Carnegie Mellon University
Software Engineering Institute

[DISTRIBUTION STATEMENT TBD]

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.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by Carnegie Mellon University or its Software Engineering Institute.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

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)

MISP
Threat Sharing

Key Features:

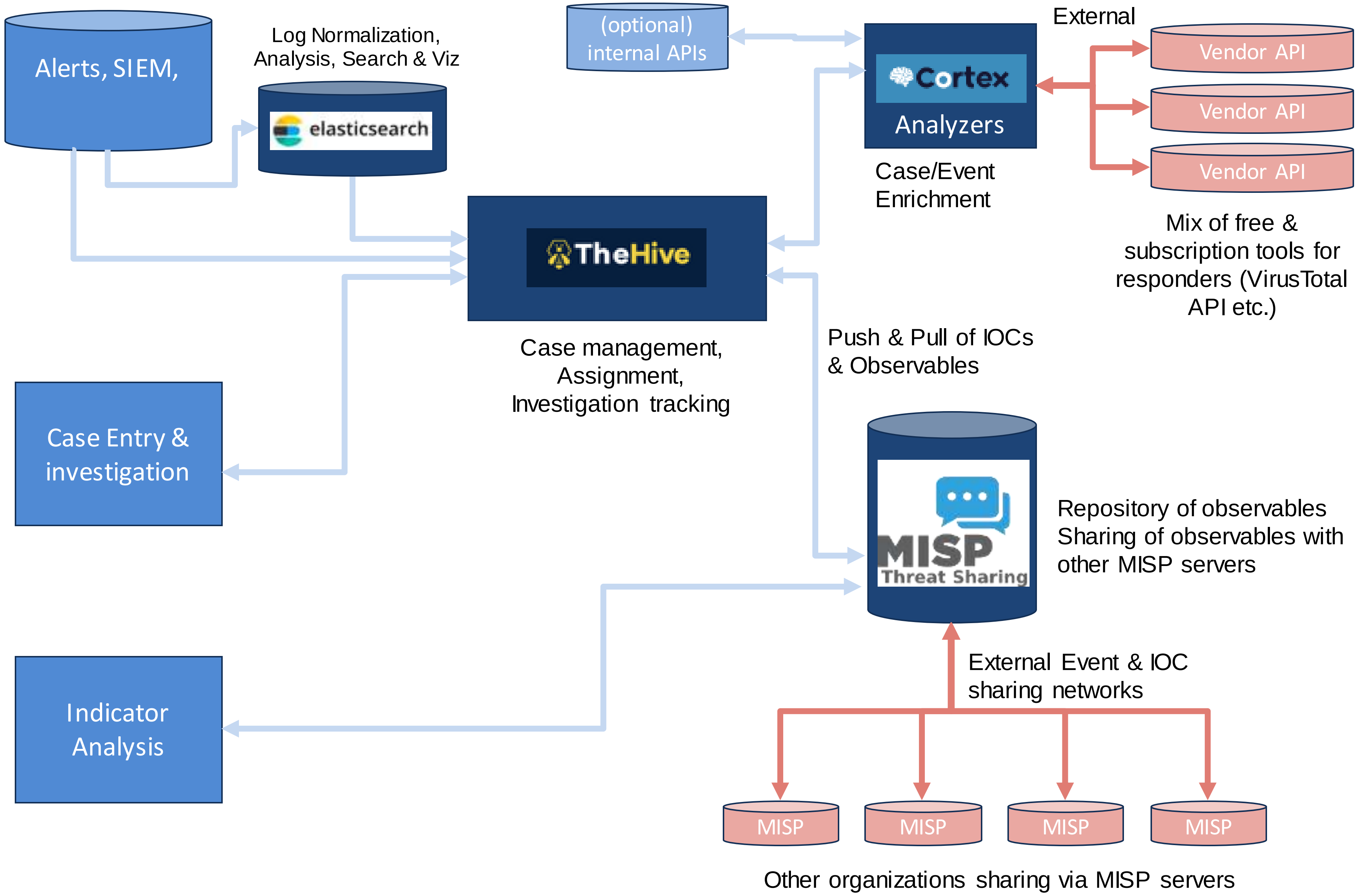
- Store, share, collaborate on cyber security indicators, malware analysis, and use to detect and prevent attacks or threats.
- Support for Events to have tags, to apply different taxonomies,
- Multi-layered Sharing groups for multiple organizations with permissions and protocols (including TLP)
- Import/Export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

Example Use

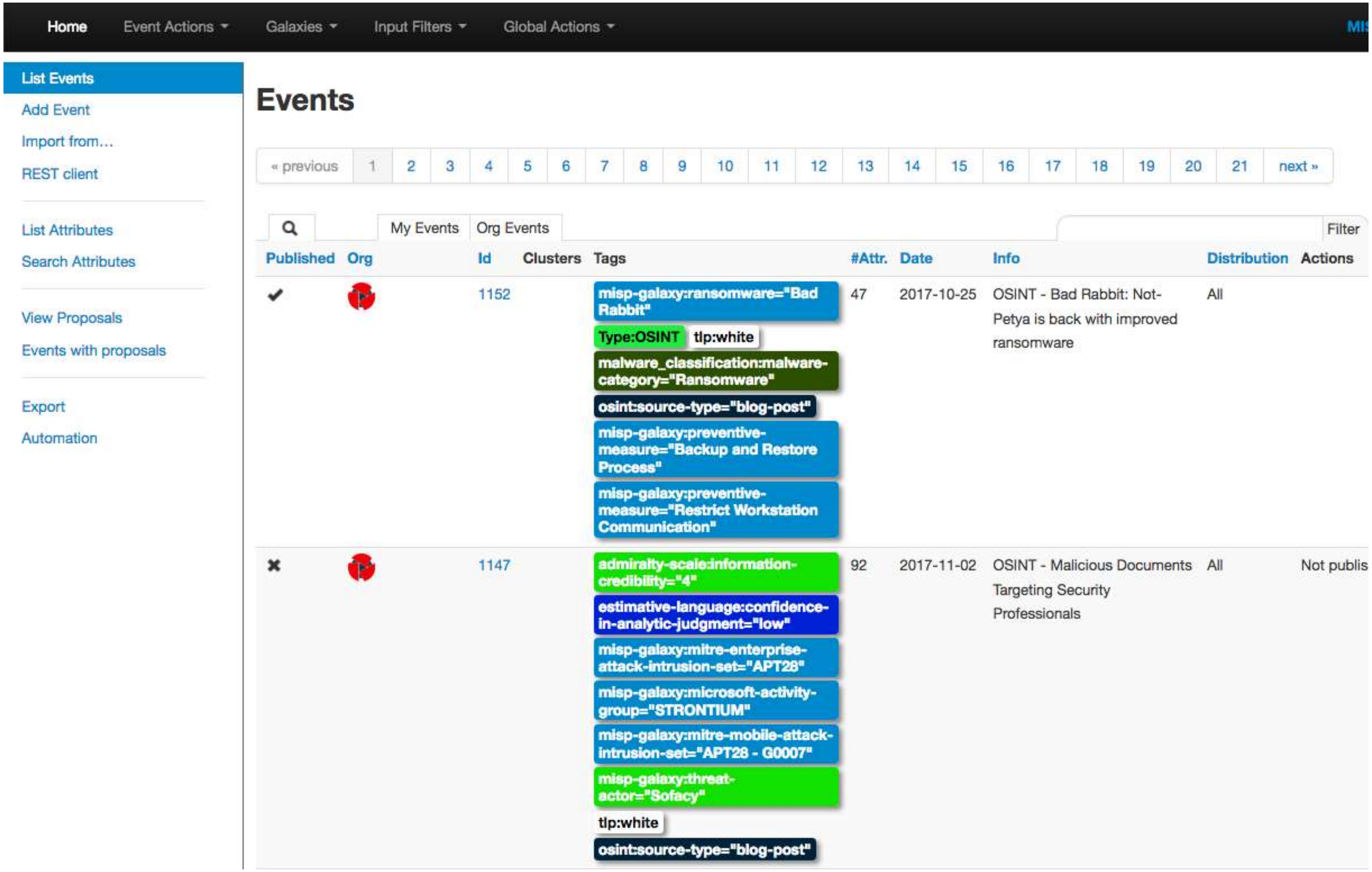
Typical Artifact and IOC flow

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 <u>certain</u> results with others using rules
6. Store historical results – for future case analysis

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


Alerts, SIEM,
Log Normalization, Analysis, Search & Viz
elasticsearch
(optional) internal APIs
Cortex
Analyzers
Case/Event Enrichment
External
Vendor API
Vendor API
Vendor API
Mix of free & subscription tools for responders (VirusTotal API etc.)
TheHive
Case management, Assignment, Investigation tracking
Push & Pull of IOCs & Observables
Case Entry & investigation
MISP Threat Sharing
Repository of observables Sharing of observables with other MISP servers
External Event & IOC sharing networks
Indicator Analysis
MISP
MISP
MISP
MISP
Other organizations sharing via MISP servers

