



Introduction to MISP

Sam Perl,
CSIRT Development and Training Team,
CERT, SEI, Carnegie Mellon University

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Copyright 2021 Carnegie Mellon University.

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.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other use. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu.

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:

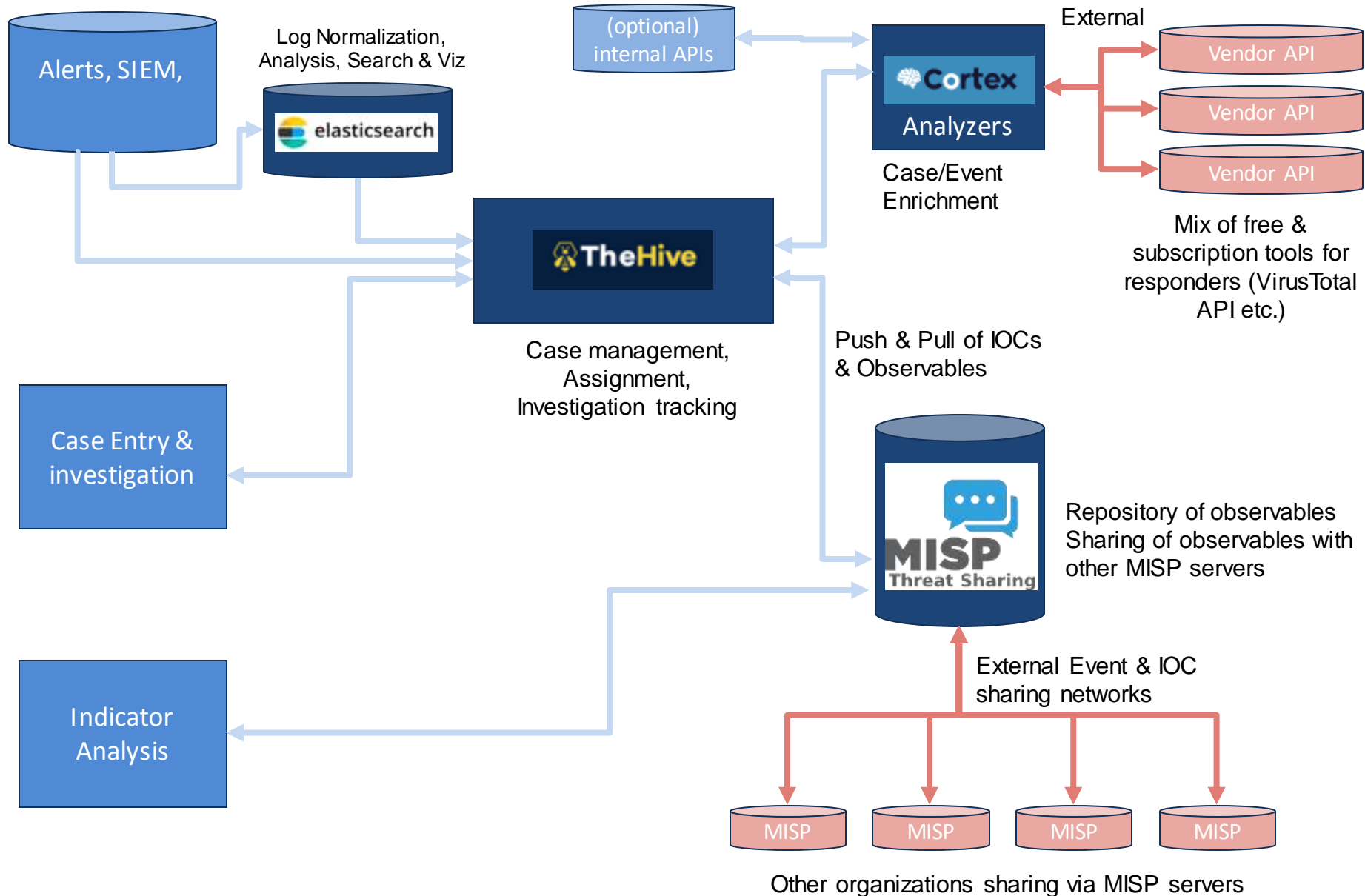
- Store, share, collaborate on cyber security indicators, malware analysis, and use to detect and prevent attacks or threats.
- Support for Events to have tags, to apply different taxonomies,
- Multi-layered Sharing groups for multiple organizations with permissions and protocols (including TLP)
- Import/Export 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



