Introduction to MISP

Sam Perl,

CSIRT Development and Training Team,

CERT, SEI, Carnegie Mellon University

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

DM21-0775

Introduction

Cybersecurity Incident Response teams want to

- Have a way to receive (trusted) data from other teams
- Ideally reduce duplication during analysis
- Move toward automated solutions where possible and appropriate
- Restrict access to certain data according to policy/practices

Information Sharing

- Can help enable private and public IT-communities to share a wide range of information.
- Sharing indicators of compromise, artifacts, context, TTP, and more within a community can have direct impact on reaction capability.
- Can help with prevention, detection, and response

Information Sharing Platforms

A platform may perform a variety of security tasks to help defenders such as:

- Receive data about threats from other network participants or publicly available data sources
- Help analysts perform correlation analysis between events such as ‘linking’ them together
- Allow analysts to add metadata to values such as URLs, Domain names, Filenames, Hash values, and much more
- Integrate with other services such as malware sandbox analysis and importing results (enrichment)
- Integrate with defensive tools including Firewalls, Intrusion Detection Systems (IDS), SIEM, or other programmable network/host event sensors such as Zeek (formerly Bro)

Sharing Platforms are only as valuable as the data they contain

- All of the platform use cases require the receipt of useful, timely, and ‘actionable’ security data.
- Data that is out of date or incorrect can cause unnecessary outages rather than prevent against attacks.
- Using incorrect and inaccurate cyber intelligence can lead to many other security failures.
- There are many teams that provide data for others to use (often called *Feeds*), but **careful** examination of each dataset is recommended.

Malware Information Sharing Platform
(now used for more than malware)

Key Features:

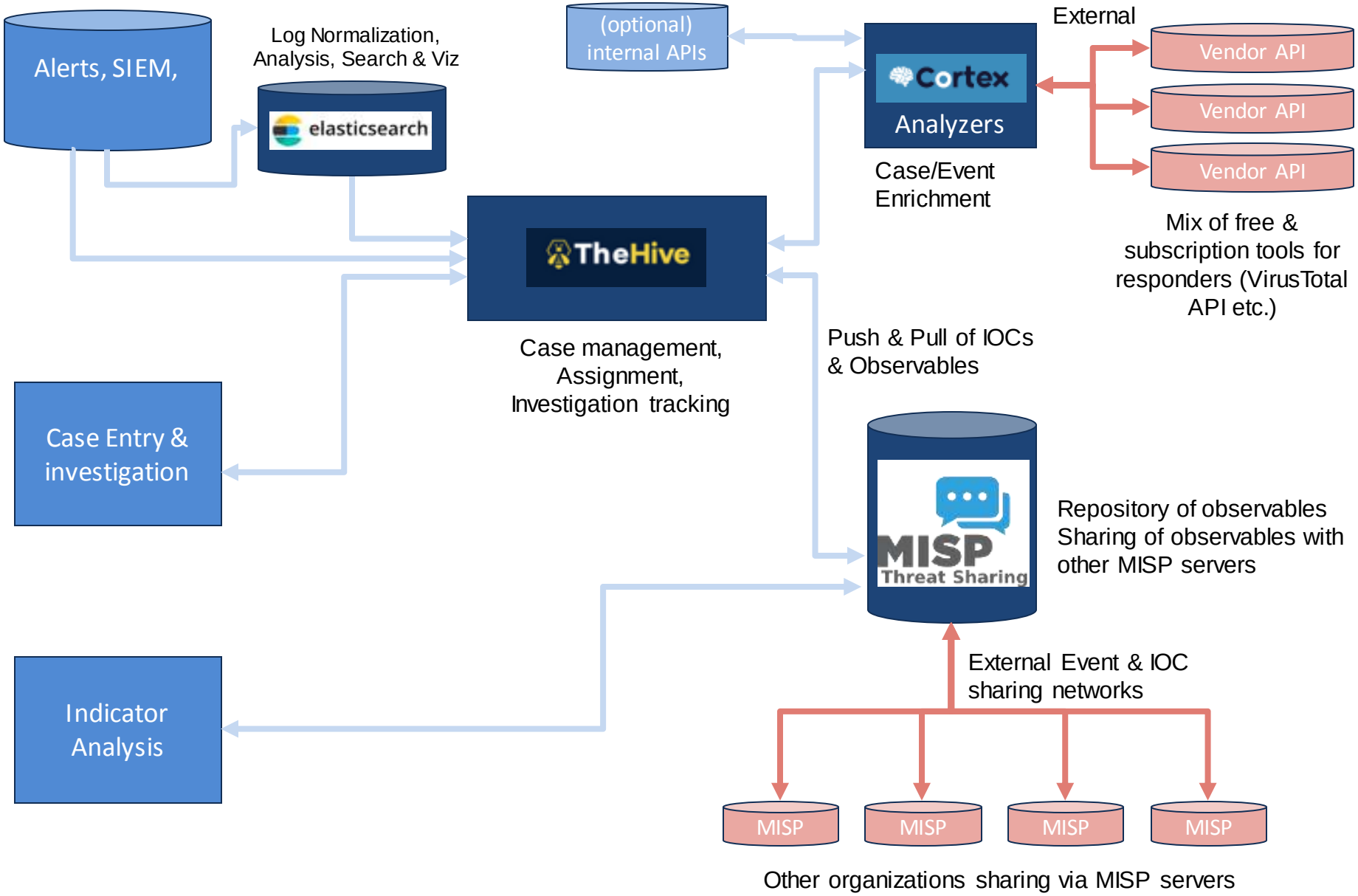
- Store, share, collaborate on cyber security indicators, malware analysis, and use to detect and prevent attacks or threats.
- Support for Events to have tags, to apply different taxonomies,
- Multi-layered Sharing groups for multiple organizations with permissions and protocols (including TLP)
- Import/Export events in various formats including indicator extraction via Regex
- Linking of attributes (observables and IOCs) between Events

