

MISP: Introduction, Concepts and Guide

This eLearning module is a prerequisite or refreshing module to read before the actual training sessions. This helps to ensure that all participants are inline with the basic knowledge of MISP. In the training modules, the various elements mentioned in this introduction will be completed in details (e.101-104, e.205-e.206 and e.302-e.304).

Structure of this document

1. **MISP Introduction:** The what, why and how about MISP
2. **MISP Basics:** A concise introduction to MISP data model
3. **How-to:** A user guide with screenshots on how to use MISP to encode and share data

MISP Introduction

What is MISP

MISP is an open-source threat-intelligence and sharing platform meant to store, correlate, enrich, analyse and share information. It enables the various type of analysts to collaborate on investigations and incidents, perform intelligence as well as helping operators to automatically feed their protective tools.

Why is MISP relevant

Information sharing is becoming more essential than ever to oppose threats. MISP strive to be the enabler and interface for real cross-sectoral sharing and support the organisations facing hybrid threats. To achieve these goals, MISP uses a practical information sharing format expressed in JSON which is built from a practical use-cases. It is flexible and can be easily extended by users to model their own data-structure.

The MISP core format as well as the common set of vocabularies provided by the various libraries supported by the tool allows users from all around the world to understand each others and rely on normalized data, making MISP a central place to collaborate.

MISP offers different alternatives to share analysis, case and report enabling users to review data produced by partners or third-parties and propose changes if need be. This happens in a decentralized way where analyst can evaluate correlation against other existing evidences and perform enrichment on the data.

These functionnalities provide the means to fulfill the ultimate goal of MISP: Bridging communities together. By fostering communication and sharing accross multiple sectors, people are able to share and collaborate seemlessly making the connection between law enforcement with CSIRTs possible.

MISP philosophy

Sharing being the principal functionnality, it is essential that everyone is able to send and receive data. As such, everyone is considered to be a producer (also called contributor) and/or a consumer at the same time. There are strictly no obligation to contribute which in turns makes the system to have a low barrier of access for users to get acquainted to the system.

MISP Basics

A cheat-sheet describing the core concepts and data-models in MISP is available [here](#).

1.1 Data Layer

First and foremost, it's important to understand how MISP is organised. Similar to all applications, some predefined data structure exists and are used to represent and save the actual data on the disk. Such structure in MISP could be for example *Attributes* or *MISP Objects*.

MISP Attributes *Attributes* are individual block containing the very information to be used or to be shared. Thanks to their characteristic called **type**, *Attributes* can represent concept such as an IP address, a domain name or cryptographic hash. In addition to having a **type** and a **value**, they can express if they are Indicators of Compromise (IoC) or supporting data where for example, the former could be a hash of a malicious binary and the later could be Observed behaviour or links toward documentation. The differentiation between IoC and observable can be done by flipping the *Attribute's to_ids* flag.

<input type="checkbox"/> 2021-11-25	Payload delivery	ip-src	118.217.182.3
<input type="checkbox"/> 2021-11-25	Payload delivery	url	https://evilprovider.com/this-is-not-malicious.exe

Figure 1: attributes

MISP Objects In most of the case, these individual blocks of information can be combined together into a more elaborated concept. When multiple *Attributes* are grouped, they form another entity that is called a *MISP Object*. For example, a *File Object* contains multiple *Attributes* such as the filename, its size, its name and so on.

By their very nature, *MISP Objects* organise and facilitate the reading of data in the application. But their efficiency can be improved even more when you add the capability to link them together with relationships to create directed graph allowing to represent stories, processes or behaviours. In MISP, creating such connections is called “create an *Object Reference*”. Viewing these relationships as a connected graph can be done by looking at the widget called *Event Graph*.