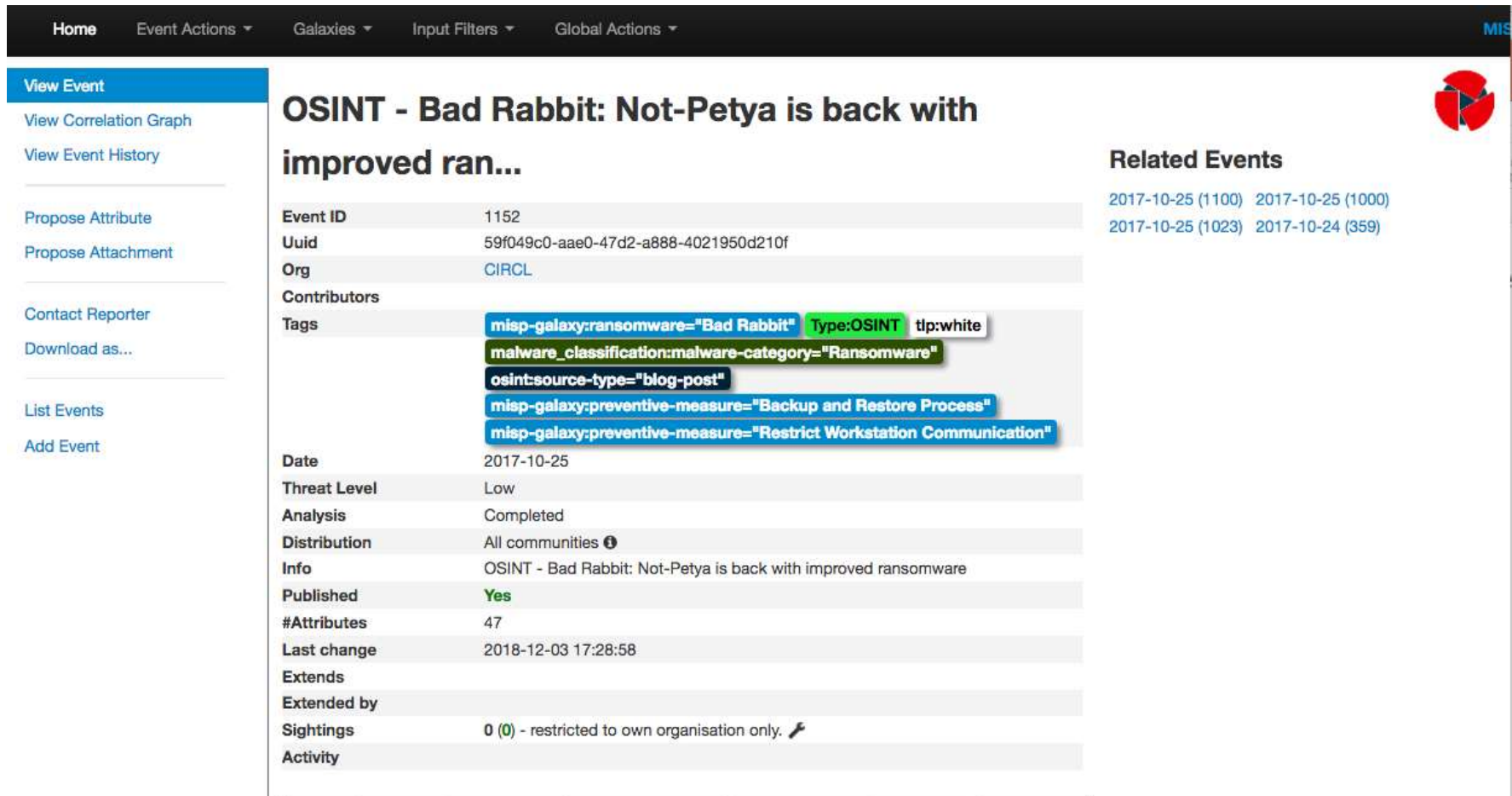
MISP – Event List

The screenshot displays the MISP (Malware Incident Response Platform) Event List interface. The top navigation bar includes links for Home, Event Actions, Galaxies, Input Filters, and Global Actions. The left sidebar contains a 'List Events' section with options like 'Add Event', 'Import from...', 'REST client', 'List Attributes', 'Search Attributes', 'View Proposals', 'Events with proposals', 'Export', and 'Automation'. The main content area, titled 'Events', shows a list of events with columns for Published status, Org, Id, Clusters, Tags, #Attr, Date, Info, Distribution, and Actions. Two events are visible: Event 1152, titled 'OSINT - Bad Rabbit: Not-Petya is back with improved ransomware', and Event 1147, titled 'OSINT - Malicious Documents Targeting Security Professionals'. Both events have a 'tlp:white' tag and are categorized as 'blog-post'.

Published	Org	Id	Clusters	Tags	#Attr	Date	Info	Distribution	Actions
✓		1152		<ul style="list-style-type: none">misp-galaxy:ransomware="Bad Rabbit"Type:OSINT tlp:whitemalware_classification:malware-category="Ransomware"osintsource-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		<ul style="list-style-type: none">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:whiteosintsource-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



The screenshot displays the MISP web interface. At the top is a navigation bar with links: Home, Event Actions, Galaxies, Input Filters, and Global Actions. On the left is a sidebar with options: View Event (selected), View Correlation Graph, View Event History, Propose Attribute, Propose Attachment, Contact Reporter, Download as..., List Events, and Add Event. The main content area shows the details of an event titled "OSINT - Bad Rabbit: Not-Petya is back with improved ran...".

Event Details:

- Event ID: 1152
- Uuid: 59f049c0-aae0-47d2-a888-4021950d210f
- Org: CIRCL
- Contributors: (empty)
- 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: (empty)
- Extended by: (empty)
- Sightings: 0 (0) - restricted to own organisation only. 🔑
- Activity: (empty)

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 mission
- 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	Related
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/301b905eb98d8d6bb559c04bbda26628a942b2c4107c07a02e8f753bdcf347c/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://osvitportal.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 



