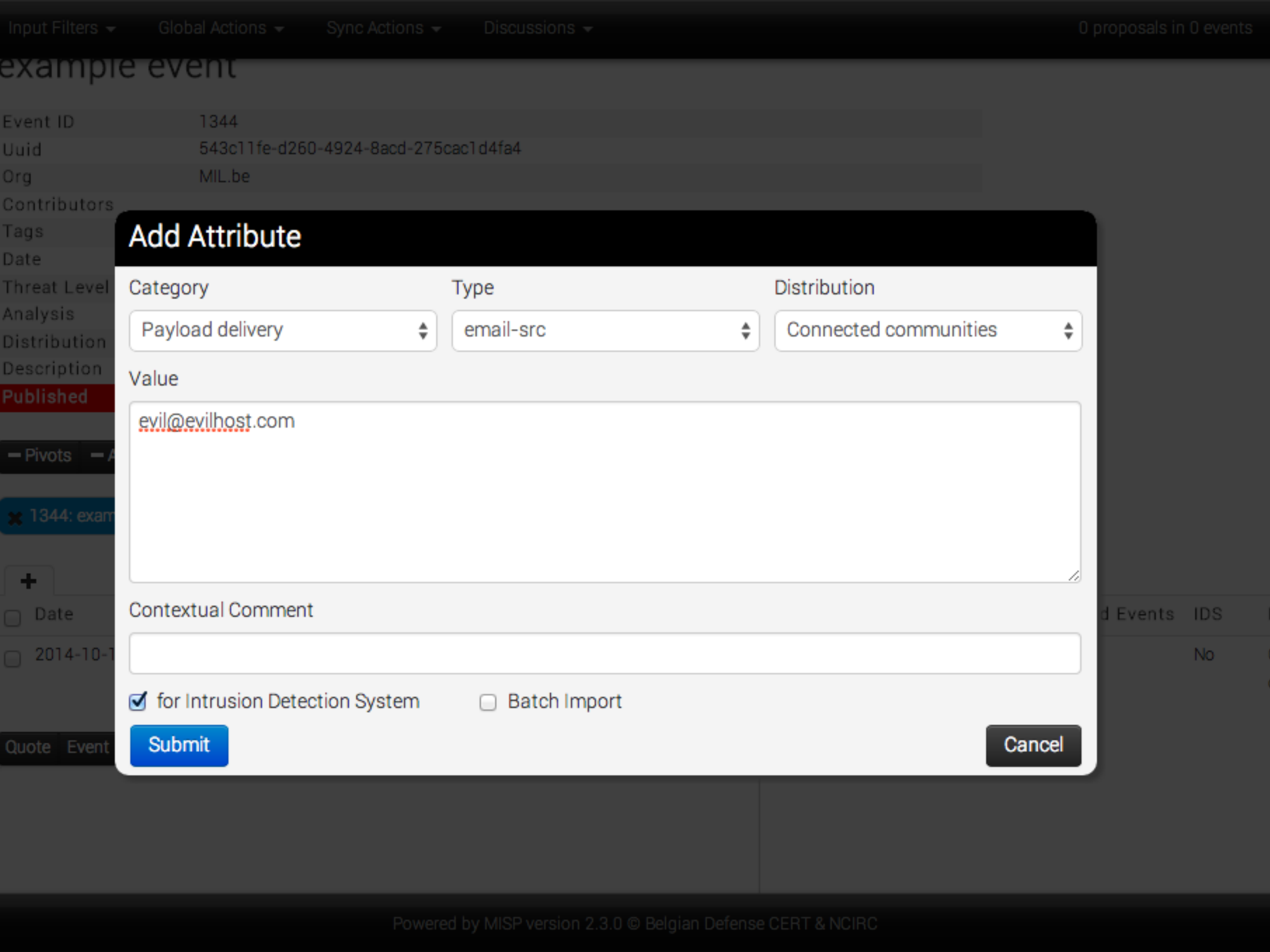
Download: PGP/GPG key

Powered by MISP version 2.3.0 © Belgian Defense CERT & NCIRC



Org	CIRCL
Contributors	
Tags	
Date	2014-09-17
Threat Level	Medium
Analysis	Completed
Distribution	All communities
Description	OSINT - 64-bit Version of MIRAS Used in Targete
Published	Yes