MISP – Event List

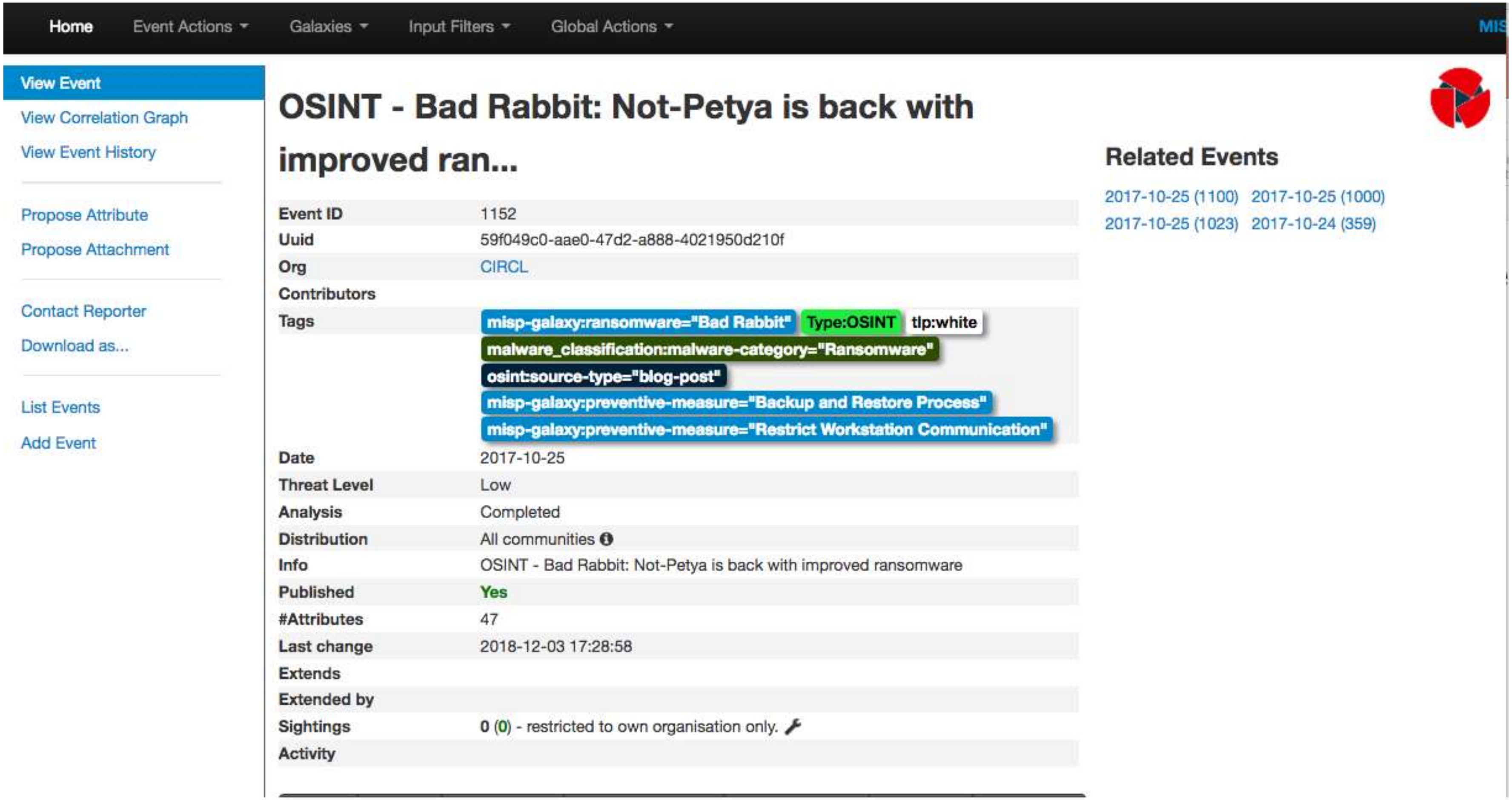


Events

Published	Org	Id	Clusters	Tags	#Attr.	Date	Info	Distribution	Actions
✓	●	1152		misp-galaxy:ransomware="Bad Rabbit" Type:OSINT tlp:white malware_classification:malware-category="Ransomware" osint:source-type="blog-post" misp-galaxy:preventive-measure="Backup and Restore Process" misp-galaxy:preventive-measure="Restrict Workstation Communication"	47	2017-10-25	OSINT - Bad Rabbit: Not-Petya is back with improved ransomware	All	
✖	●	1147		admiralty-scale:information-credibility="4" estimative-language:confidence-in-analytic-judgment="low" misp-galaxy:mitre-enterprise-attack-intrusion-set="APT28" misp-galaxy:microsoft-activity-group="STRONTIUM" misp-galaxy:mitre-mobile-attack-intrusion-set="APT28 - G0007" misp-galaxy:threat-actor="Sofacy" tlp:white osint:source-type="blog-post"	92	2017-11-02	OSINT - Malicious Documents Targeting Security Professionals	All	Not publis

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

MISP – Store an Event



OSINT - Bad Rabbit: Not-Petya is back with improved ran...

Event ID	1152
Uuid	59f049c0-aae0-47d2-a888-4021950d210f
Org	CIRCL
Contributors	
Tags	misp-galaxy:ransomware="Bad Rabbit" Type:OSINT tlp:white malware_classification:malware-category="Ransomware" osint:source-type="blog-post" misp-galaxy:preventive-measure="Backup and Restore Process" misp-galaxy:preventive-measure="Restrict Workstation Communication"
Date	2017-10-25
Threat Level	Low
Analysis	Completed
Distribution	All communities
Info	OSINT - Bad Rabbit: Not-Petya is back with improved ransomware
Published	Yes
#Attributes	47
Last change	2018-12-03 17:28:58
Extends	
Extended by	
Sightings	0 (0) - restricted to own organisation only.
Activity	

Related Events

2017-10-25 (1100) 2017-10-25 (1000)
2017-10-25 (1023) 2017-10-24 (359)

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.

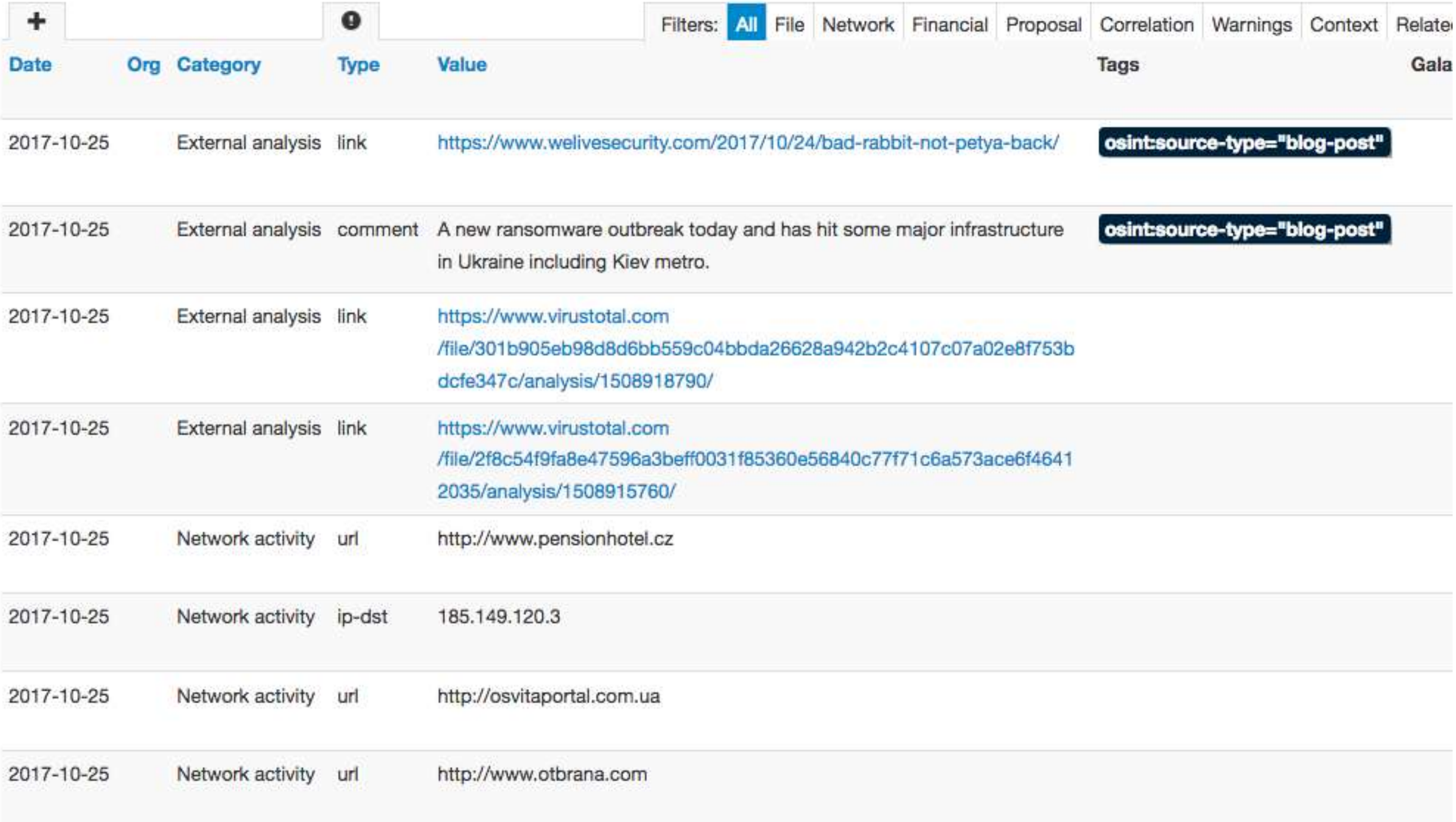
More Information Sharing Examples

- 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



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/301b905eb98d8d6bb559c04bbda26628a942b2c4107c07a02e8f753bdcfe347c/analysis/1508918790/		
2017-10-25		External analysis	link	https://www.virustotal.com/file/2f8c54f9fa8e47596a3beff0031f85360e56840c77f71c6a573ace6f46412035/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