<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

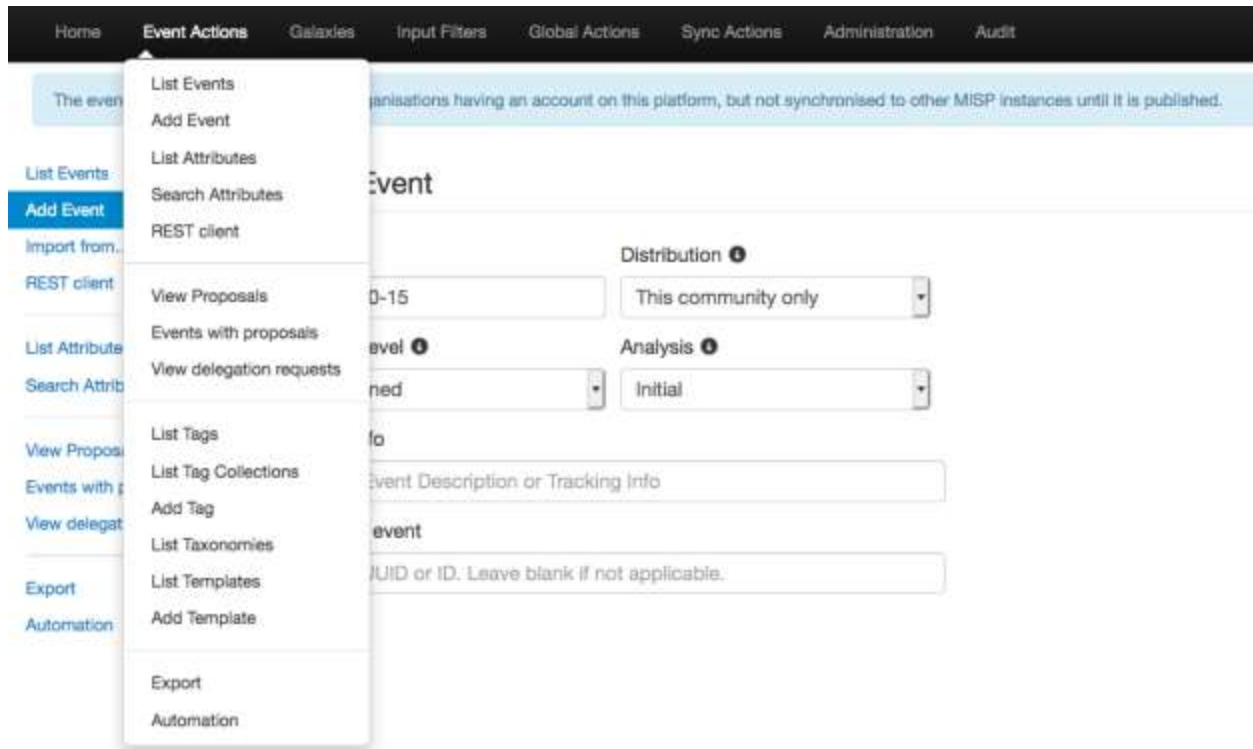


Known Existing and Public MISP Communities

- **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

[Home](#) [Event Actions](#) [Galaxies](#) [Input Filters](#) [Global Actions](#) [Sync Actions](#) [Administration](#) [Audit](#)

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.

[List Events](#)
Add Event
[Import from...](#)
[REST client](#)

[List Attributes](#)
[Search Attributes](#)

[View Proposals](#)
[Events with proposals](#)
[View delegation requests](#)

[Export](#)
[Automation](#)

Add Event

Date

2019-10-15

Threat Level ⓘ

Medium

Event Info

Quick Event Description or Tracking Info

Extends event

Event UUID or ID. Leave blank if not applicable.

Add

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

Add Event

[Home](#) [Event Actions](#) [Galaxies](#) [Input Filters](#) [Global Actions](#) [Sync Actions](#) [Administration](#) [Audit](#) [MISP](#) [Comms](#) [Log out](#)

The event has been saved






[View Event](#)
[View Correlation Graph](#)
[View Event History](#)

[Edit Event](#)
[Delete Event](#)
[Add Attribute](#)
[Add Object](#)
[Add Attachment](#)
[Populate from...](#)
[Enrich Event](#)
[Merge attributes from...](#)

[Publish Event](#)
[Publish \(no email\)](#)
[Contact Reporter](#)
[Download as...](#)