Date	Category	Type	Value
2014-09-17	Antivirus detection	text	BKDR64_MIRAS.B
2014-09-17	Artifacts dropped	filename	%System%/wbem/ra
2014-09-17	Network activity	domain	microsoften.com
2014-09-17	Network activity	ip-dst	96.39.210.49
2014-09-17	External analysis	link	http://blog.trendmicr



example event

Event ID	1344
Uuid	543c11fe-d260-4924-8acd-275cac1d4fa4
Org	MIL.be
Contributors	
Tags	
Date	
Threat Level	
Analysis	
Distribution	
Description	
Published	

Add Attribute

Category: Payload delivery

Type: email-src

Distribution: Connected communities

Value: evil@evilhost.com

Contextual Comment:

☑ for Intrusion Detection System ☐ Batch Import

☐ Date	d Events	IDS
☐ 2014-10-1		No

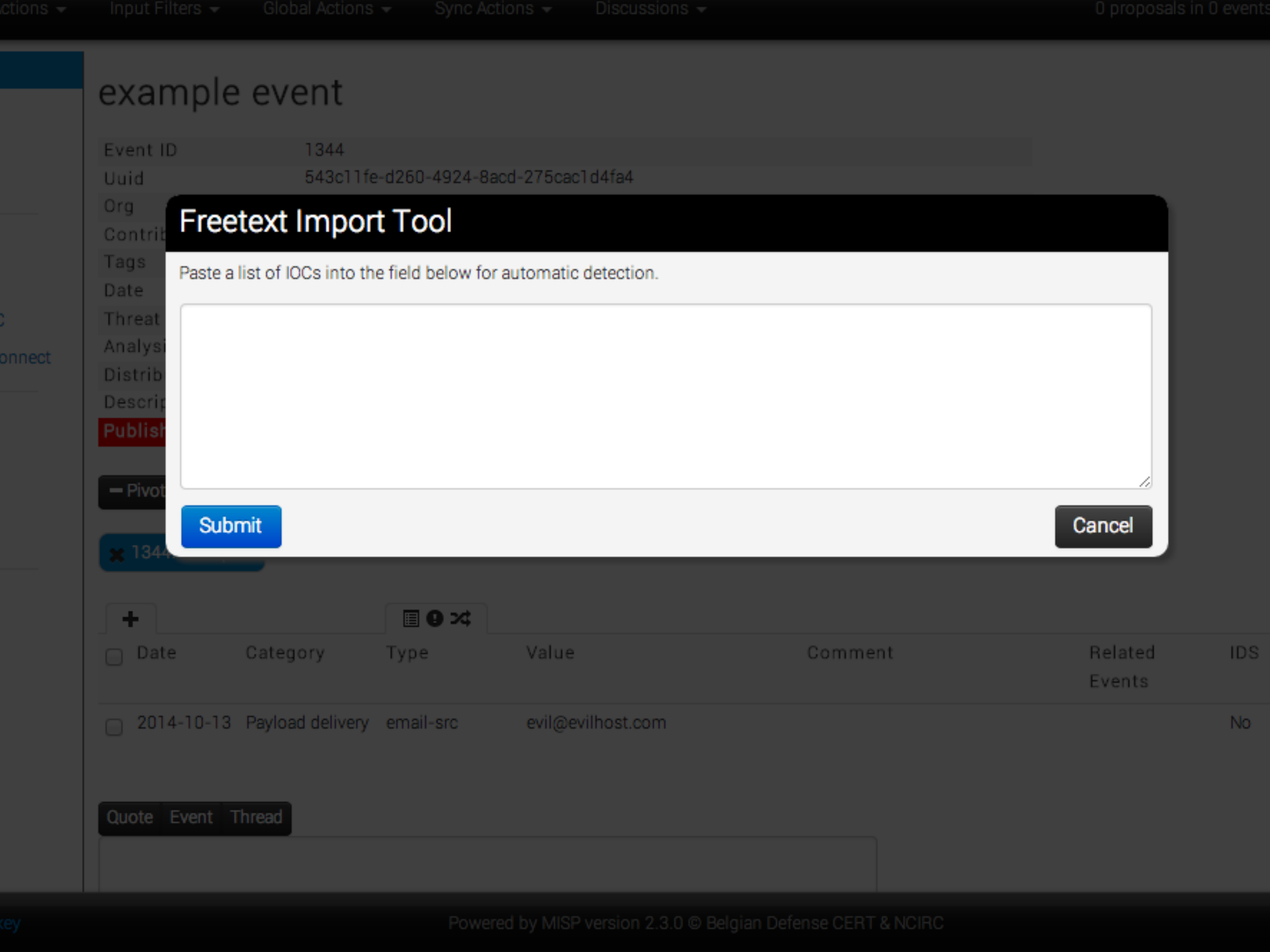
Powered by MISP version 2.3.0 © Belgian Defense CERT & NCIRC