Example Use

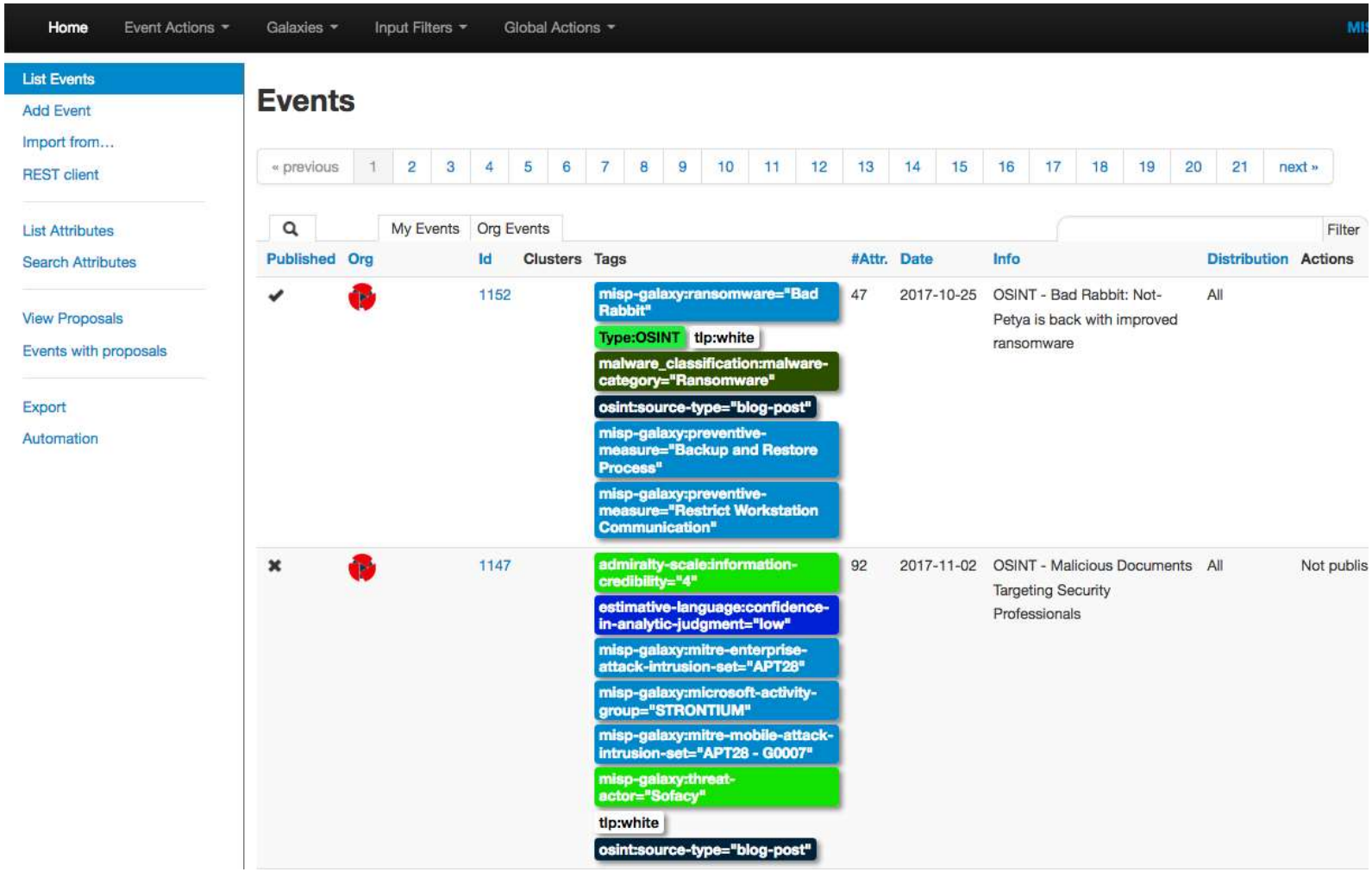
Typical Artifact and IOC flow

1. Receive an alert, Create and Work a case
2. Ideally, “Search” on various case details such as IOCs
3. Track Artifacts, ‘IOC’, analysis, and other relevant data
   - Perform correlation on different data types
   - ‘Link’ values to data types – such as Groups, Mitigations, Frameworks, other
   - Send data types for analysis (suspected malware) and incorporate results
4. Use data to respond, track, correlate and aggregate events, develop mitigations, signatures, etc.
5. Share certain results with others using rules
6. Store historical results – for future case analysis

Sample design plan for open-src tool integration and data flow

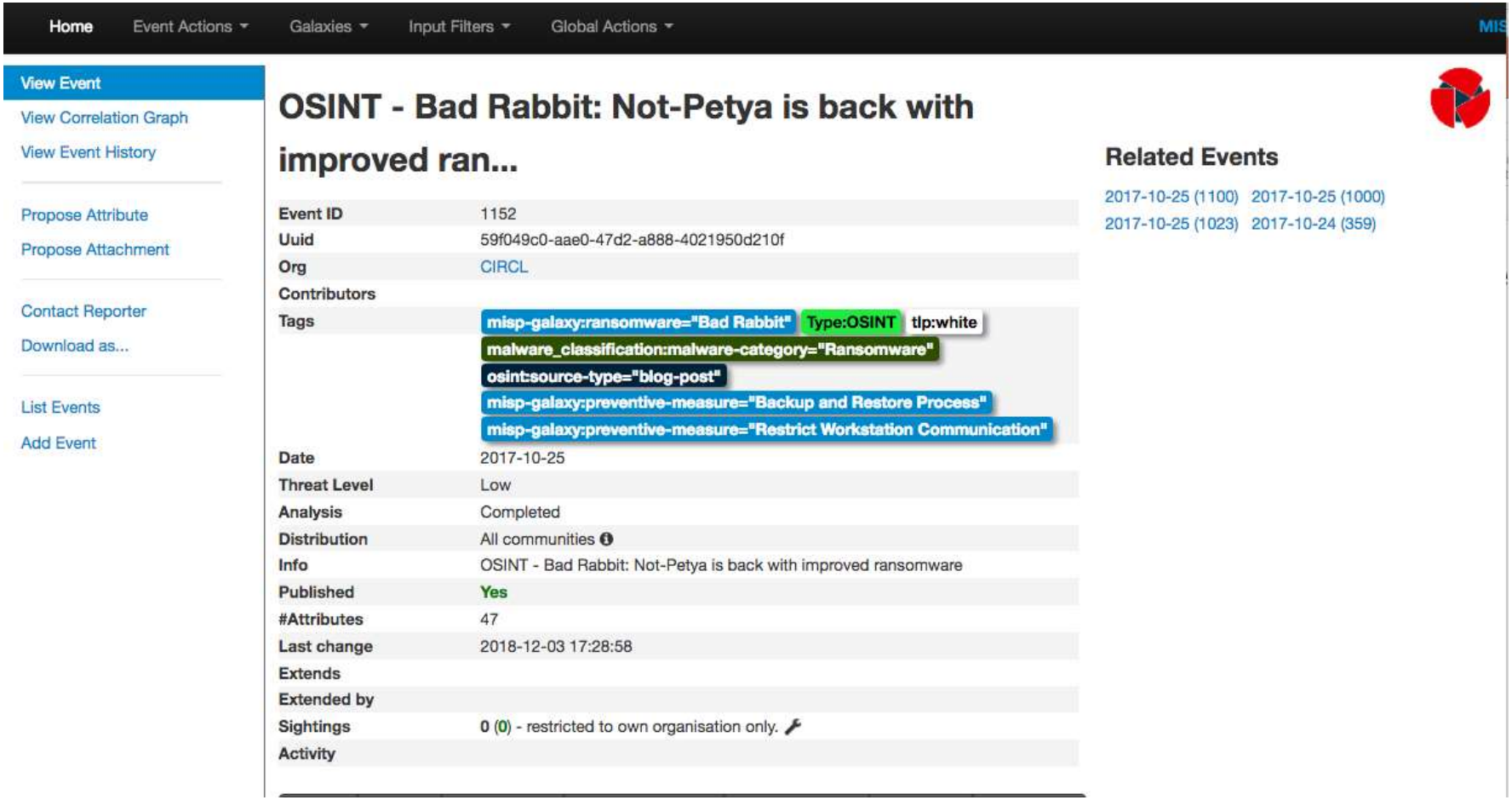


MISP – Event List



Events from the the CIRCL MISP dataset imported into a MISP server. tlp:white

MISP – Store an Event



Events have standard fields and include Tags. *Tags* are built using *Taxonomies*

Type of Information to Be Shared

Indicators of Compromise (IOCs) – Provide warnings that a network has been compromised, enabling the parties concerned to anticipate cyber breaches and take appropriate steps. Examples of IOCs

- Unusual network activity
- Login failures
- Unusual privileged account user activity
- Change in system configuration
- Logins from non-business locations facilitate detection and response of cybercrime
- Technical aspects of attacks; Tools exist which facilitate systemic discovery of new technical aspects of attacks

Types of Information to Be Shared

Tools, techniques and procedures (TTP)

- Awareness of cyber attacker and criminal behavior is imperative to the prevention and detection misson
- Knowing what cyber criminals do and how they do it, allows for deeper understanding and recognition of source threat, suspicious patterns, malware, infrastructure launch points, and more.
- Can help organizations to plan a stronger defense against attackers and/or cybercrime.

More Information Sharing Examples

- Affected host
- Location of System
- Malware
  - Known bad destination
  - Threat rating based on sensors
- Check for false positives
- Triage malware samples
- Use templates

- First correlation of events
- Adding business context
- Adding tags
- Upload samples to sandbox

- Malware reverse engineering
- Manual investigation
- IOCs
- Strategic advice
- Forensic artifacts

MISP – Attributes (IOCs) attached to the Event

Filters: All | File | Network | Financial | Proposal | Correlation | Warnings | Context | Relate

Date	Org	Category	Type	Value	Tags	Gala
2017-10-25		External analysis	link	https://www.welivesecurity.com/2017/10/24/bad-rabbit-not-petya-back/	osint:source-type="blog-post"	
2017-10-25		External analysis	comment	A new ransomware outbreak today and has hit some major infrastructure in Ukraine including Kiev metro.	osint:source-type="blog-post"	
2017-10-25		External analysis	link	https://www.virustotal.com /file/301b905eb98d8d6bb559c04bbda26628a942b2c4107c07a02e8f753b dcfe347c/analysis/1508918790/		
2017-10-25		External analysis	link	https://www.virustotal.com /file/2f8c54f9fa8e47596a3beff0031f85360e56840c77f71c6a573ace6f4641 2035/analysis/1508915760/		
2017-10-25		Network activity	url	http://www.pensionhotel.cz		
2017-10-25		Network activity	ip-dst	185.149.120.3		
2017-10-25		Network activity	url	http://osvitaportal.com.ua		
2017-10-25		Network activity	url	http://www.otbrana.com		

Attributes have different *Categories* and *Types*

Taxonomies as Tags

- Allows for a structured list of terms to select from such as:
  - Types of attacks, Specific Courses of Action COA, and much more
- Benefit: Terms can be used across organizations and teams
- Can define different types of data and types of values and can be aligned to other standards and frameworks – such as enumerations of adversary TTPs in publicly available reports
- MISP allows for both public and private taxonomies

Main Benefit

Complex data values can be semantically associated with custom lists. The lists can be set by an individual or a community.