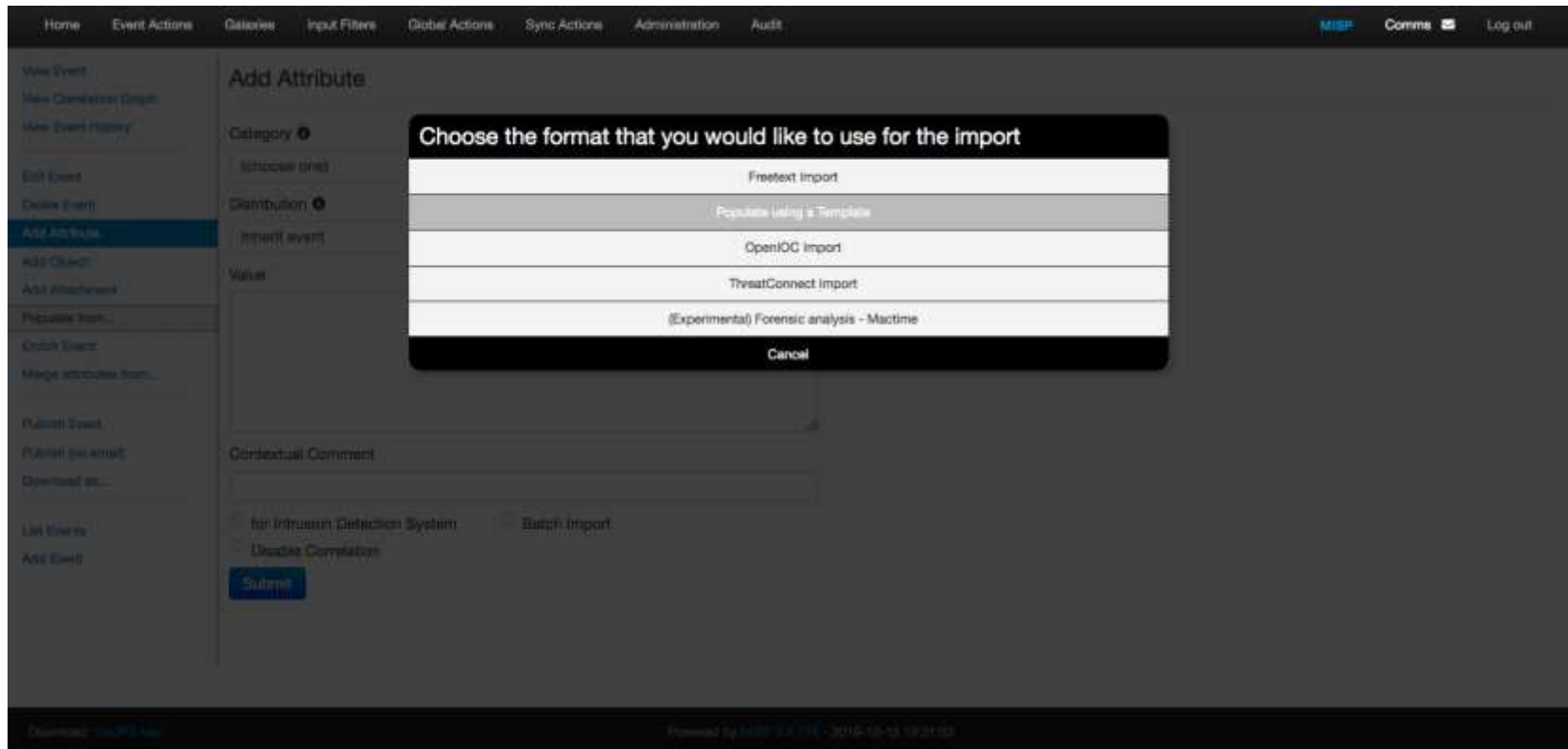
[List Events](#)
[Add Event](#)

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

Event ID	1458
UUID	5da81e3a-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: CSV/PG key](#) Powered by MISP 2.4.118 - 2019-10-15 19:30:03

Add Event – Populate Event Data from Other Data



Add Tags to Your Event – Context for Others

The screenshot displays the MISP web interface. On the left, a sidebar menu is open, showing the 'Event Actions' dropdown menu. The 'Add Tag' option is highlighted in blue. The main content area shows a detailed view of an event titled 'A BIG Event is hitting the Communications Sector right now (TEST DEMO). These ar...'. The event details include a unique ID (1428), a UUID (5d3d1c3a-da14-4b68-b89f-7494a0110000), a category (Communications Sector), a contact email (comms@test.test), a date (2019-10-15), a priority (High), and a status (Ongoing). The event is set to 'This community only'. Below the details, there is a 'Modification map' showing a single change, and a 'Signings' section indicating 0 signatures. At the bottom, there is a 'Galaxies' section with a search bar and a '1428: A BIG...' button. The footer of the interface shows the version (MISP 2.4.119) and the timestamp (2019-10-15 19:43:00).

Add Attributes to Your Event IOCs and External Analysis

The screenshot displays the 'Freetext Import Results' page in the MISP interface. The page has a dark header with navigation links: Home, Event Actions, Outcomes, Input Filters, Global Actions, Type Actions, Administration, and Audit. On the right of the header are links for 'MISP', 'Comms', and 'Log out'.

On the left, a sidebar contains a 'Freetext Import Result' section with links: View Event, View Correlation Graph, View Event History, Edit Event, Delete Event, Add Attribute, Add Object, Add Attachment, Populate from..., Enrich Event, Merge attributes from..., Propose Attribute, Propose Attachment, Download as..., List Events, and Add Event.

The main content area is titled 'Freetext Import Results' and includes a warning: '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'. Below the warning is a checkbox for 'Proposals instead of attributes'.