2021-12-09	Object name: file []
	References: 1 [] +
	Referenced by: 1 []
<input type="checkbox"/> 2021-12-09	Payload delivery malware-sample: malware-sample
	malicious.exe f1a3e62de12faecee82bf4599cc1fdcd
<input type="checkbox"/> 2021-12-09	Payload delivery filename: filename
	malicious.exe
<input type="checkbox"/> 2021-12-09	Payload delivery md5: md5
	f1a3e62de12faecee82bf4599cc1fdcd ⓘ
<input type="checkbox"/> 2021-12-09	Payload delivery sha1: sha1
	d836f2ee449b74913d1efc615eeb459b65e4f791 ⓘ
<input type="checkbox"/> 2021-12-09	Payload delivery sha256: sha256
	d90401420908dbb4b3488a306467e8ffc57577ce9d5eee016578ff6a3ada1 2e ⓘ
<input type="checkbox"/> 2021-12-09	Other size-in-bytes: size-in-bytes
	751328

Figure 2: objects

MISP Events Now that we have the structures to encode information, we need another structure to be able to group them together in order to avoid dealing with a soup of *Attributes* and *MISP Objects*. *MISP Events* or commonly called *Events* are envelopes allowing to assemble *Attributes* and *Objects* contextually linked. Typically, *Events* are used to encode incidents, events or reports.

Threat Intelligence Tools: Event Graph, Event Timeline and Event Reports

MISP Event Graph The MISP *Event Graph* feature is a widget accessible when viewing an *Event*. It allows analysts to visualise or create relationships between different entities in order to describe in a concise manner complex scenarios such as events performed in parallel or multiple-step attacks.

MISP Event Timeline In some situation, temporality is crucial to understand the order of events, actions or processes. To help analysts visualise and adjust the time component of *Attributes* or *Objects*, a complete timeline viewer and editor is available allowing users to describe complex time-based information.

View Event

View Correlation Graph

View Event History

Edit Event

Delete Event

Add Attribute

Add Object

Add Attachment

Add Event Report

Populate from...

Enrich Event

Merge attributes from...

Propose Attribute

Propose Attachment

Publish Event

Publish (no email)

Delegate Publishing

Publish event to ZMQ

Download as...

List Events

Add Event

Event example

Event ID 15

UUID ca1d856f-86de-4819-889a-f5a107ac16cc

Creator org Training

Owner org ORGNAME

Creator user admin@admin.test

Tags tip:white x osint:lifetime="perpetual" x osint:certainity="50" x workflow.state="draft" x smo:sync x +

Date 2021-11-25

Threat Level High

Analysis Initial

Distribution Your organisation only

Info Event report example

Published No

#Attributes 12 (1 Object)

First recorded change 2021-11-25 10:26:27

Last change 2022-03-04 06:26:43

Modification map

Sightings 0 (0) - restricted to own organisation only.

+Pivots +Galaxy +Event graph +Event timeline +Correlation graph +ATT&CK matrix +Event reports -Attributes -Discussion

< previous next > view all

Scope toggle Deleted Decay score SightingDB Context Related Tags Filtering tool

Date	Org	Category	Type	Value	Tags	Galaxies	Comment	Correlate	Related Events	Feed hits	IDS	Distribution	Sightings	Activity	Actions
2022-03-04		Object name: file		References: 0								Inherit			
2022-03-04		Payload delivery	md5:	cf524cea4cd82a222670c6a7b18c966								Inherit			
			md5												
2021-11-25		Payload delivery	filename:	malware.exe								Inherit			