Attempted descriptions at emerging threat behavior can be proposed and adopted and emerging data can be structured.

For example, one team built a taxonomy for Cryptocurrency threats based on CipherTrace reports to differentiate crypto related events from each other. Can be thought of as a "sub category"

- cryptocurrency-threat:Crypto Robbing Ransomware
- cryptocurrency-threat:Lightning Network Transactions (these are *off-chain* in a sense, so even harder to track)
- cryptocurrency-threat:SIM Swapping (usually specific to attacks on mobile based wallets)
- And more

MISP taxonomies - Flexible Classification for Information Sharing

MISP taxonomies is a solution to use existing taxonomies (or create your own) to **classify your cybersecurity events, indicators and threats**. This technique is integrated as a default mechanism for tagging in MISP (Malware Information Sharing Platform & Threat Sharing) and to support a distributed classification where organizations can share **common taxonomies in a local or distributed fashion**.

Classifications are distributed as simple JSON files to use with MISP but **can be easily integrated into any other information sharing software**. You can also propose new taxonomies to the community.

Examples of machine tags and human readable tags :

admiralty-scale:source-reliability="c"
admiralty-scale:Source Reliability="Fairly reliable"

admiralty-scale:information-credibility="3"
admiralty-scale:Information Credibility="Possibly true"

nato:classification="NU"
nato:Classification="NATO UNCLASSIFIED"

tlp:amber
Traffic Light Protocol:(TLP:AMBER) Information exclusively given to an organization; sharing limited within the organization to be effectively acted upon.

MISP Threat Sharing

https://github.com/MISP/misp-taxonomies/

(over 35 taxonomies)

And now Data Objects

Only available in newer versions (2.4.80 +)

Allow for template based combinations of attributes.

Groups different kind of attributes (taxonomies) together using specific templates

Among other things, used to support sharing/import in **DHS CISA AIS** format **(sector list, source markings, etc.)**

Integration with Data Services (MISP Modules)

- Can be used for data enrichment (expansion, import and export)
- Check information against outside databases in the background (expansion) and display via hover over as needed by analysts.
- Written in Python

Examples

- Hover over a CVE to display more information
- Submit files (artifact attachments) or URLs and receive a report that is imported and converted to MISP attributes such as hostname, domain, ip-src, ip-dst, various hash functions
- Also modules to export or import various formats

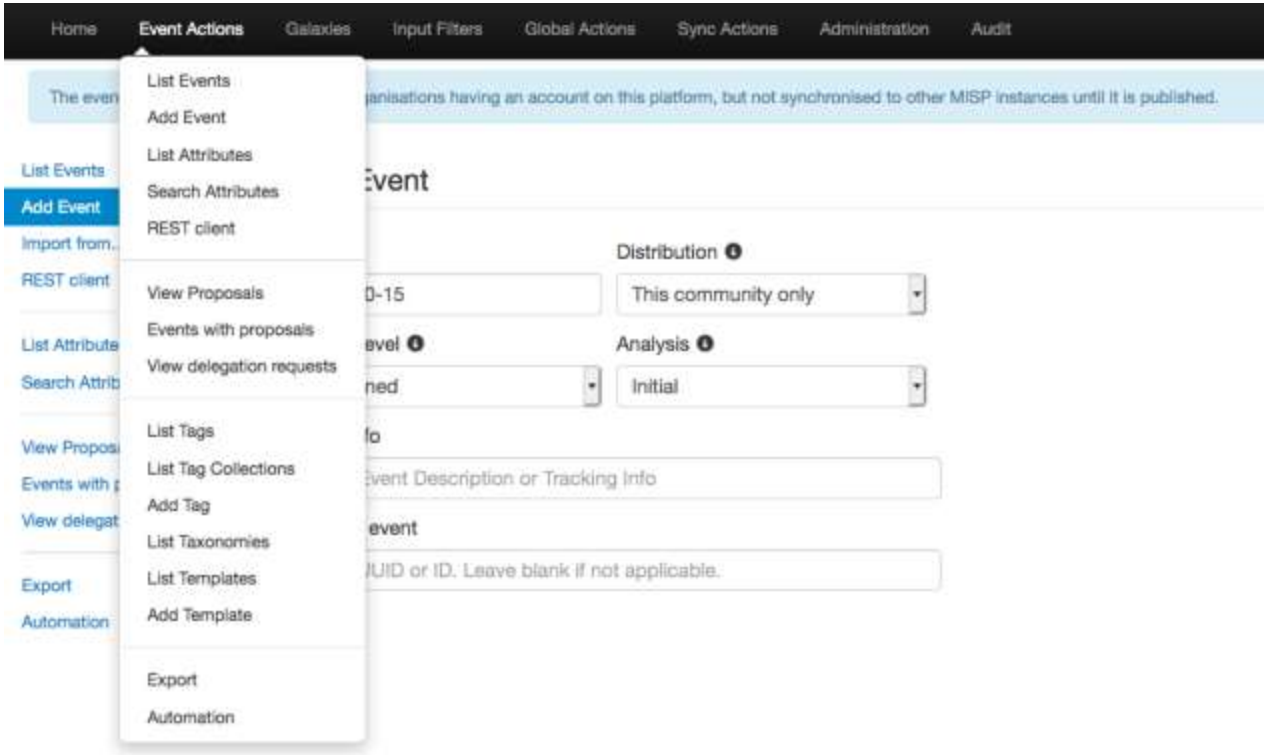
Sharing Communities & Data

Known Existing and Public MISP Communities

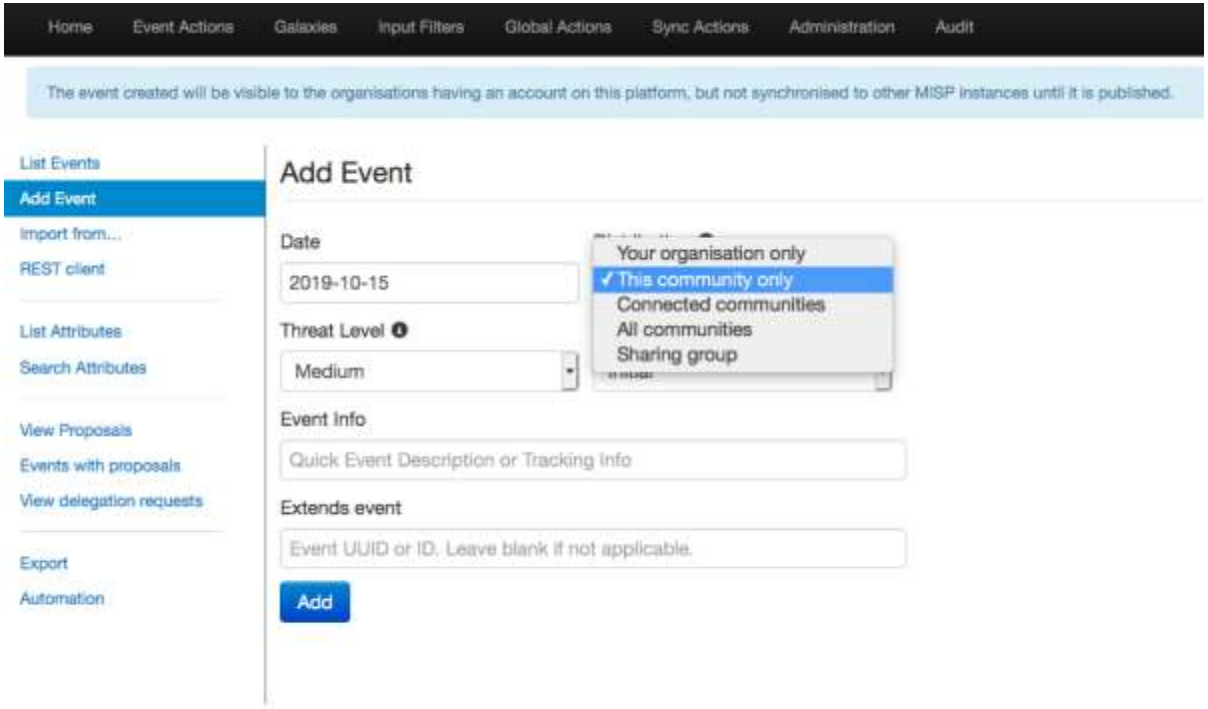
- **CIRCL MISP Community**
- CiviCERT MISP Community
- Fidelis malware/RAT Community
- CSSA Cyber Security Sharing & Analytics (CSSA)
- **FIRST MISP Community**
- NATO MISP Community
- MISP Feed Communities
- CIRCL OSINT Feed
- Botvrij.eu OSINT feed