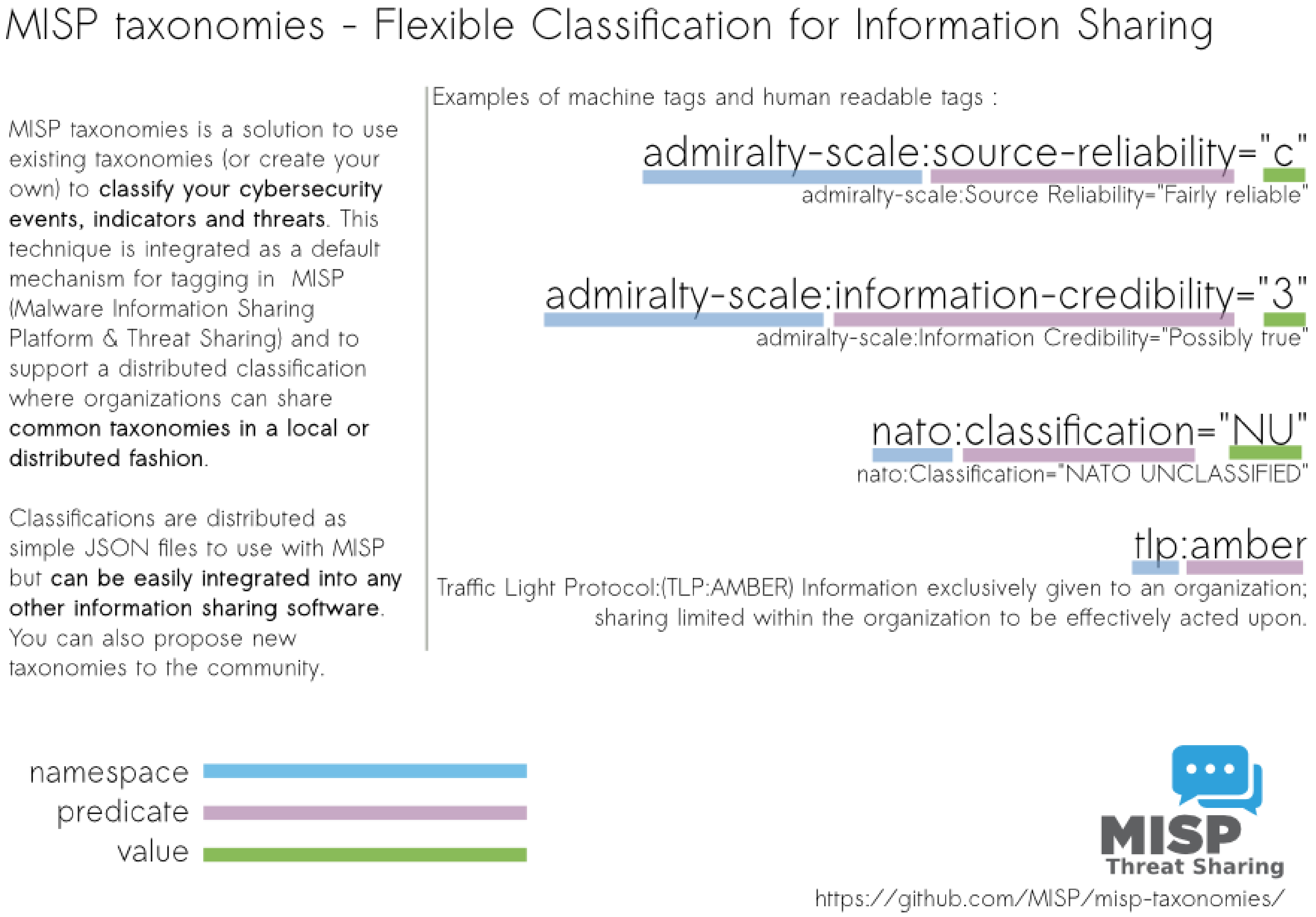
Main Benefit

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.

namespace

predicate

value

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

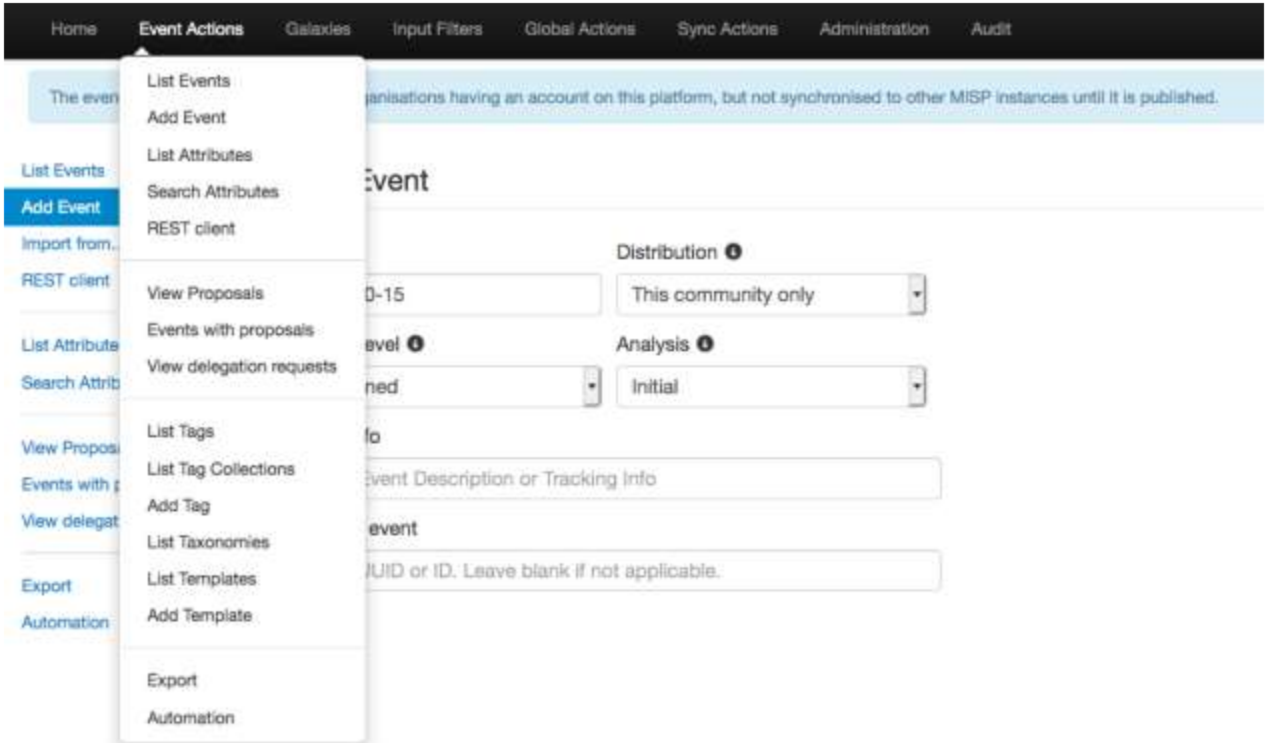
Sharing Communities & Data

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



The even ganisations having an account on this platform, but not synchronised to other MISP instances until it is published.

Event

0-15

Distribution: This community only

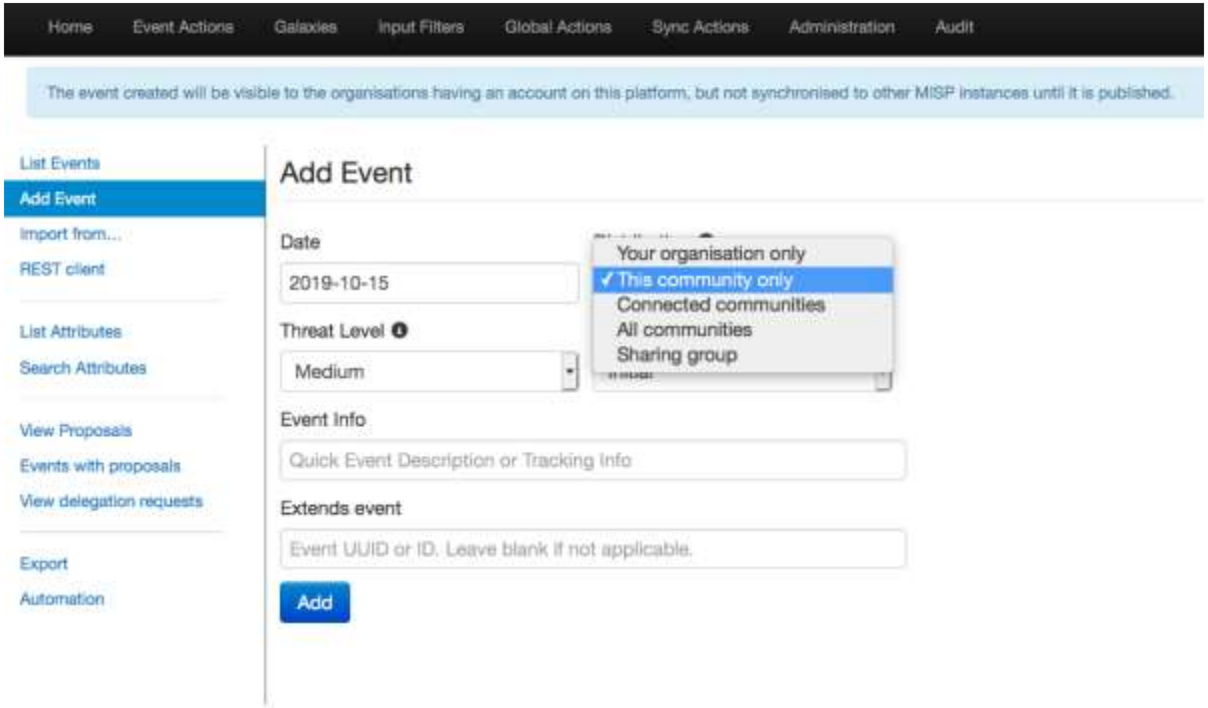
evel: ned

Analysis: Initial

fo: Event Description or Tracking Info

event: UUID or ID. Leave blank if not applicable.

Set Distribution of Event



The event created will be visible to the organisations having an account on this platform, but not synchronised to other MISP instances until it is published.