Categories

1. Payload delivery
2. Artifacts dropped
3. Payload installation
4. Persistence mechanism
5. Network activity
6. Payload type
7. Attribution
8. …

Types

- md5, sha1, filename, ip-src, ip-dst
- hostname, domain
- email-src, email-dst, email-subject, email-attachment, url
- user-agent
- regkey|value
- snort-rule
- pattern-in-file, pattern-in-traffic, pattern-in-memory
- Yara,
- …



example event

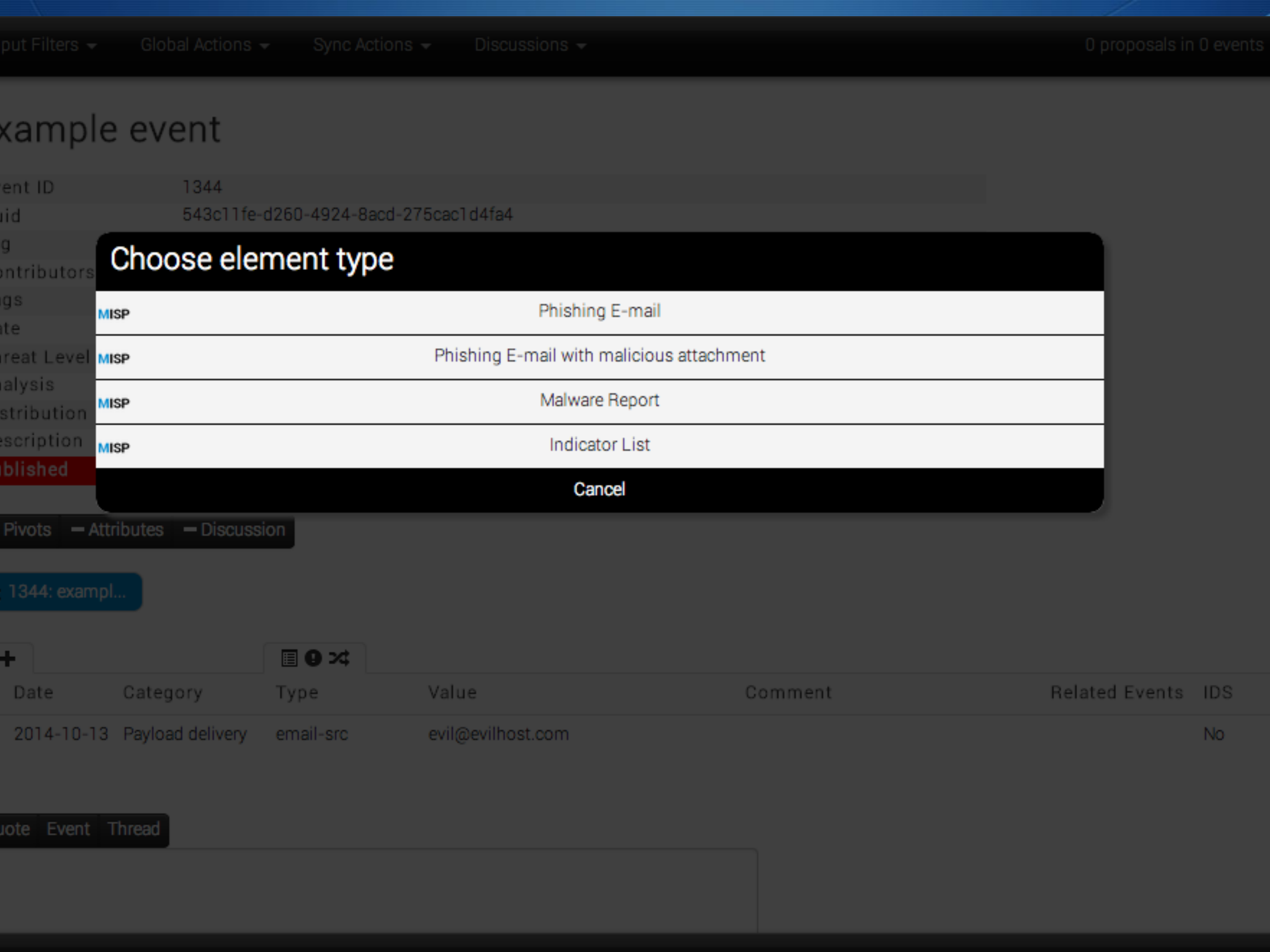
Event ID	1344
Uuid	543c11fe-d260-4924-8acd-275cac1d4fa4
Org	
Contrib	
Tags	
Date	
Threat	
Analysi	
Distrib	
Descrip	
Publish	