A table lists the imported attributes:

Value	Similar Attributes	Category	Type	IDS	Disable Correlation	Distribution	Comment	Tags	Action
https://www.smeeye.com/blog/threat-research/2018/10/mahalo-f	1390	External analysis	url	<input type="checkbox"/>	<input type="checkbox"/>	Inherit event			<input type="checkbox"/>
https://www.virustotal.com/gui/file/15cc54a2fbdadfa317b6eeb0		External analysis	file	<input type="checkbox"/>	<input type="checkbox"/>	Inherit event			<input type="checkbox"/>

Below the table is a 'Submit attributes' button. At the bottom right, there is a text input field for 'Update all comment fields' and a 'Change all' button.

The footer of the interface shows 'Download: GnuPG key' on the left and 'Powered by MISP 2.4.119 - 2019-10-10 18:03:10' on the right.

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

The screenshot displays the MISP web interface. The top navigation bar includes links for Home, Event Actions, Galleries, Input Filters, Global Actions, Sync Actions, Administration, and Audit. The left sidebar contains links for Contact Reporter, Download as..., List Events, and Add Event.

The main content area shows the details of a specific event. At the top, a red bar indicates the event is 'Published' and 'No' (likely No Correlation). Below this, fields show 'Attributes: 3 (0 Object)', 'First recorded change: 2019-10-15 19:37:04', 'Last change: 2019-10-15 19:37:04', and 'Sightings: 0 (0) - restricted to own organisation only'. A 'Modification map' is also visible.

Below the event details, there are tabs for 'Pictures', 'Gallery', 'Event graph', 'Correlation graph', 'ATT&CK matrix', 'Attributes', and 'Discussion'. The 'Event graph' tab is selected, showing a graph with one node labeled '1458: A SIG...'. Below the graph is a 'Galaxies' section with a search bar and a 'view all' link.

The bottom section shows a table of related events. The table has columns for Date, Org, Category, Type, Value, Tags, Galaxies, Comment, Correlate, and Related Events. Three events are listed, all dated 2019-10-15:

Date	Org	Category	Type	Value	Tags	Galaxies	Comment	Correlate	Related Events
2019-10-15	sho256	Payload delivery	sha256	18cc64e27bdad3a317b6e6c2b7d33875cc8f010a810889d7b6b030f02b05					1390
2019-10-15	url	External analysis	url	https://www.5nays.com/blog/threat-research/2019/10/nahalo-5n7-responding-to-new-tactic-and-techniques.html					1390
2019-10-15	link	External analysis	link	https://www.virusotal.com/gafile/18cc64e27bdad3a317b6e6c2b7d33875cc8f010a810889d7b6b030f02b05/detection					

A tooltip is visible over the 'Related Events' column, showing details for the first event: 'Org: OUGEDD', 'Date: 2019-10-10', 'Info: Malware-Fix: Responding to the Criminal Operations' New Tools and Techniques', and 'Correlating Value: 18cc64e27bdad3a317b6e6c2b7d33875cc8f010a810889d7b6b030f02b05'.

The footer of the interface shows 'Powered by MISP 2.4.118 - 2019-10-15 19:37:05'.

Publish Events

The screenshot displays a web-based security event management system. The main header includes navigation links: Home, Event Actions, Basics, Input Filters, Global Actions, Syslog Actions, Administration, and Audit. The user is logged in as 'misp' with a 'Comme' profile and a 'Log out' option.

The central area shows a list of events. The selected event is titled 'A BIG Event is hitting the Communications Sector right now (TEST DEMO). These ar...'. The event details are as follows:

- Event ID: 1458
- UUID: 50d7f8e0-0514-40b0-b0b0-7d4b0e0e0e0e
- Creator org: Communications Sector
- Owner org: Communications Sector
- Email: comms@b0b0.b0b0
- Type: [Icon] [Icon] [Icon]
- 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: 3 (2 shared)
- First received change: 2019-10-15 18:20:58
- Last change: 2019-10-15 18:20:58
- Modifications: 0
- Signings: 0 (0 - needed to show signature only)

A 'Publish Event' dialog box is overlaid on the event details, asking: 'Are you sure this event is complete and everyone should be informed?'. It has 'Yes' and 'No' buttons.