Add Event

Date: 2019-10-15

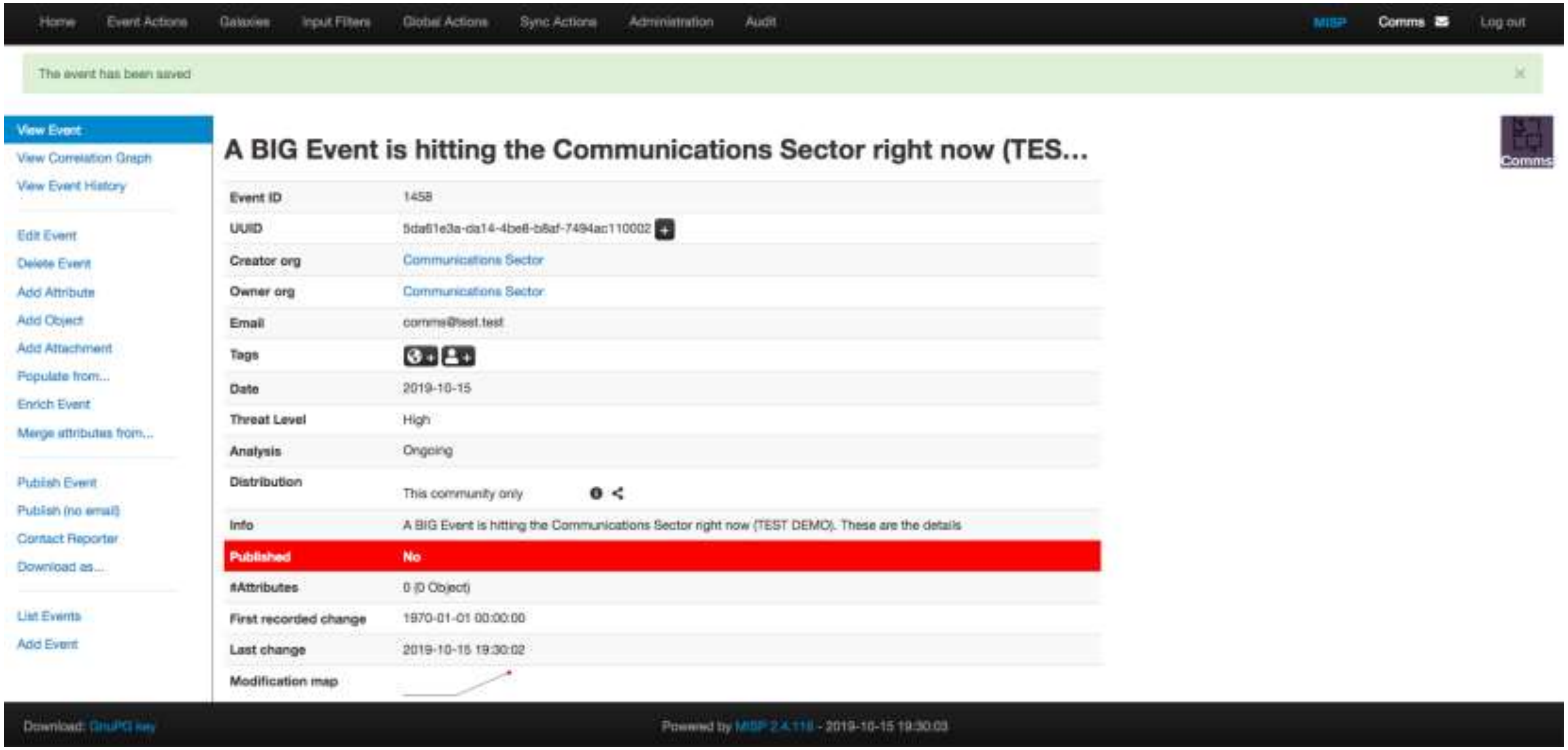
Threat Level: Medium

- Your organisation only
- ✓ This community only
- Connected communities
- All communities
- Sharing group

Event Info: Quick Event Description or Tracking Info

Extends event: Event UUID or ID. Leave blank if not applicable.

Add Event



The event has been saved

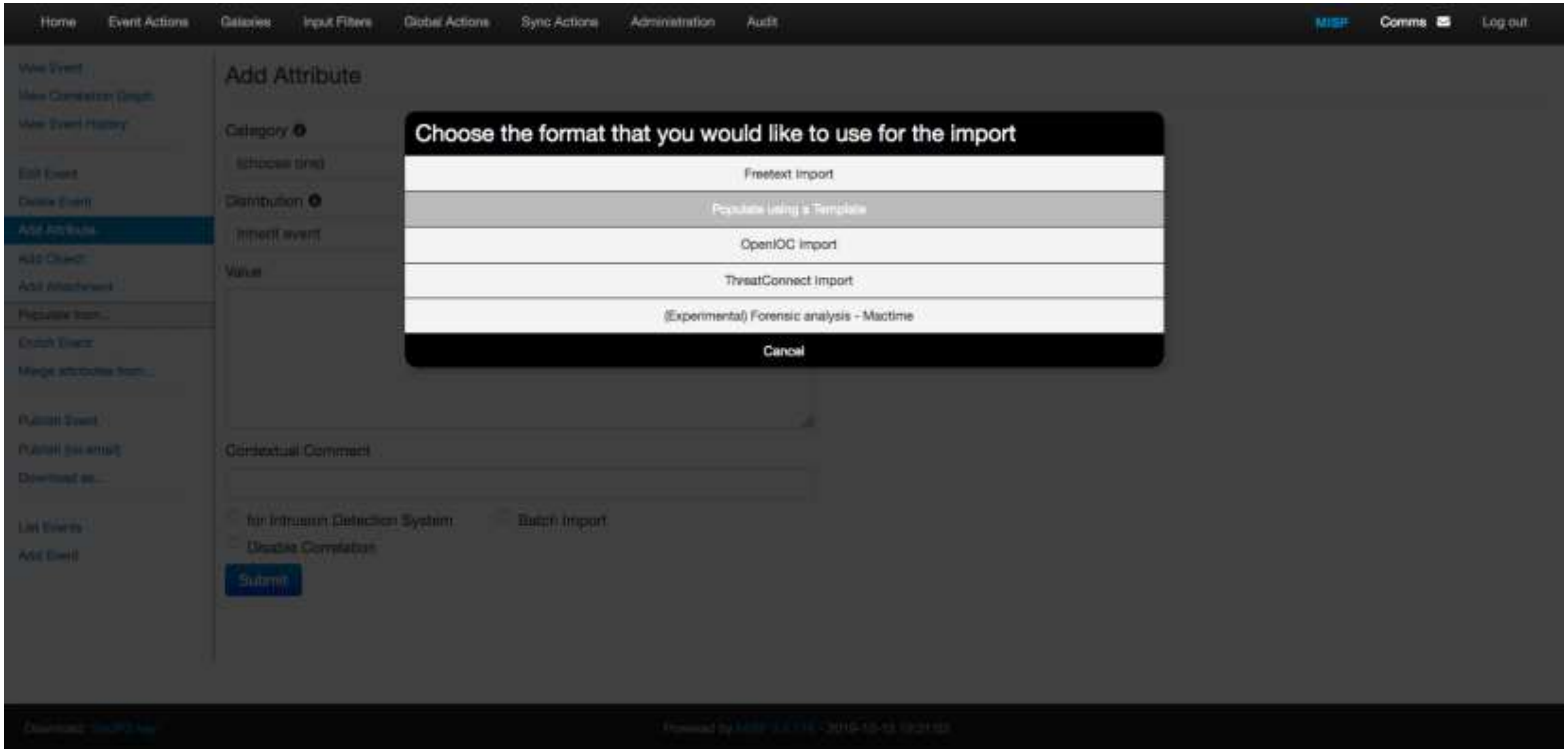
A BIG Event is hitting the Communications Sector right now (TES...

Event ID	1458
UUID	5da61e3a-da14-4be8-b8af-7494ac110002
Creator org	Communications Sector
Owner org	Communications Sector
Email	comms@test.test
Tags	
Date	2019-10-15
Threat Level	High
Analysis	Ongoing
Distribution	This community only
Info	A BIG Event is hitting the Communications Sector right now (TEST DEMO). These are the details
Published	No
#Attributes	0 (0 Object)
First recorded change	1970-01-01 00:00:00
Last change	2019-10-15 19:30:02
Modification map	

Download: GnuPG key

Powered by MISP 2.4.116 - 2019-10-15 19:30:03

Add Event – Populate Event Data from Other Data



Add Attribute

Category: (choose one)