Event Walkthrough

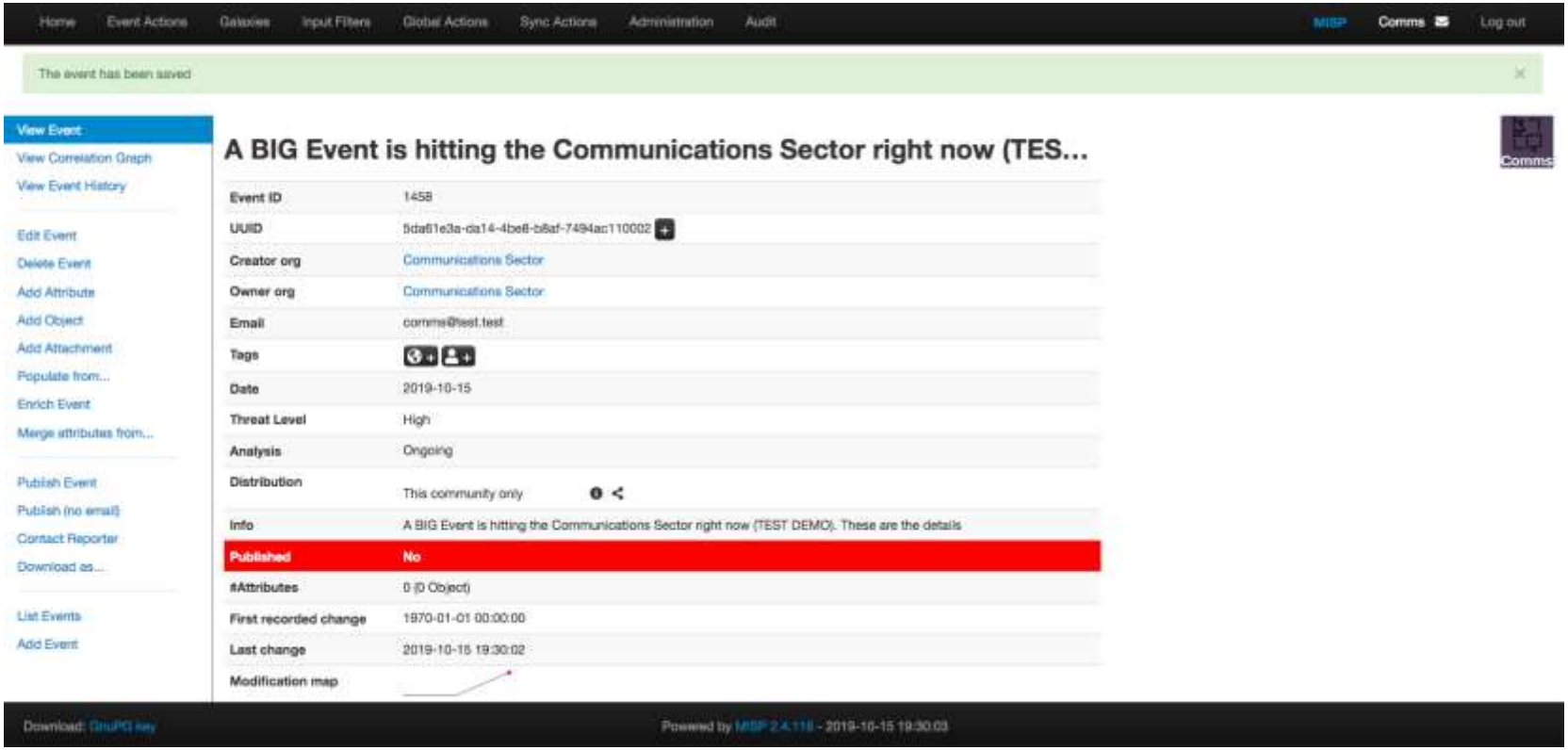
Adding Events - Menu



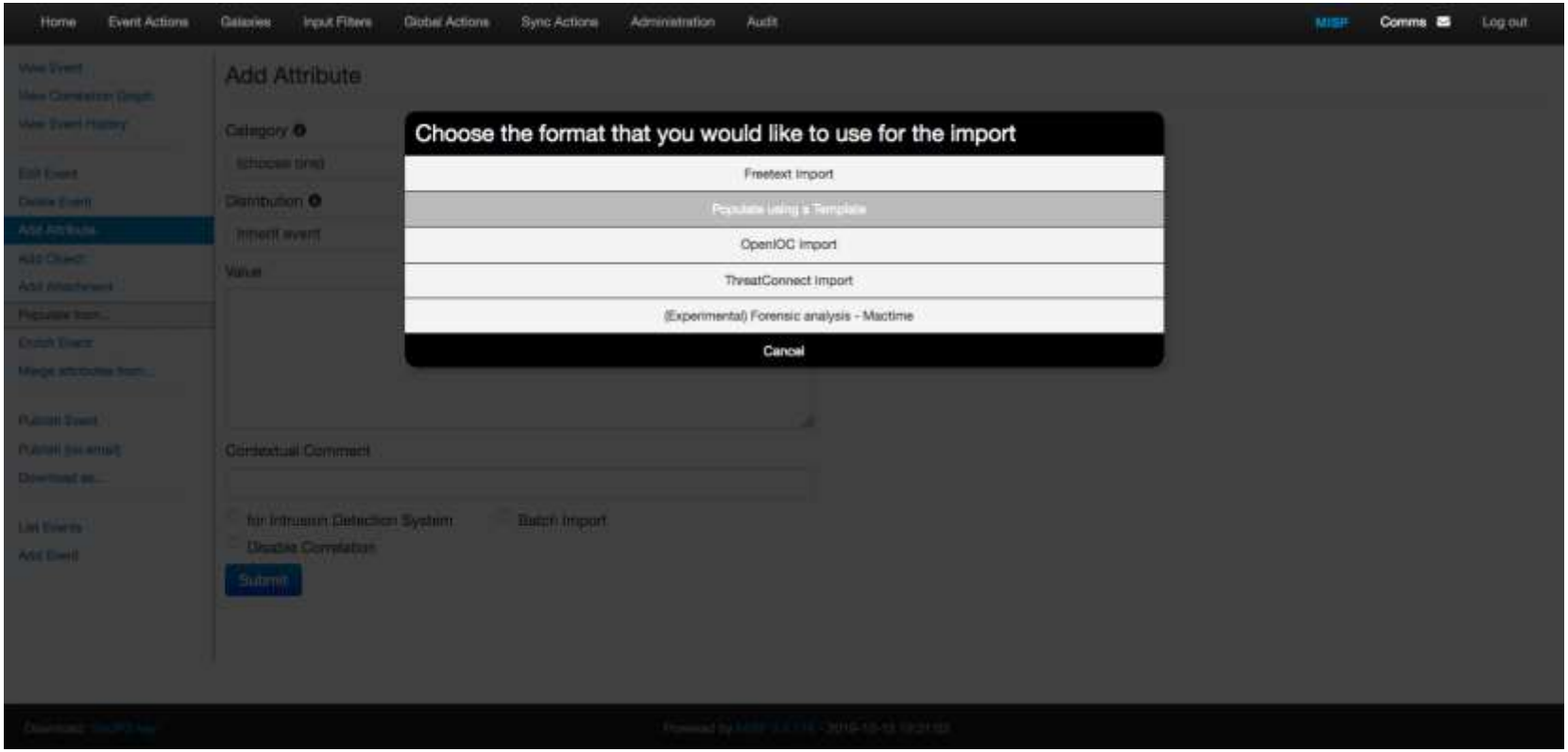
Set Distribution of Event