Enter value to search

Figure 3: event

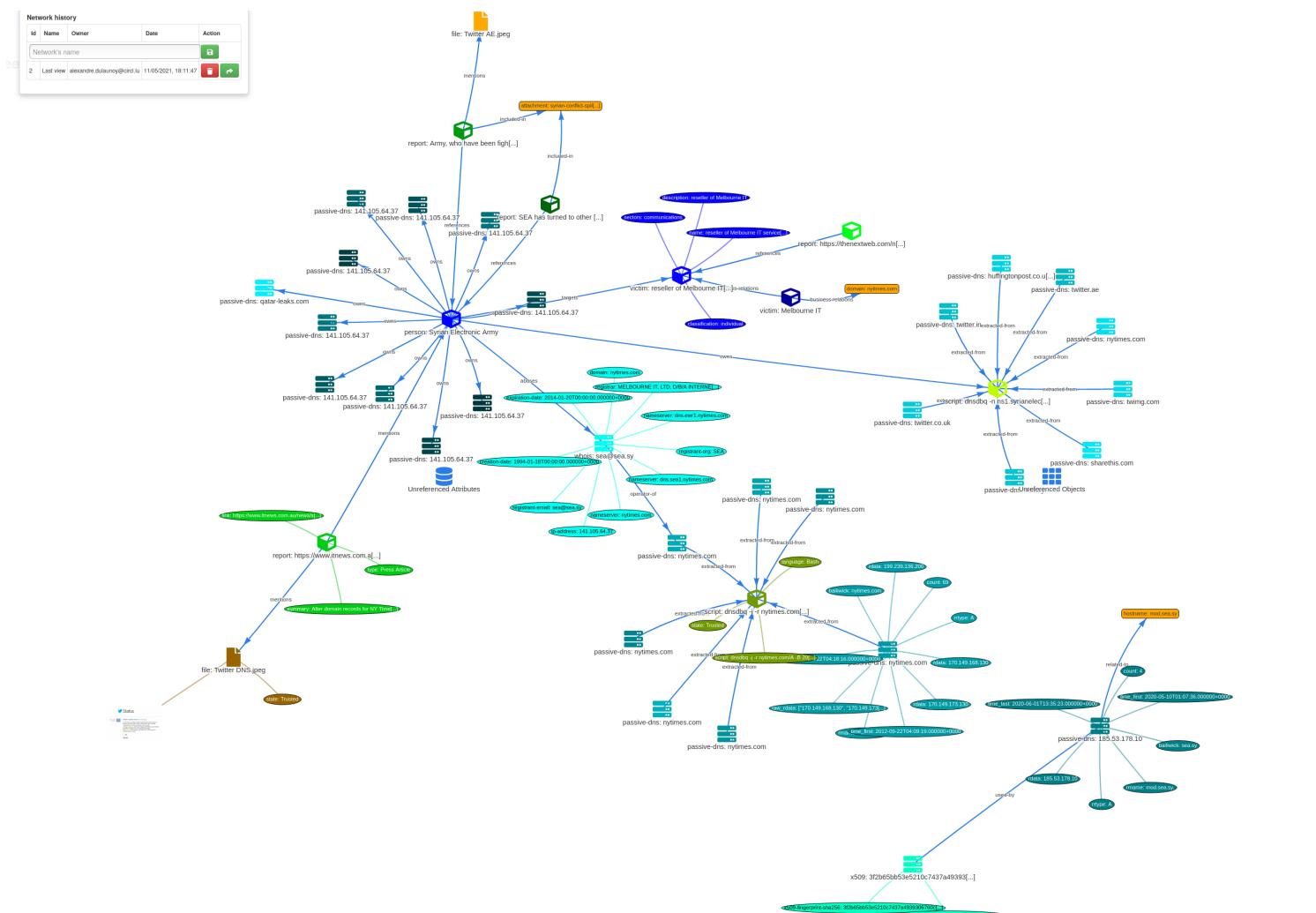


Figure 4: event-graph

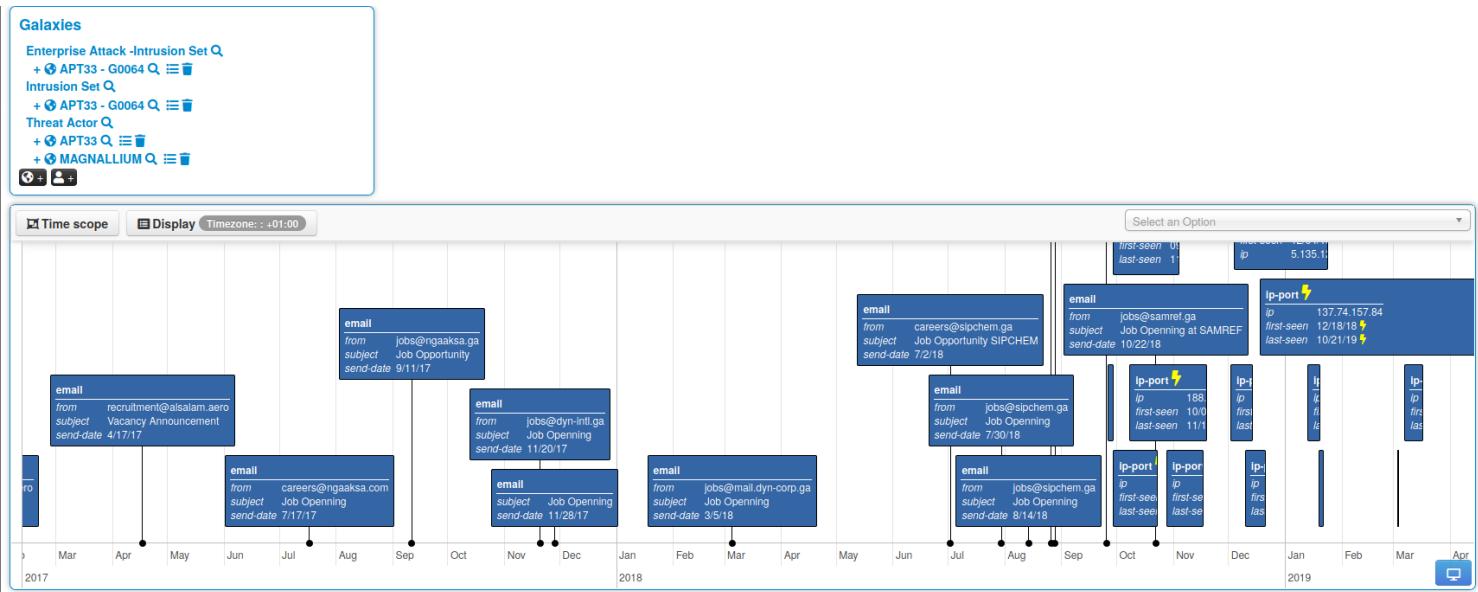


Figure 5: event-timeline

MISP Event Reports In addition to encode data into pre-formatted structure, MISP offers a tool to write report. Such report are called *Events reports* and are contained in an *Event* where they use the markdown syntax to write formatted text. They also provide directives specific to MISP allowing writers to reference other entities contained in the *Event*. This extended syntax supports referencing *Attributes*, *Objects*, *Tags* and *Galaxy Clusters*.

1.2 Context Layer

One of the most critical aspects often left aside is contextualisation. If done properly, it allows the reader to know more about where this data comes from, what it is about, how relevant it is for the user and finally, what can be done with it.

In MISP, contextualising data is as simple as attaching a label to the relevant entity. However, choosing the right labels is the difficult part. We can distinguish two types of labels: *Tags* and *Galaxy Clusters*.

Tags *Tags* are simple labels coming from a curated list of vocabulary (Also called *Taxonomy*). They are mainly used to classify data in order to ease data consumption and automation. For example, the following *Tags* can be used to quickly classify information: - **tlp**: Allow a favorable classification scheme for sharing sensitive information while keeping the control over its distribution at the same time. - **adversary**: An overview and description of the adversary infrastructure and allowed actions - **collaborative-intelligence**: Common language to support analysts to perform their analysis. The objective of this language is to advance collaborative analysis and to share earlier than later. - **estimative-language**: Estimative language to describe quality and credibility of underlying sources, data, and methodologies

Galaxy Clusters *Galaxy Clusters* are knowledge base items having descriptions, links, synonyms and any other meta-information. *Clusters* are regrouped into a higher-level structure called *Galaxy*. *Clusters* enable analysts to assign complex high-level contextual information to data-structures. Example of *Galaxy Clusters*:

- **threat-actor="Sofacy"** having information such as suspected-state-sponsor, victims, links-to-documentation, target-category and synonyms.
- **country="Luxembourg"** having information such as country-code, languages, TLD, Capital and so on.