Distribution: Inherit event

Value

Contextual Comment

□ for Intrusion Detection System □ Batch Import

□ Disable Correlation

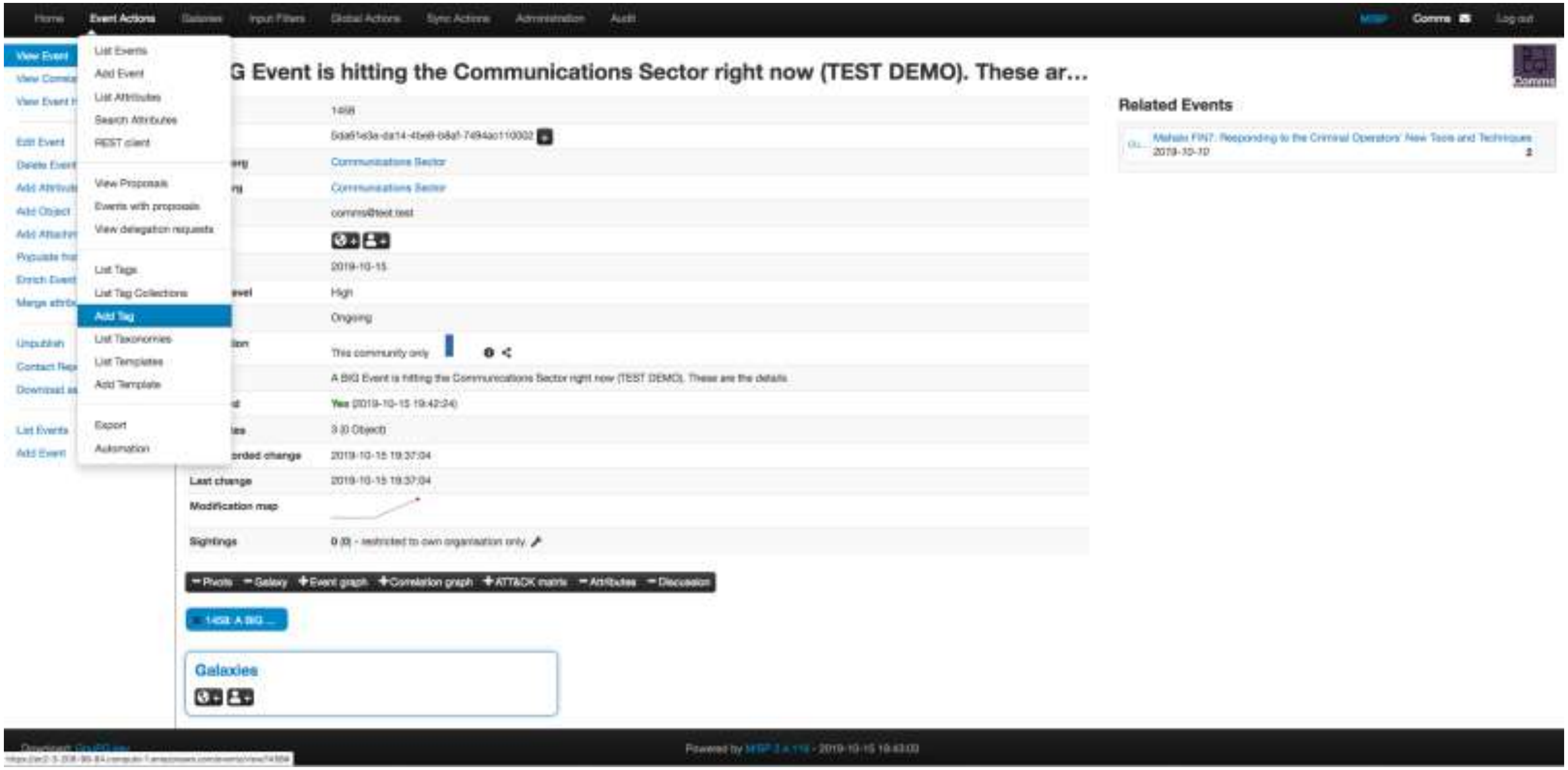
Submit

Choose the format that you would like to use for the import

- Freetext Import
- Populate using a Template
- OpenIOC Import
- ThreatConnect Import
- (Experimental) Forensic analysis - Mactime

Cancel

Add Tags to Your Event – Context for Others



G Event is hitting the Communications Sector right now (TEST DEMO). These ar...

1458

5da61e3a-da14-4be8-b8af-7494ac110002

…erg Communications Sector

…rg Communications Sector

comms@test.test

2019-10-15

…evel High

Ongoing

…ion This community only

A BIG Event is hitting the Communications Sector right now (TEST DEMO). These are the details

…d Yes (2019-10-15 19:42:24)

…ies 3 (0 Object)

…orded change 2019-10-15 19:37:04

Last change 2019-10-15 19:37:04

Modification map

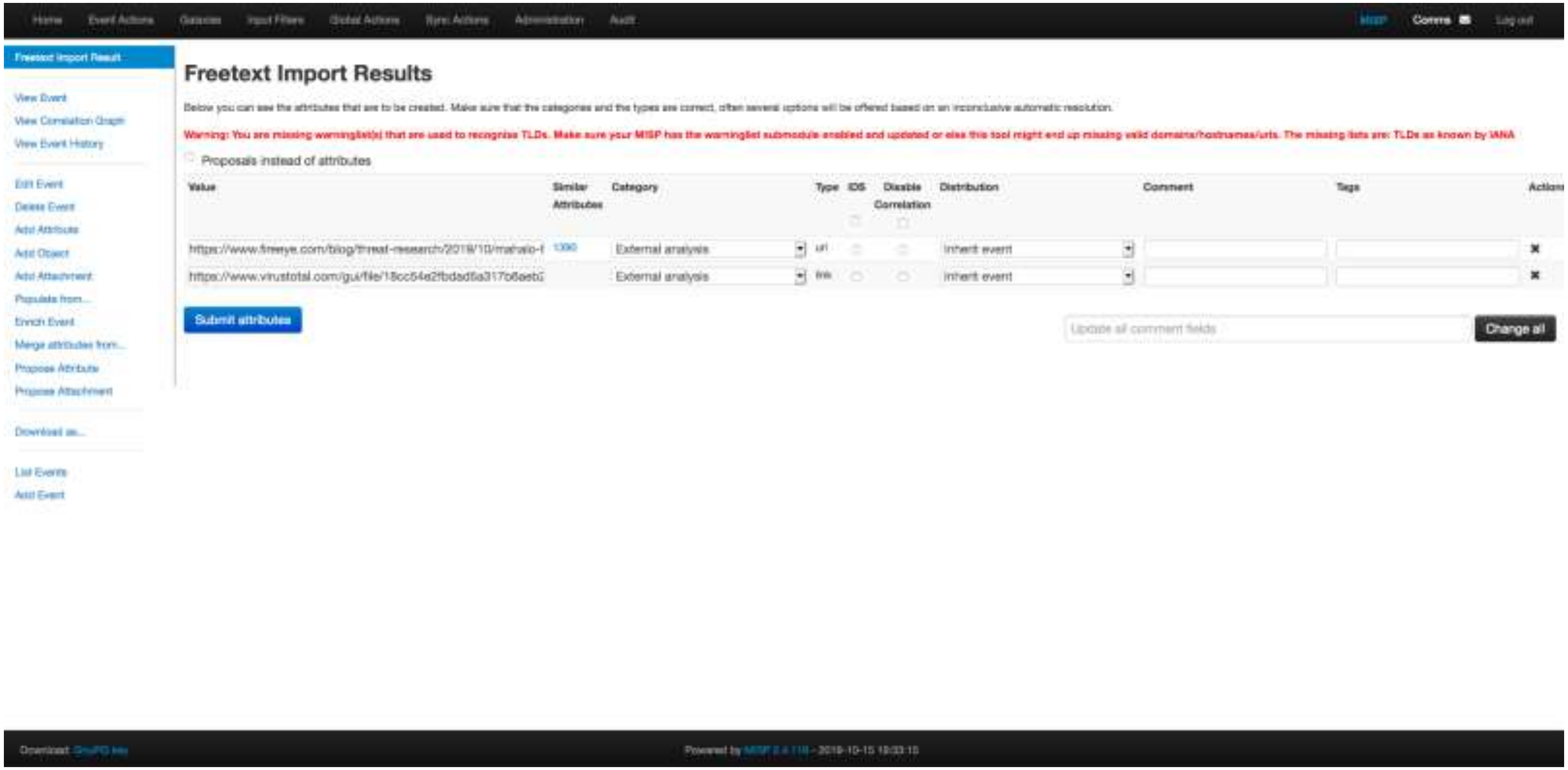
Sightings 0 (0) - restricted to own organisation only

Related Events

Mahalo FIN7: Responding to the Criminal Operators' New Tools and Techniques
2019-10-10 2

Powered by MISP 2.4.116 - 2019-10-15 19:43:00

Add Attributes to Your Event IOCs and External Analysis



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.

Warning: You are missing warninglist(s) that are used to recognise TLDs. Make sure your MISP has the warninglist submodule enabled and updated or else this tool might end up missing valid domains/hostnames/urls. The missing lists are: TLDs as known by IANA

○ Proposals instead of attributes

Value	Similar Attributes	Category	Type	IDS □	Disable Correlation □	Distribution	Comment	Tags	Actions
https://www.fireeye.com/blog/threat-research/2019/10/mahalo-f	1390	External analysis	url	○	○	Inherit event			✖
https://www.virustotal.com/gui/file/18cc54e2fbdad6a317b6aeb2		External analysis	link	○	○	Inherit event			✖