The right sidebar shows 'Related Events' with a link to 'Security T107: Responding to the Critical Operations Team Data and Security'.

The bottom of the interface shows a 'Timeline' section and a footer with the text 'Powered by MISP - 2.12.102 - 2019-10-15 18:21:01'.

Organization List

Home | Event Actions | Schedules | Input Filters | Global Actions | Sync Actions | Administration | Audit

Admin | Log out

Add User | List Users | Contact Users

Add Organisation

List Organisations

Add Role | List Roles | Server Settings & Maintenance | Update Progress | Jobs | Scheduled Tasks | Backlogs Event | Manage Event Backlogs | Backlogs Organisation | Manage Org Backlogs

Local organisations having a presence on this instance

[+ previous](#) [next >](#) [View all](#)

Local organisations			Known remote organisations			All organisations			Enter value to search				Filter
ID	Logo	Name	UUID	Description	Nationality	Sector	Type	Contacts	Added by	Local	Users	Restrictions	Actions
22		Energy_SectorCSIRT	Sdbf1260-9a58-4294-00e0-7480ac110002	A demo CSIRT for the energy Sector	Not specified				admin@admin.test	Yes	1		✕ 📄 🔍
21		National CSIRT	5cb810c7-42ec-48f4-a296-8090ac110002	A national CSIRT for demonstration purposes	Not specified				admin@admin.test	Yes	1		✕ 📄 🔍
1		ORGNAME	5b809eb7-da30-4709-b039-00a7ac110002	Automatically generated admin organisation	Not specified		ADMIN		Unknown	Yes	1		✕ 📄 🔍
23		Transportation_SectorCSIRT	Sdbf1355-c5d4-4790-91d5-7430ac110002	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

[+ previous](#) [next >](#) [View all](#)

Download: [SQLPDS key](#)

Powered by MISP 2.6.119 • 2019-05-15 19:21:54

Create New Sharing Group

The screenshot shows a web application interface for creating a new sharing group. At the top is a dark navigation bar with links: Home, Event Actions, Galaxies, Input Filters, Global Actions, Sync Actions, Administration, and Audit. On the left is a sidebar menu with links: My Profile, Dashboard, List Organisations, Role Permissions, List Sharing Groups, Add Sharing Group (highlighted in blue), User Guide, Terms & Conditions, and Statistics. The main content area is titled 'New Sharing Group' and contains a form with four tabs: General (selected), Organisations, MISP Instances, and Summary and Save. The form fields are: Name (text input with value 'NatCritical Infrastructure Sharing Group'), Releasable to (text input with placeholder 'Example: Community1, Organisation1, Organisation2'), and Description (text area with value 'A sharing group for the sector CSIRTs inside of the NatCSIRT constituency'). At the bottom of the form is a checkbox labeled 'Make the sharing group selectable (active)' which is checked, and a 'Next page' button.

Home Event Actions Galaxies Input Filters Global Actions Sync Actions Administration Audit

My Profile
Dashboard
List Organisations
Role Permissions
List Sharing Groups
Add Sharing Group
User Guide
Terms & Conditions
Statistics