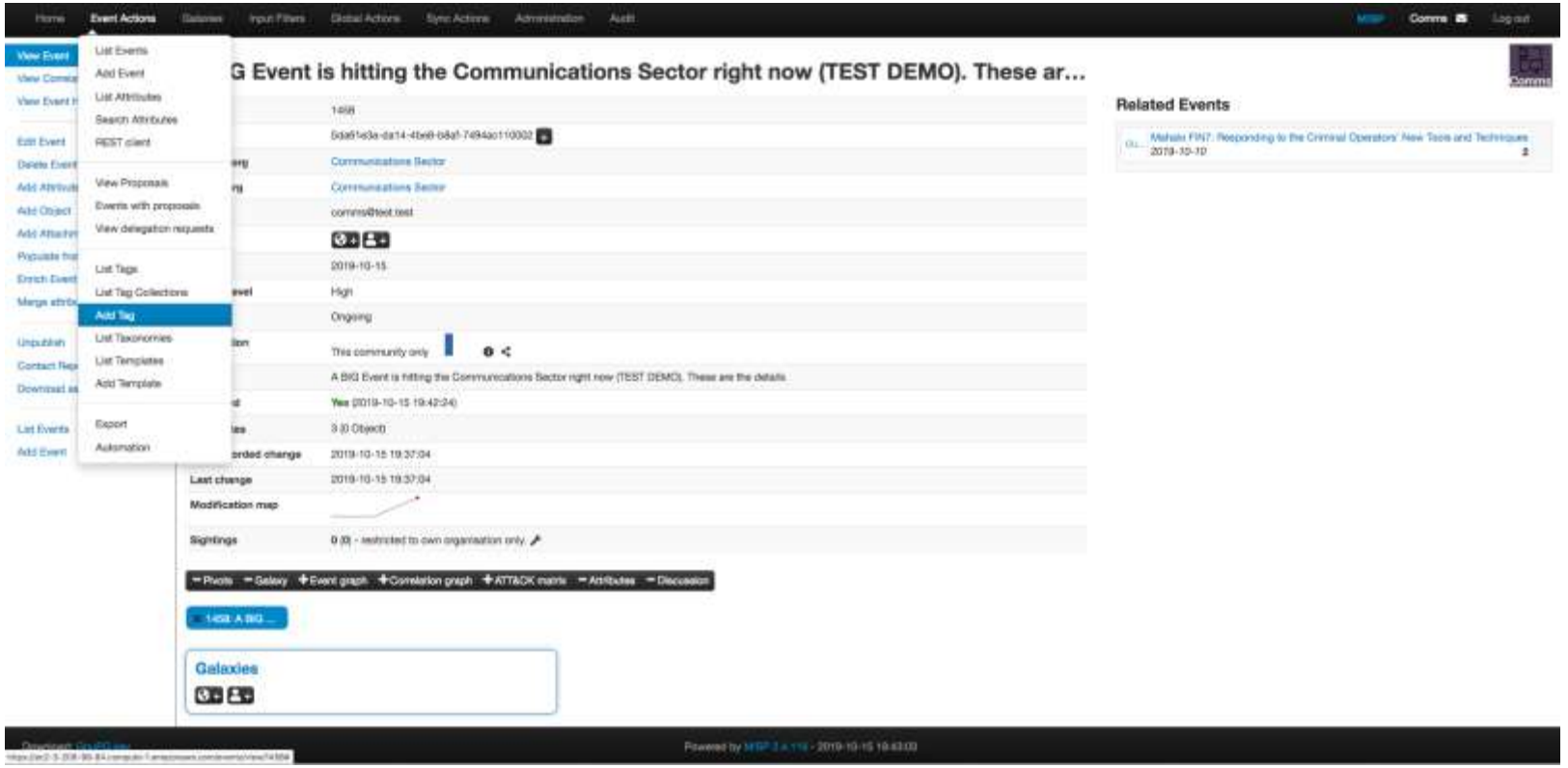
Add Event



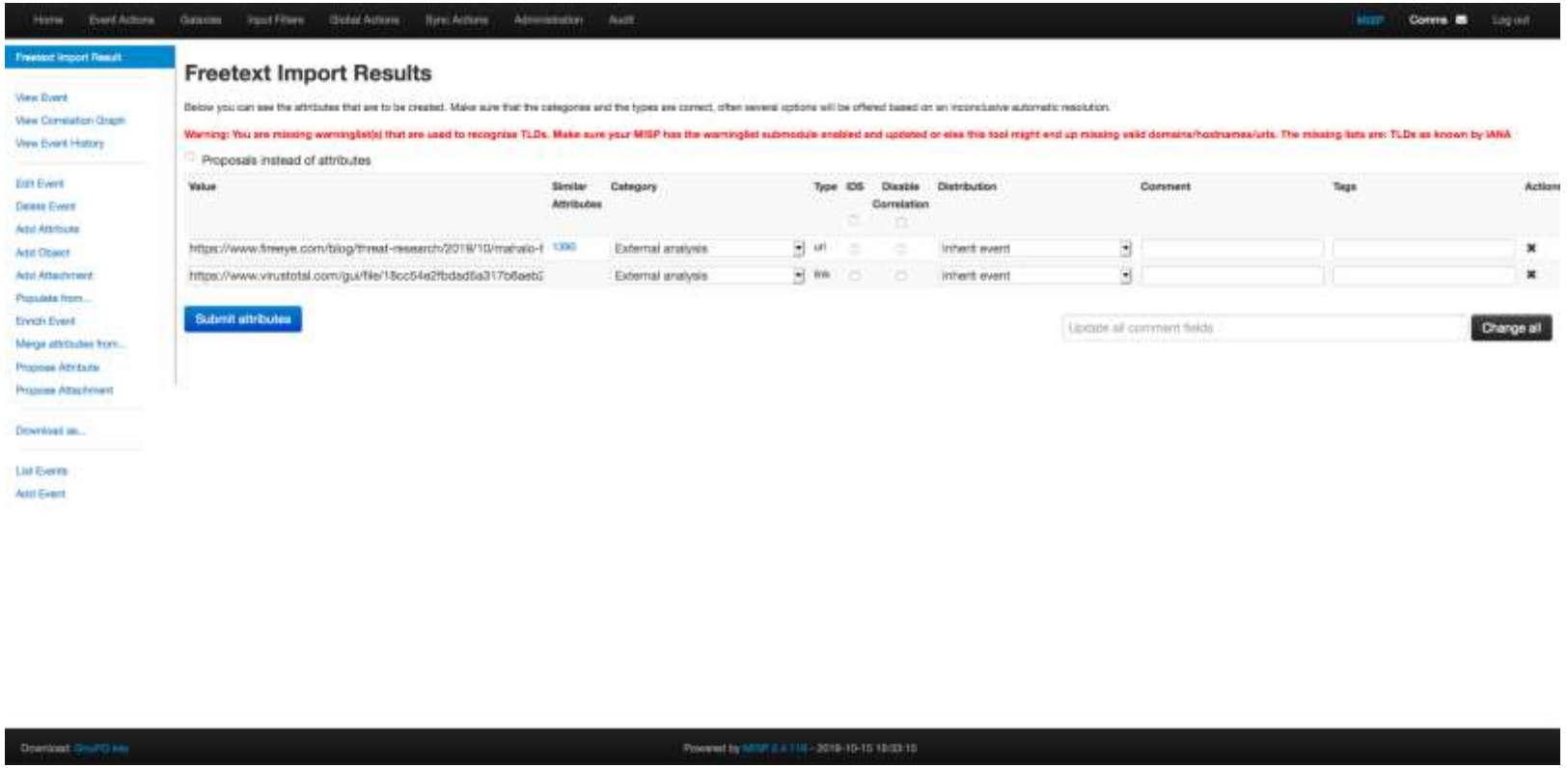
Add Event – Populate Event Data from Other Data