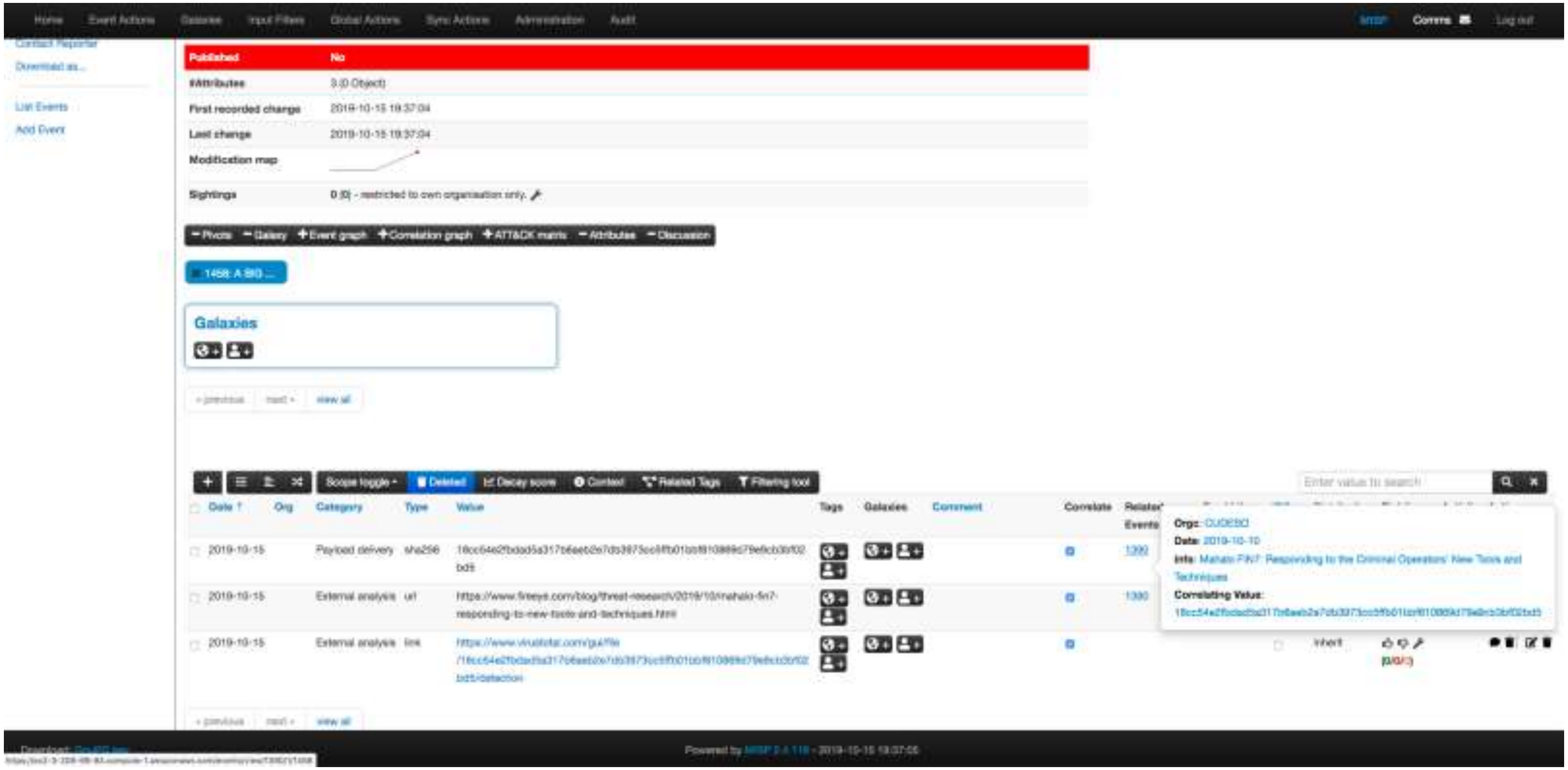
Update all comment fields

Download: GnuPG key

Powered by MISP 2.4.116 - 2019-10-15 19:03:15

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



Published	No
#Attributes	3 (0 Object)
First recorded change	2019-10-15 19:37:04
Last change	2019-10-15 19:37:04
Modification map	
Sightings	0 (0) - restricted to own organisation only.

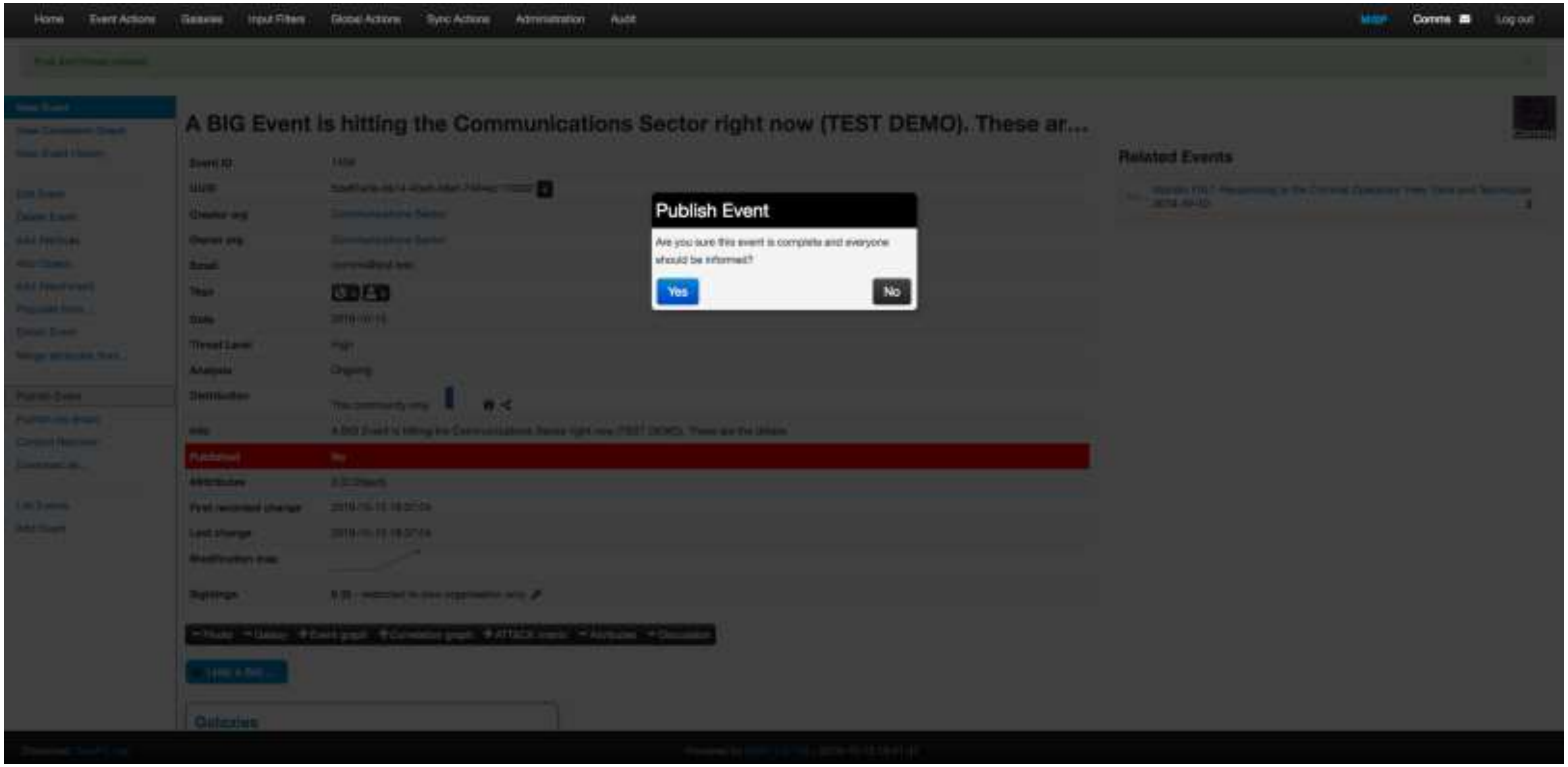
Date	Org	Category	Type	Value	Tags	Galaxies	Comment	Correlate	Related Events
2019-10-15		Payload delivery	sha256	[illegible]				☑	1300
2019-10-15		External analysis	url	https://www.fireeye.com/blog/threat-research/2019/10/mahalo-fin7-responding-to-new-tools-and-techniques.html				☑	1300
2019-10-15		External analysis	link	https://www.virustotal.com/gui/file/[illegible]/detection				☑	

Orgc: CUCESO
Date: 2019-10-10
Info: Mahalo FIN7: Responding to the Criminal Operators' New Tools and Techniques
Correlating Value: [illegible]

Inherit (0/0/0)

Powered by MISP 2.4.118 - 2019-10-15 19:37:05

Publish Events

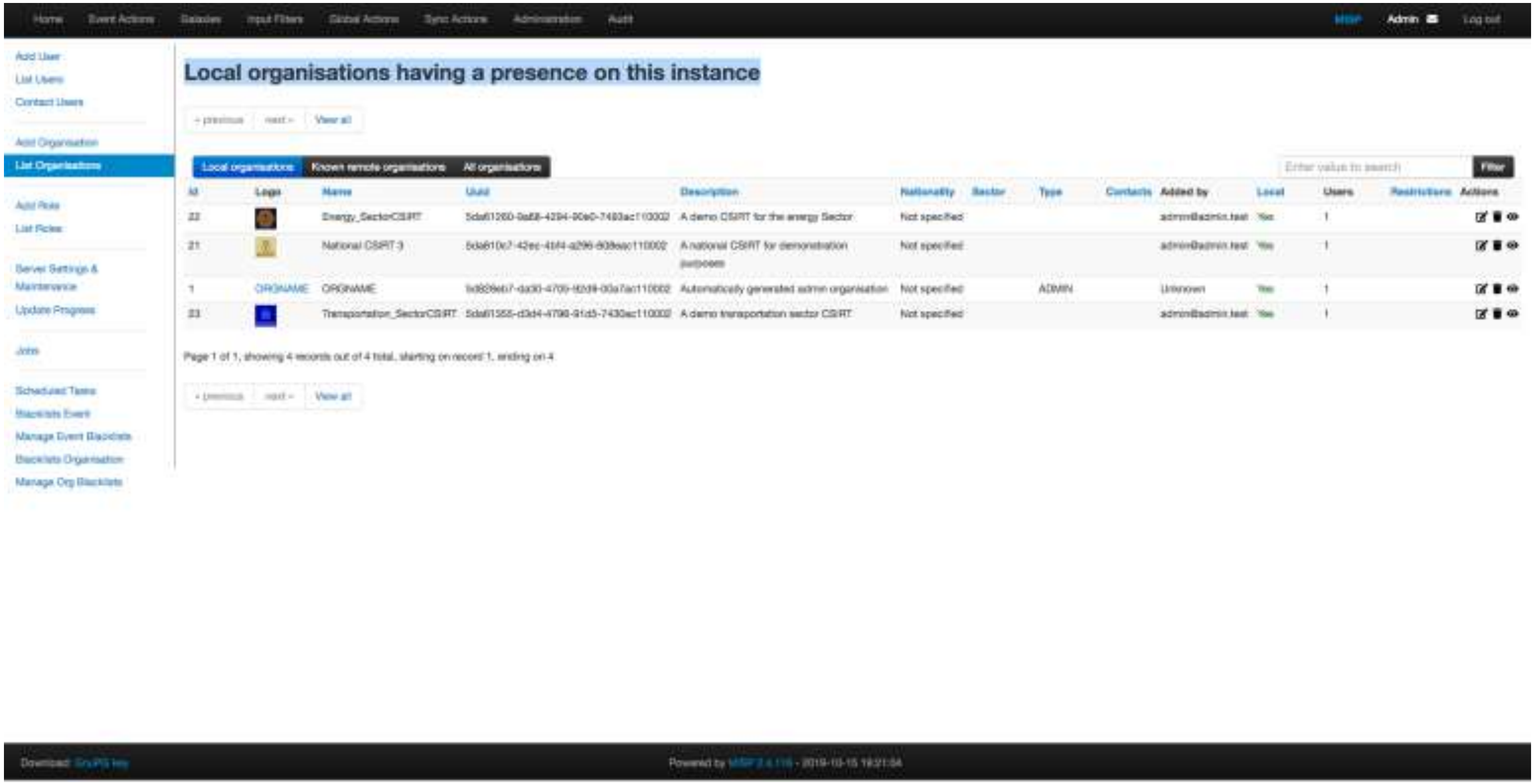


A BIG Event is hitting the Communications Sector right now (TEST DEMO). These ar...