Freetext Import Tool

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

	Date	Category	Type	Value	Comment	Related Events	IDS
□	2014-10-13	Payload delivery	email-src	evil@evilhost.com			No

Powered by MISP version 2.3.0 © Belgian Defense CERT & NCIRC



xample event

ent ID	1344
iid	543c11fe-d260-4924-8acd-275cac1d4fa4
g	
ntributors	
gs	
te	
reat Level	
alysis	
stribution	
scription	
blished	

Choose element type

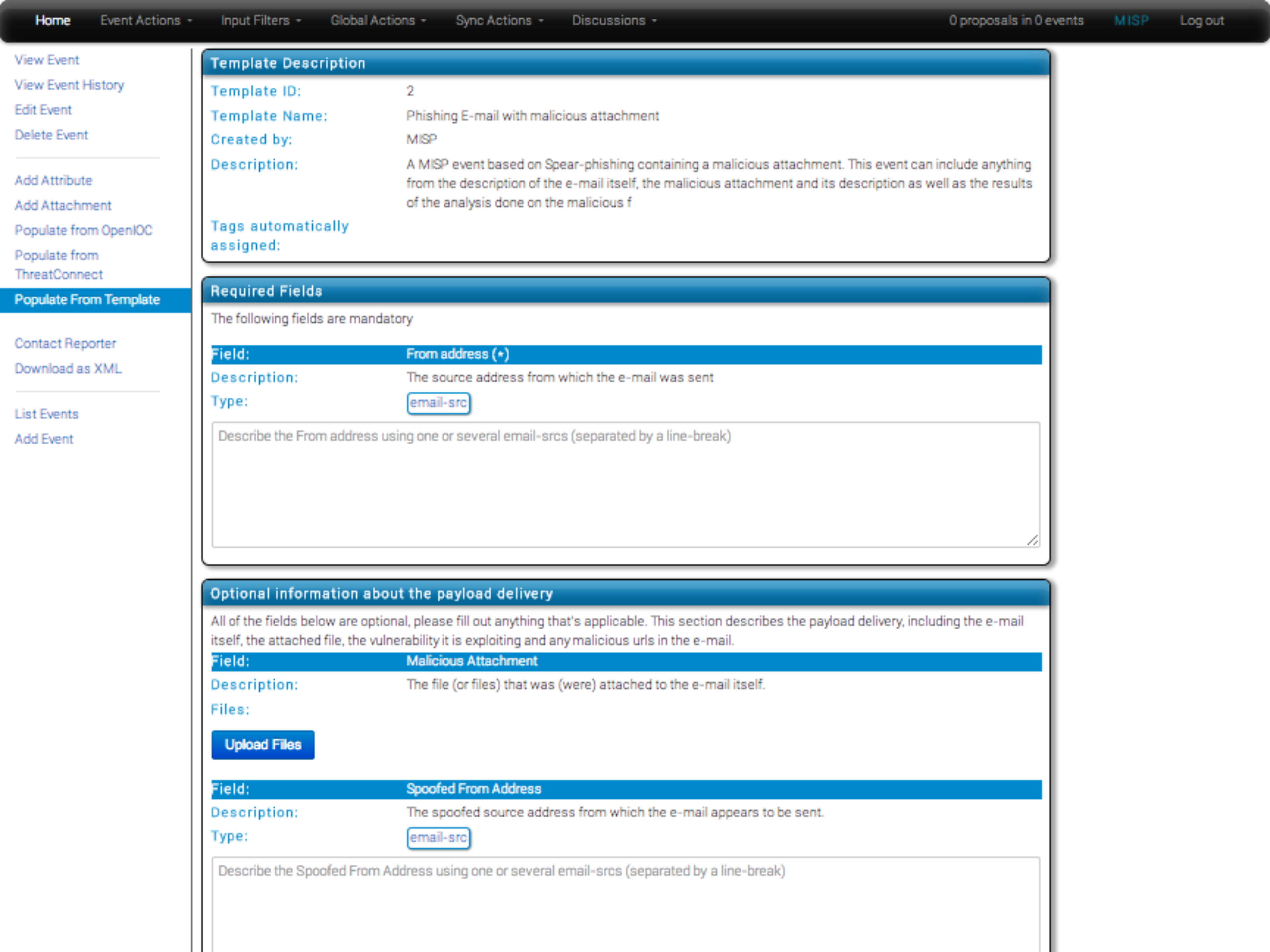
MISP Phishing E-mail

MISP Phishing E-mail with malicious attachment

MISP Malware Report

MISP Indicator List

Date	Category	Type	Value	Comment	Related Events	IDS
2014-10-13	Payload delivery	email-src	evil@evilhost.com			No



Template Description

Template ID:	2
Template Name:	Phishing E-mail with malicious attachment
Created by:	MISP
Description:	A MISP event based on Spear-phishing containing a malicious attachment. This event can include anything from the description of the e-mail itself, the malicious attachment and its description as well as the results of the analysis done on the malicious f
Tags automatically assigned:	

Required Fields

The following fields are mandatory

Field:	From address (*)
Description:	The source address from which the e-mail was sent
Type:	email-src

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

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)

Roadmap

- **v2.4**
  - Sharing groups or 'Releasable to' model
  - Modular import / export with plugins
- **v3.0+**
  - New data model allowing composite objects (ex: file described by hashes, filenames, ...)
  - Import of STIX data and better support for OpenIOC
  - Support Cyber Threat Intelligence structures such as Campaigns, Threat Actors, TTPs,...
  - Further integration with other tools: Import/Export from/to sandboxes, external feeds, ...
  - Enrichment by gathering additional information on the data you're entering.

Contributors

Contributed by

- Belgian Defense
- NATO NCIRC
- CERT-EU
- CIRCL
- Community !!!

NCIRC
NATO
COMPUTER INCIDENT
RESPONSE CAPABILITY

computer
emergency
response
team
CERT-EU
for the EU institutions, bodies
and agencies

CIRCL
Computer Incident
Response Center
Luxembourg

Next big step !

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

http://misp-project.org

Thank you for giving us your feedback and helping MISP rule the world.