Add Tags to Your Event – Context for Others

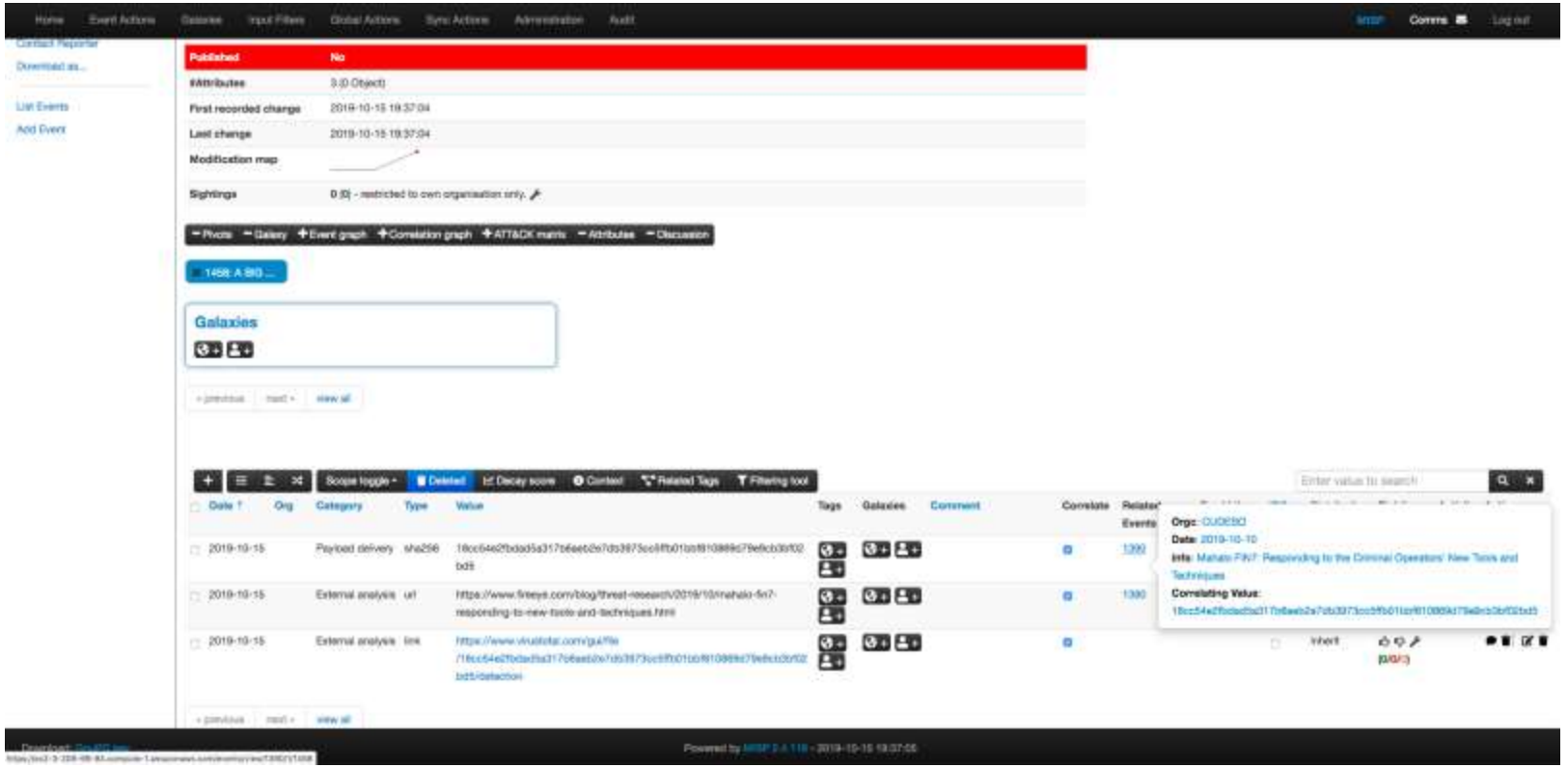


Add Attributes to Your Event IOCs and External Analysis

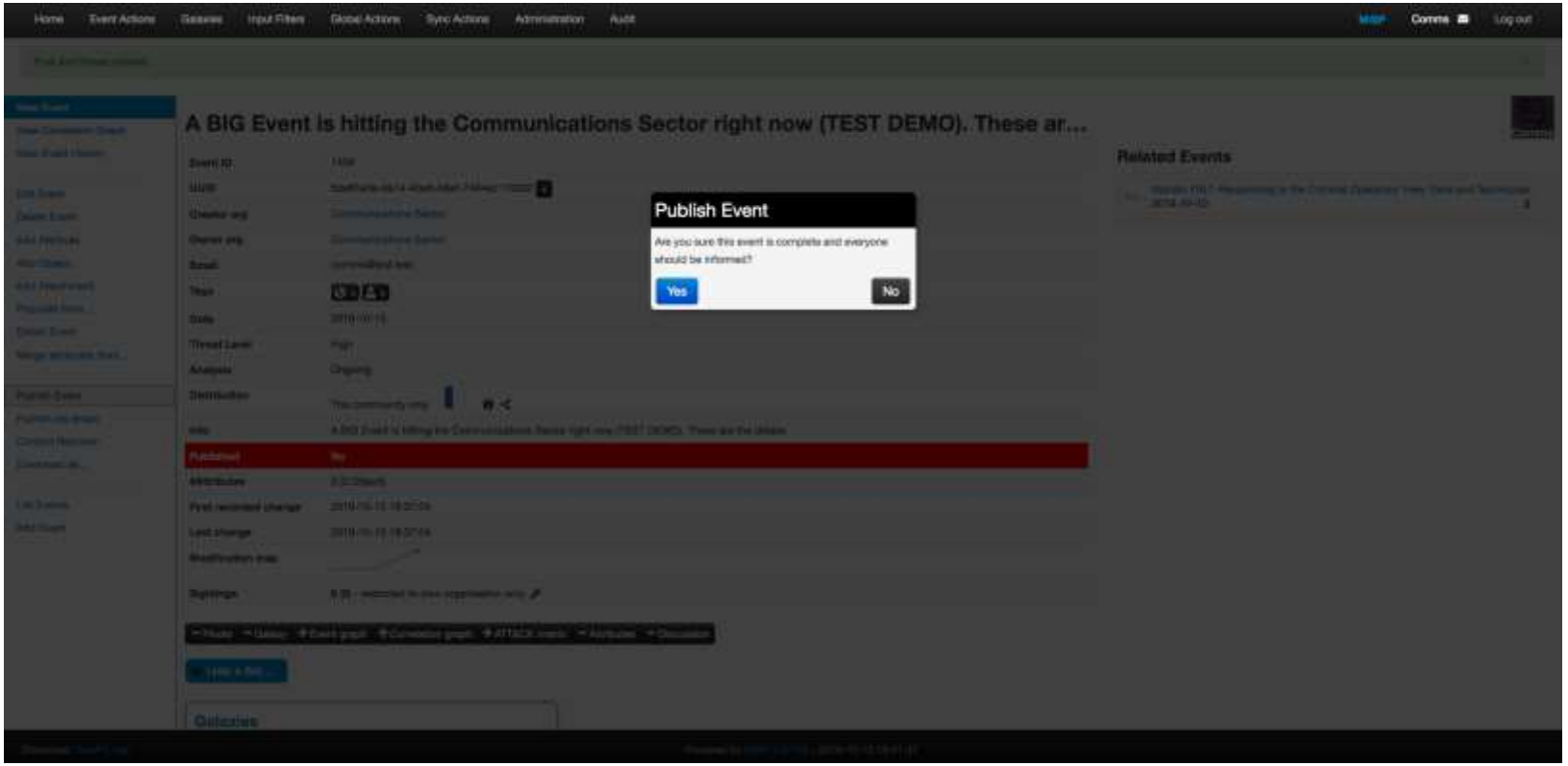


You can also import ‘free’ text and make use of IOC parsing tools to make initial extraction and ‘type’ predictions

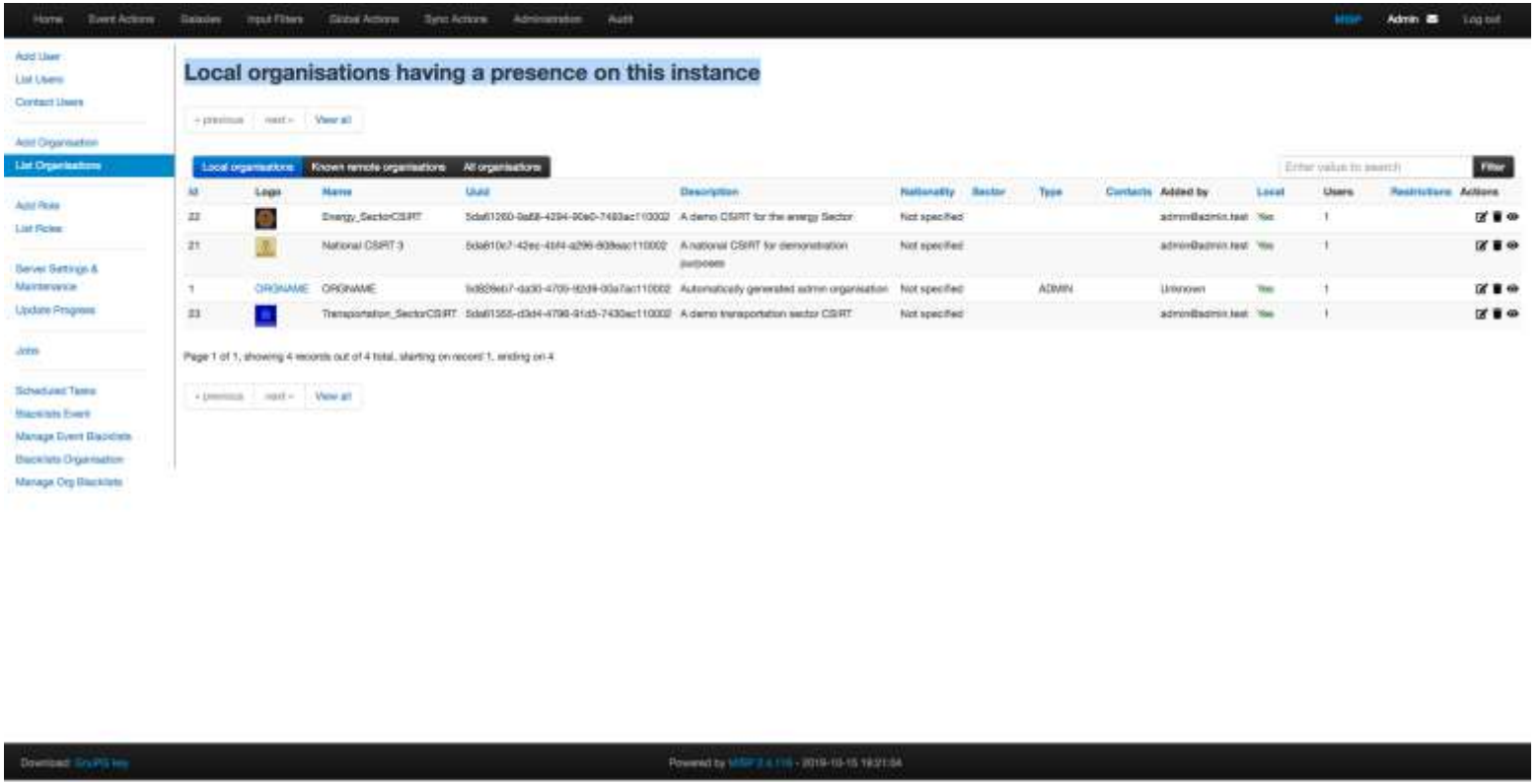
After You Add an Event, MISP looks for events with the same values