Publish Event

Are you sure this event is complete and everyone should be informed?

Organization List



Local organisations having a presence on this instance

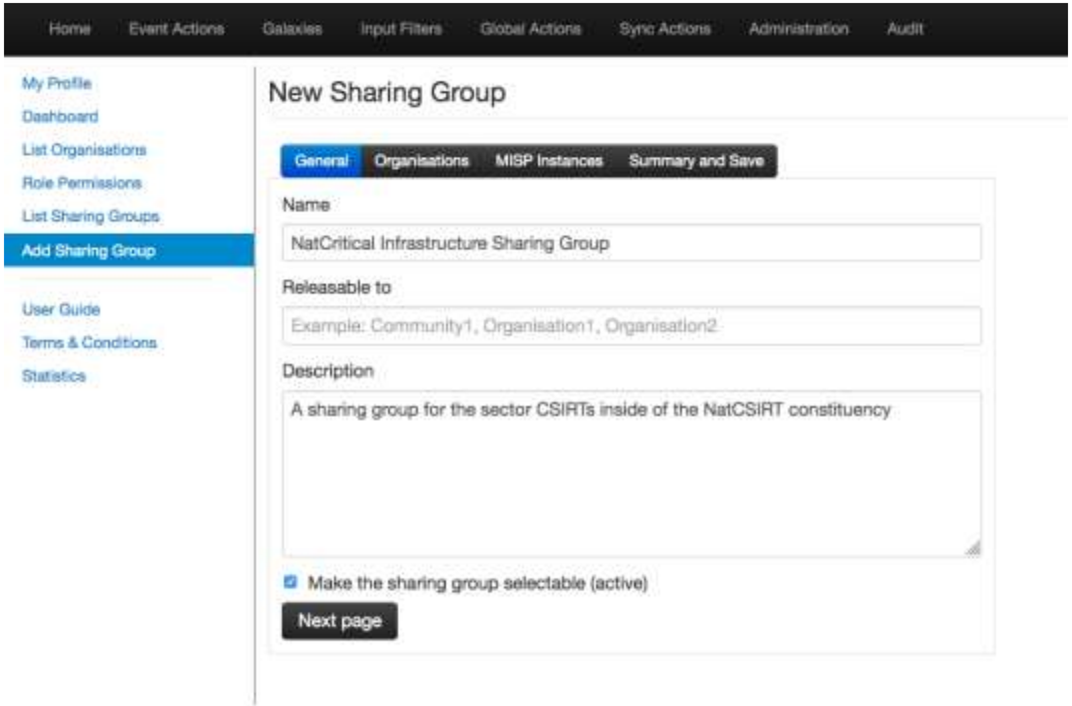
Id	Logo	Name	Uuid	Description	Nationality	Sector	Type	Contacts	Added by	Local	Users	Restrictions	Actions
22		Energy_SectorCSIRT	5da61260-0a68-4294-90e0-7483ac110002	A demo CSIRT for the energy Sector	Not specified				admin@admin.test	Yes	1		
21		National CSIRT 3	5da610c7-42ec-4bf4-a296-608eac110002	A national CSIRT for demonstration purposes	Not specified				admin@admin.test	Yes	1		
1	ORGNAME	ORGNAME	5d829eb7-da30-4709-92d9-00a7ac110002	Automatically generated admin organisation	Not specified		ADMIN		Unknown	Yes	1		
23		Transportation_SectorCSIRT	5da61355-d3d4-4798-91d5-7430ac110002	A demo transportation sector CSIRT	Not specified				admin@admin.test	Yes	1		

Page 1 of 1, showing 4 records out of 4 total, starting on record 1, ending on 4

Download: GnuPG key

Powered by MISP 2.4.116 - 2019-10-15 19:21:04

Create New Sharing Group



New Sharing Group

Name

NatCritical Infrastructure Sharing Group

Releasable to

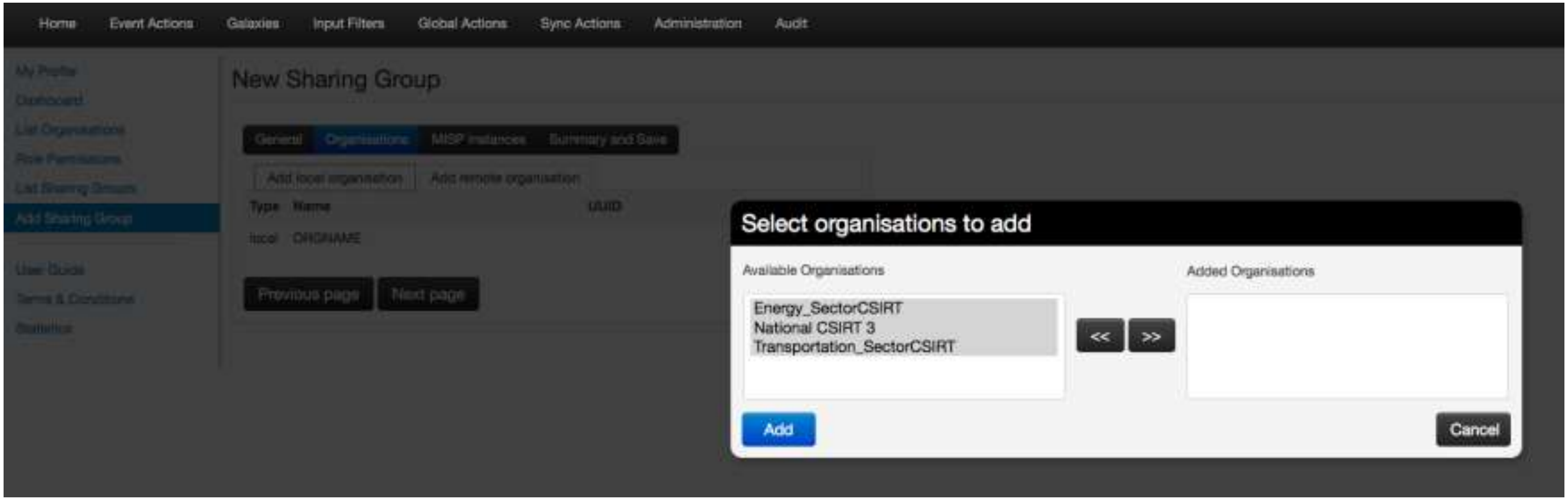
Example: Community1, Organisation1, Organisation2

Description

A sharing group for the sector CSIRTs inside of the NatCSIRT constituency

☑ Make the sharing group selectable (active)