New Sharing Group

General Organisations MISP Instances Summary and Save

Name
NatCritical Infrastructure Sharing Group

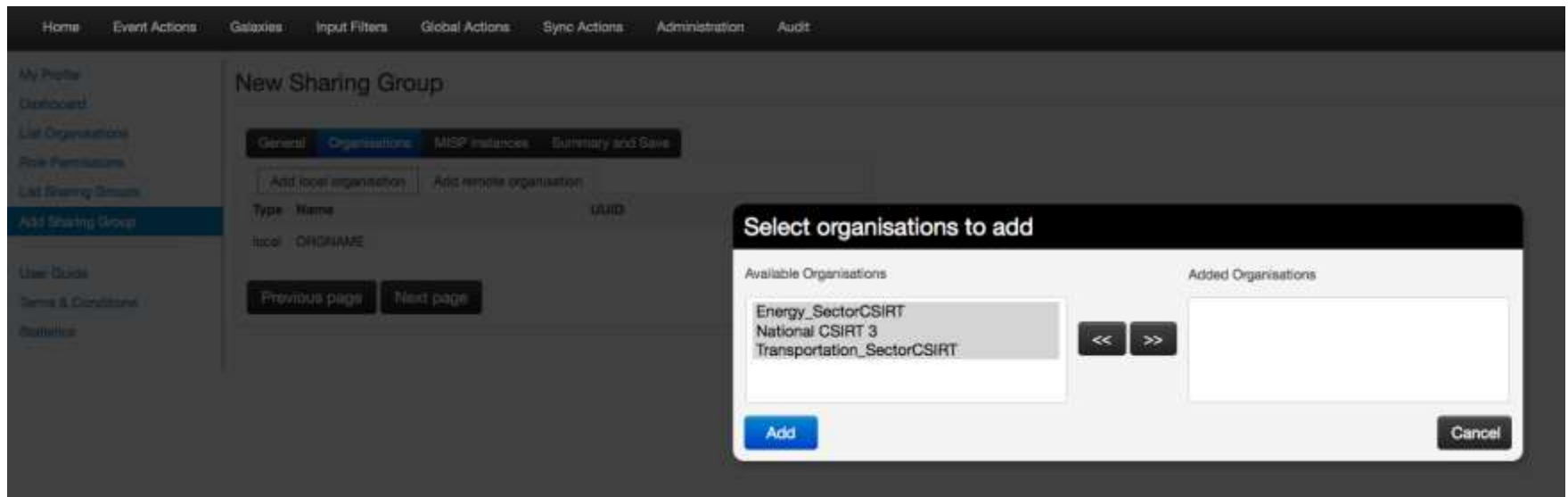
Releasable to
Example: Community1, Organisation1, Organisation2

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

☒ Make the sharing group selectable (active)

Next page

Add Local Organizations



Confirm Sharing Group You Want to Add

[Home](#) [Event Actions](#) [Galaxies](#) [Input Filters](#) [Global Actions](#) [Sync Actions](#) [Administration](#) [Audit](#)

[My Profile](#)
[Dashboard](#)
[List Organisations](#)
[Role Permissions](#)
[List Sharing Groups](#)
[Add Sharing Group](#)
[User Guide](#)
[Terms & Conditions](#)
[Statistics](#)

New Sharing Group

[General](#) [Organisations](#) [MISP Instances](#) [Summary and Save](#)

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.

[Previous page](#) [Submit](#)

View Sharing Group

[Home](#) [Event Actions](#) [Galaxies](#) [Input Filters](#) [Global Actions](#) [Sync Actions](#) [Administration](#) [Audit](#)

[My Profile](#)
[Dashboard](#)
[List Organisations](#)
[Role Permissions](#)
[Edit Sharing Group](#)
[View Sharing Group](#)
[List Sharing Groups](#)
[Add Sharing Group](#)

[User Guide](#)
[Terms & Conditions](#)
[Statistics](#)

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

The screenshot displays the MISP web interface. The top navigation bar includes links for Home, Event Actions, Galaxies, Input Filters, and Global Actions. On the left, a sidebar under 'View Event' offers options like 'View Correlation Graph', 'View Event History', 'Propose Attribute', 'Propose Attachment', 'Contact Reporter', and 'Download as...'. The main content area shows the details for an event titled 'OSINT - Bad Rabbit: Not-Petya is back with improved ran...'. The event information includes:

- Event ID:** 1152
- Uuid:** 59f049c0-aae0-47d2-a888-4021950d210f
- Org:** CIRCL
- Contributors:** (empty)
- Tags:** misp-galaxy:ransomware="Bad Rabbit" (Type:OSINT, tlp:white), malware_classification:malware-category="Ransomware", osintsource-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:** (empty)
- Extended by:** (empty)
- Sightings:** 0 (0) - restricted to own organisation only.
- Activity:** (empty)

On the right, a 'Related Events' section lists other events from the same date and time, such as '2017-10-25 (1100)' and '2017-10-25 (1000)'.

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