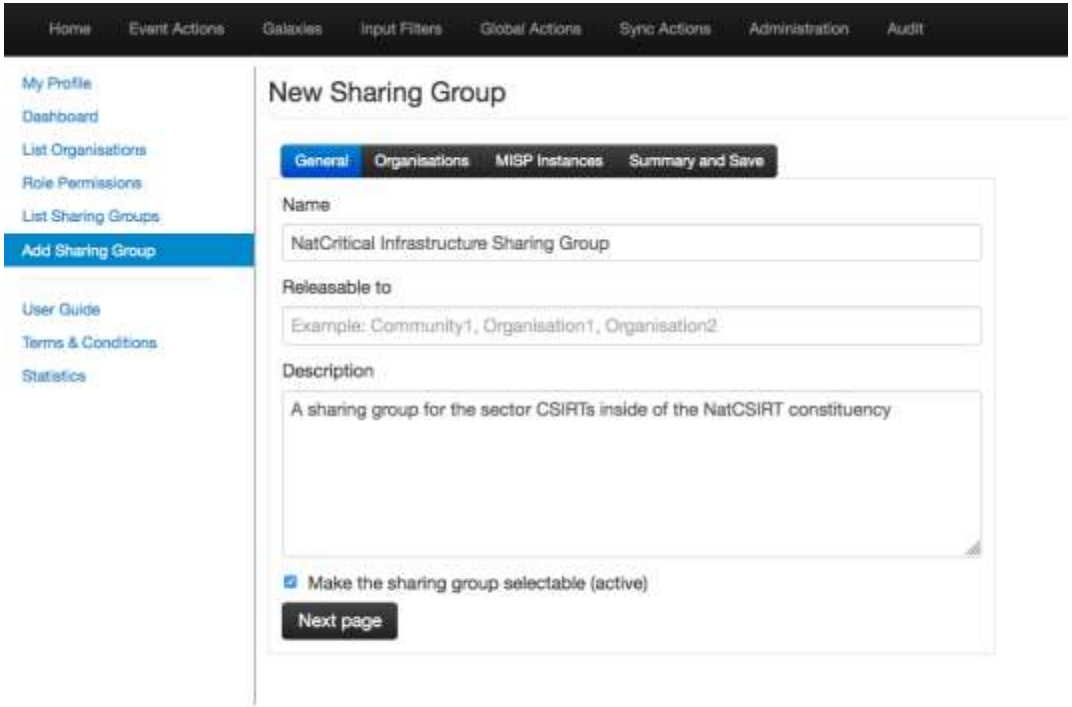
Publish Events



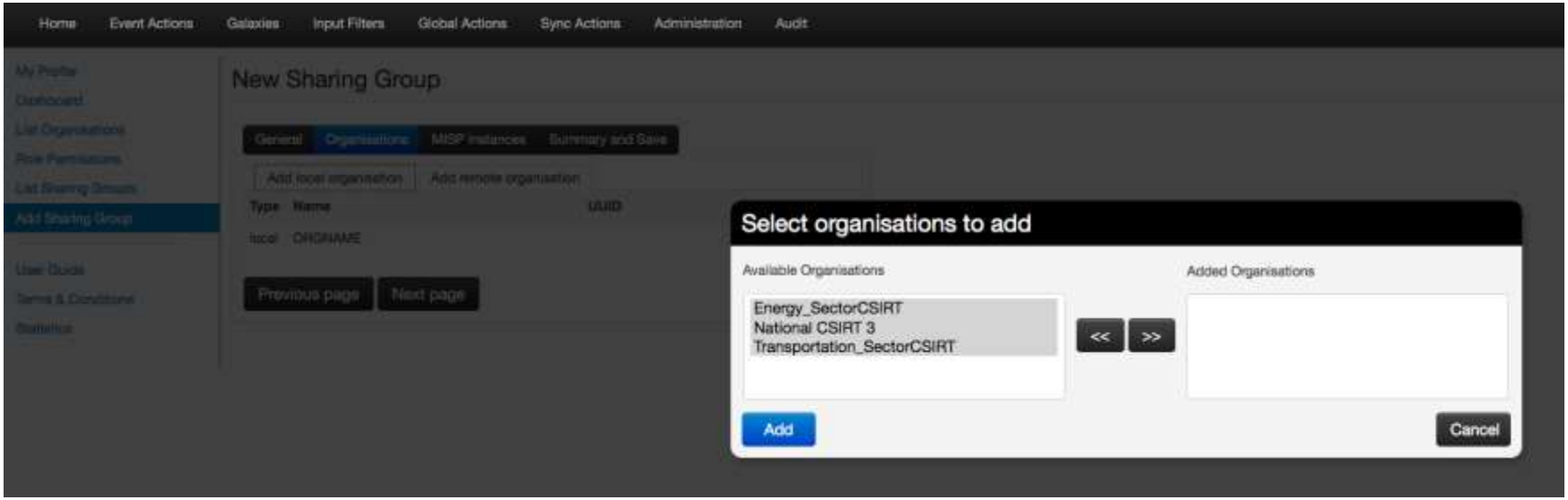
Organization List



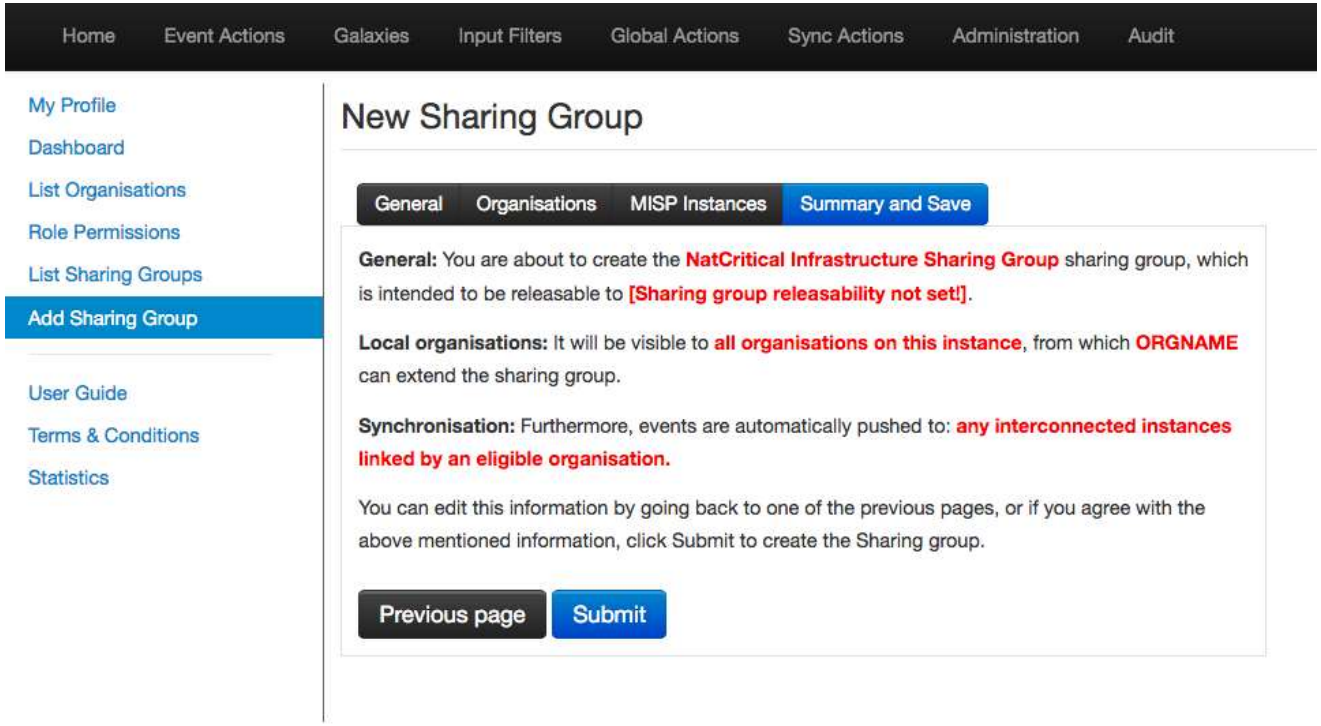
Create New Sharing Group



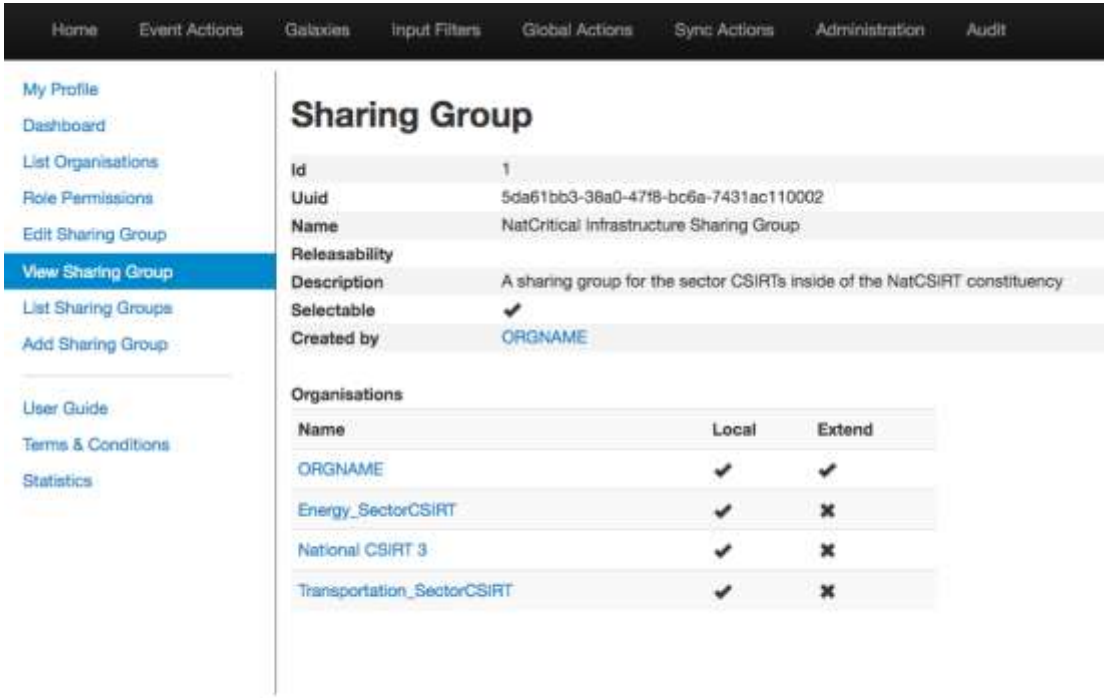
Add Local Organizations



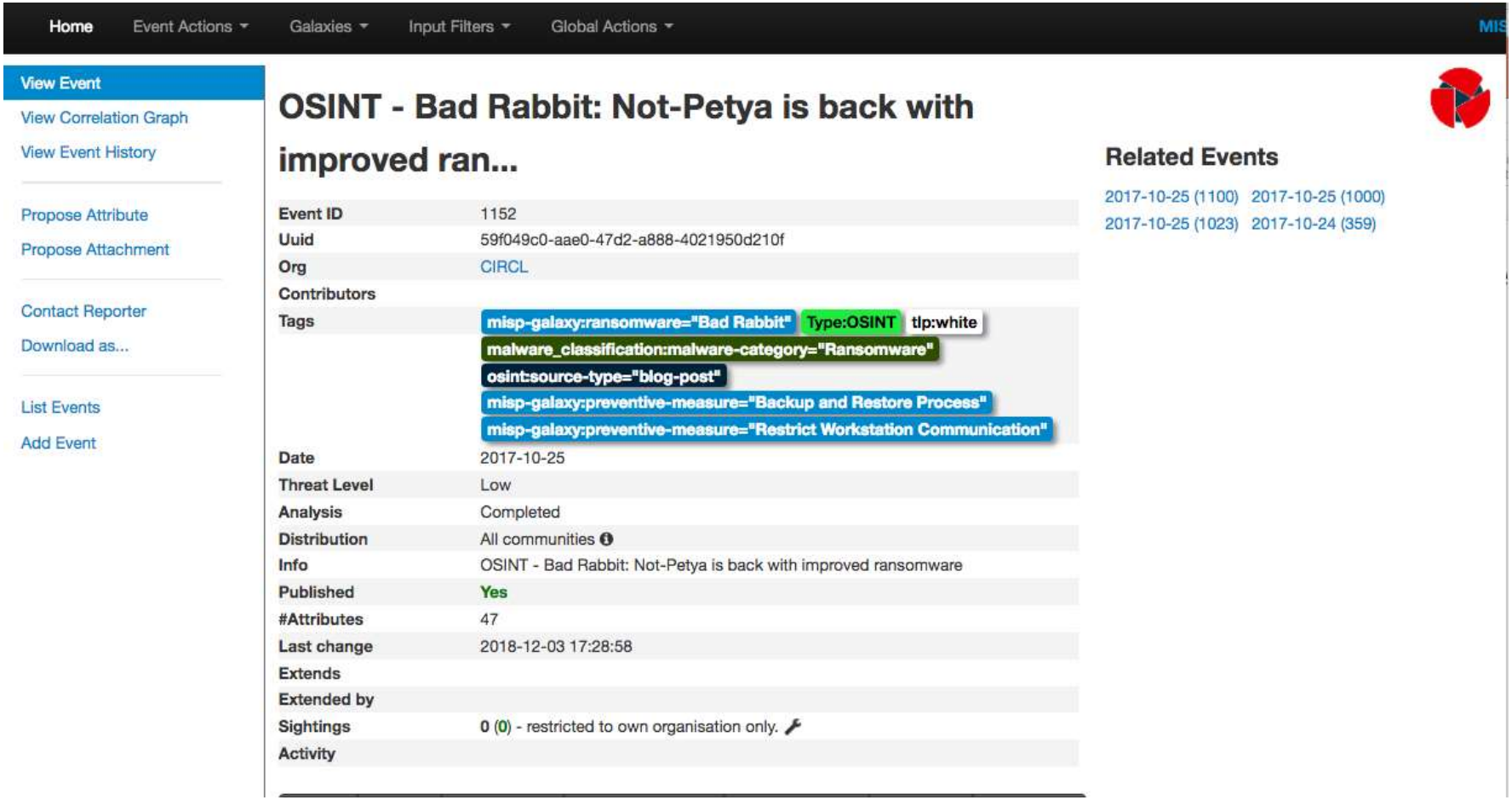
Confirm Sharing Group You Want to Add



View Sharing Group



Others can review your data and may add their own ‘sightings’ or links



Events have standard fields and include Tags. *Tags* are built using *Taxonomies*

Challenges

Data Feeds Require Analysis

- Reports are not always entered by their original authors
- Integration with IDS requires blacklist/whitelist management
- Teams may share using different schemas (but at least they are sharing !)
- Private communities may have more context than public (not a MISP problem alone)
- Dashboard tools are add-ons
- Recommend having technical resources to help with administration and scripts (Linux, Python, SQL, PHP, etc.)

Has had some security bugs

Such as https://cve.circl.lu/cve/CVE-2019-9482

In MISP 2.4.102, an authenticated user can view sightings that they should not be eligible for. Exploiting this requires access to the event that has received the sighting. The issue affects instances with restrictive sighting settings (event only / sighting reported only).

Some are side projects to integrate other tools with MISP more natively (such as Maltego) https://cve.circl.lu/cve/CVE-2020-12889

But developers are responsive and provide fixes for them, updates sometimes multiple times a month.

Summary

1. Sharing Platforms with quality data can help improve correlations and actionable defenses (IDS, etc.) for Cyber Protection and Incident Response Teams
2. Taxonomies for Term re-use and common language may improve shared understanding
3. MISP is an open source platform for storing and sharing events, attributes and adding meta-data for taxonomies, tags.
4. MISP can fit into a larger ecosystem of tools
5. Communities can share Events attached to IOC, TTP, and Mitigations
6. Has features for restricting distribution, private taxonomy, defining sharing groups, correlation.
7. Has integrations with other data services for enrichment

Discussions & Questions?

Contact Information

sjperl@cert.org