Add Local Organizations



New Sharing Group

Type	Name	UUID
local	ORGNAME	

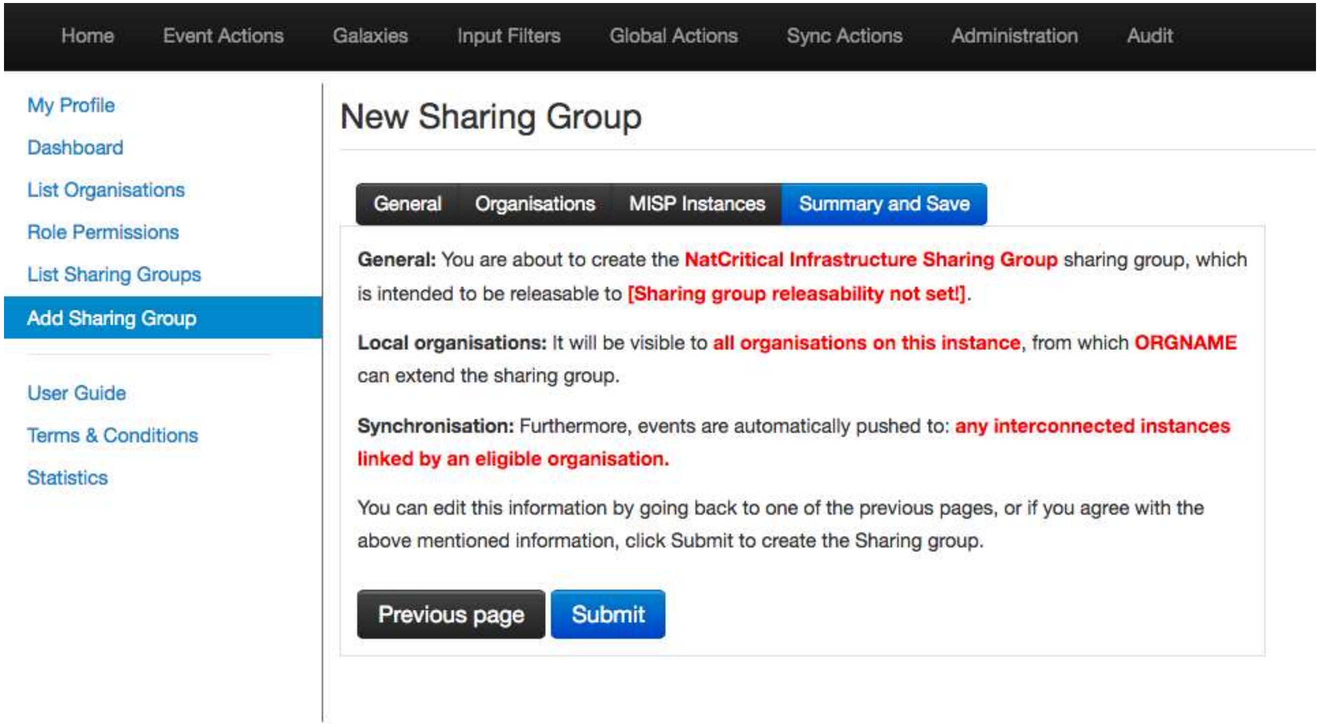
Select organisations to add

Available Organisations

Energy_SectorCSIRT
National CSIRT 3
Transportation_SectorCSIRT

Added Organisations

Confirm Sharing Group You Want to Add



New Sharing Group

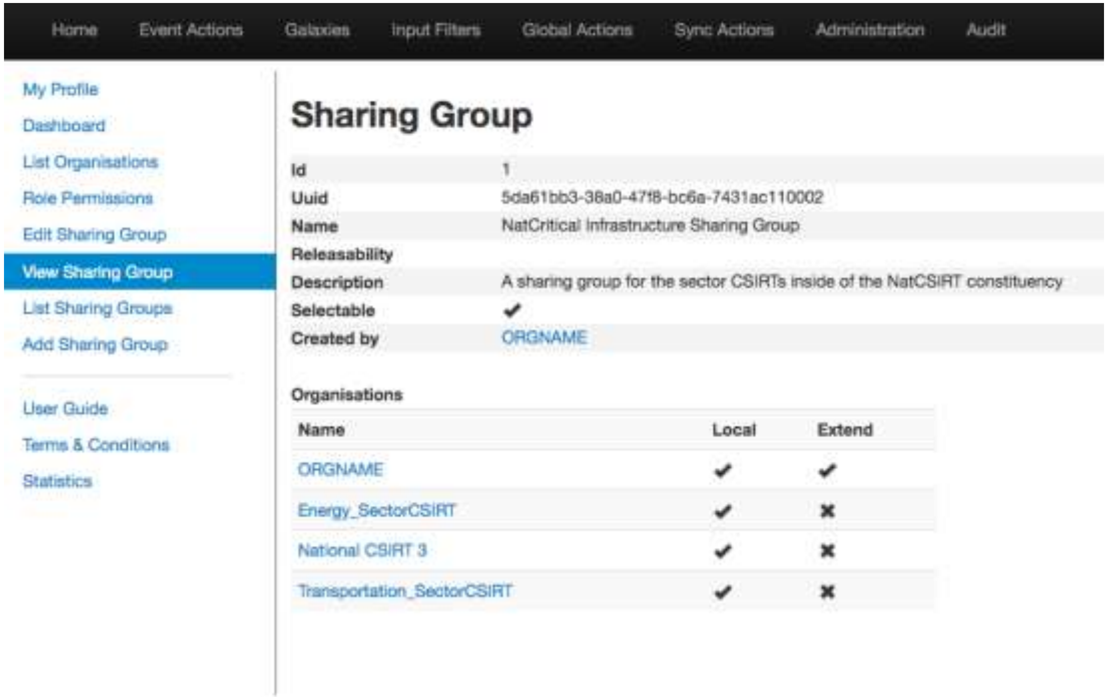
General: You are about to create the **NatCritical Infrastructure Sharing Group** sharing group, which is intended to be releasable to **[Sharing group releasability not set!]**.

Local organisations: It will be visible to **all organisations on this instance**, from which **ORGNAME** can extend the sharing group.

Synchronisation: Furthermore, events are automatically pushed to: **any interconnected instances linked by an eligible organisation.**

You can edit this information by going back to one of the previous pages, or if you agree with the above mentioned information, click Submit to create the Sharing group.

View Sharing Group



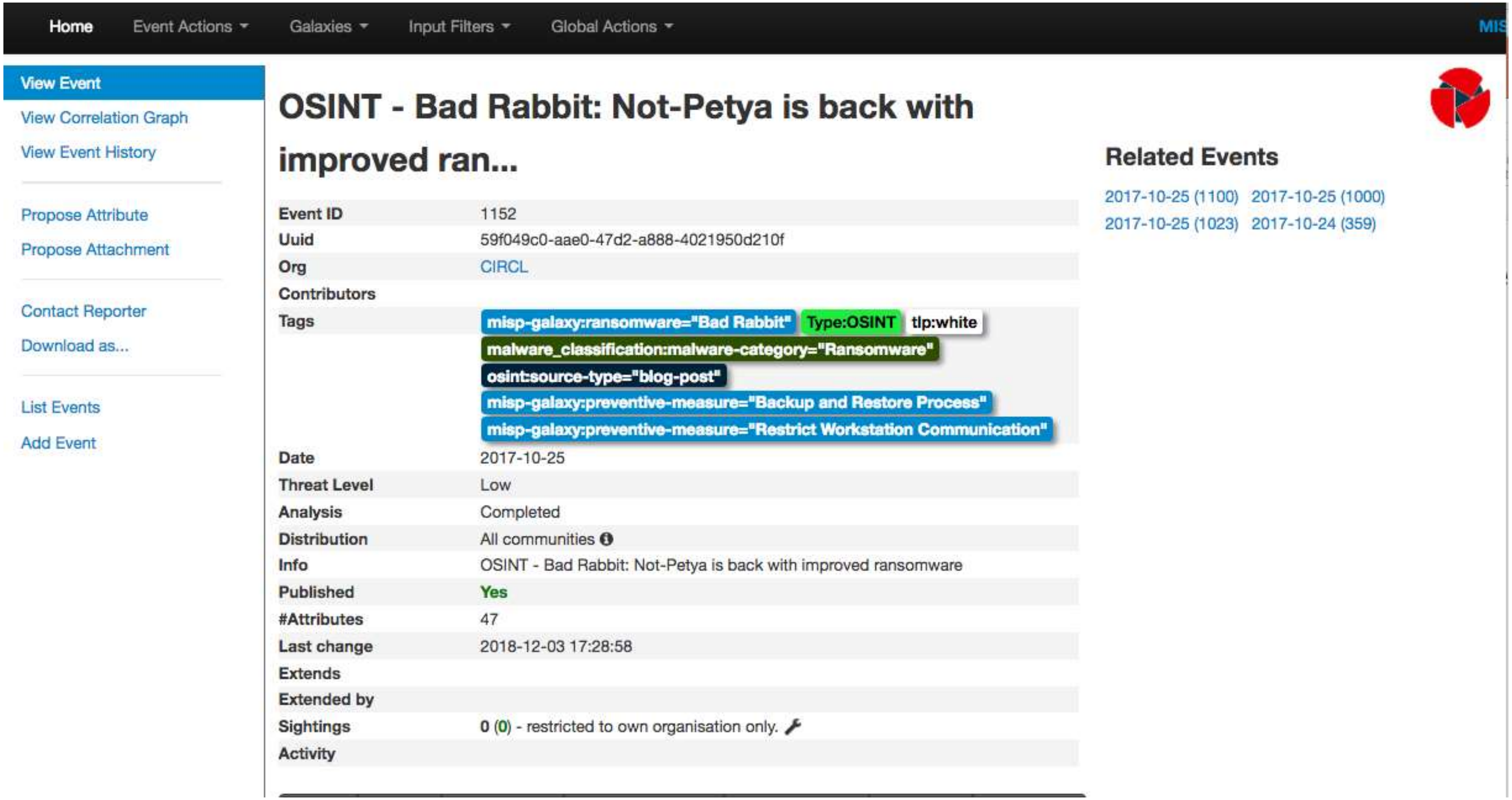
Sharing Group

Id	1
Uuid	5da61bb3-38a0-47f8-bc6a-7431ac110002
Name	NatCritical Infrastructure Sharing Group
Releasability	
Description	A sharing group for the sector CSIRTs inside of the NatCSIRT constituency
Selectable	✓
Created by	ORGNAME

Organisations

Name	Local	Extend
ORGNAME	✓	✓
Energy_SectorCSIRT	✓	✖
National CSIRT 3	✓	✖
Transportation_SectorCSIRT	✓	✖

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



OSINT - Bad Rabbit: Not-Petya is back with improved ran...

Event ID	1152
Uuid	59f049c0-aae0-47d2-a888-4021950d210f
Org	CIRCL
Contributors	
Tags	misp-galaxy:ransomware="Bad Rabbit" Type:OSINT tlp:white malware_classification:malware-category="Ransomware" osint:source-type="blog-post" misp-galaxy:preventive-measure="Backup and Restore Process" misp-galaxy:preventive-measure="Restrict Workstation Communication"
Date	2017-10-25
Threat Level	Low
Analysis	Completed
Distribution	All communities ℹ
Info	OSINT - Bad Rabbit: Not-Petya is back with improved ransomware
Published	Yes
#Attributes	47
Last change	2018-12-03 17:28:58
Extends	
Extended by	
Sightings	0 (0) - restricted to own organisation only.
Activity	

Related Events

2017-10-25 (1100) 2017-10-25 (1000)
2017-10-24 (1023) 2017-10-24 (359)

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