MITRE's ATT&CK Another advantage that *Galaxy Clusters* have compared to simple labels is the fact that the list of *Clusters* belonging to the same *Galaxy* can be arranged as a matrix to have improved readability and aggregation. One of the biggest success of this kind of matrices is definitely the MITRE ATT&CK framework. It describes tactics, techniques and procedures of adversaries. ATT&CK is very popular and its usage is highly recommended as it offers very precise classification and is globally understood and supported by other tools.

1.3 Anatomy of a complete Event

1.4 Distribution Levels

Distribution level is the term used in MISP to determine who can read which data and how it should be shared. The distribution can be set on entities such as *Event* or *Attributes*, where the most restrictive priority will always take priority.

Event report: Winnti Group targeting universities in Hong Kong

[Markdown](#) [Raw](#) [Edit report](#)

This report is an excerpt meant for demo purposes. The full report can be found online at [link https://www.welivesecurity.com/2...](https://www.welivesecurity.com/2...)

Winnti Group targeting universities in Hong Kong

In November 2019, we discovered a new campaign run by the Winnti Group [threat-actor Axiom](#) against two Hong Kong universities. We found a new variant of the ShadowPad backdoor [malpedia ShadowPad](#), the group's flagship backdoor, deployed using a new launcher and embedding numerous modules. The Winnti malware was also found at these universities a few weeks prior to ShadowPad.

ShadowPad found at several Hong Kong universities

In November 2019, ESET's machine-learning engine, Augur, detected a malicious and unique sample present on multiple computers belonging to two Hong Kong universities where the Winnti malware had already been found at the end of October. The suspicious sample detected by Augur is actually a new 32-bit ShadowPad launcher. Samples from both ShadowPad and Winnti found at these universities contain campaign identifiers and C&C URLs with the names of the universities, which indicates a targeted attack.

In addition to the two compromised universities, thanks to the C&C URL format used by the attackers we have reasons to think that at least three additional Hong Kong universities may have been compromised using these same ShadowPad and Winnti variants.

DLL side-loading

The launcher is a 32-bit DLL named [file hpqhsvei.dll](#) which is the name of a legitimate DLL loaded by [filename %WINDIR%temp\hpqhwind.exe](#). This executable is from HP and is usually installed with their printing and scanning software called [HP Digital Imaging](#). In this case the legitimate [filename %WINDIR%temp\hpqhwind.exe](#) was dropped by the attackers, along with their malicious [filename %WINDIR%temp\hpqhvsel.dll](#), in [C:\Windows\Temp](#).

When the malicious DLL is loaded at hpqhwind.exe startup, its DLLMain function is called that will check its parent process for the following sequence of bytes at offset [0x10BA](#):

```
85 C0 ; test eax, eax
0F 84 ; jz
```

In the case where the parent process is [filename %WINDIR%temp\hpqhwind.exe](#) this sequence of bytes is present at this exact location and the malicious DLL will proceed to patch the parent process in memory.

Figure 6: event-report

Name	Expanded	Numerical Value	# Events	# Attributes	Tag	Enabled	Actions
estimative-language.confidence-in-analytic-judgment="high"	Confidence in analytic judgment: High	95	15	4	estimative-language:confidence-in-analytic-judgment="high"	✓	edit delete
estimative-language.confidence-in-analytic-judgment="low"	Confidence in analytic judgment: Low	0	9	0	estimative-language:confidence-in-analytic-judgment="low"	✓	edit delete
estimative-language.confidence-in-analytic-judgment="moderate"	Confidence in analytic judgment: Moderate	55	26	4	estimative-language:confidence-in-analytic-judgment="moderate"	✓	edit delete
estimative-language.likelihood-probability="almost-certain"	Likelihood or probability: Almost certain(ly) - nearly certain - 95-99%	95	21	8	estimative-language:likelihood-probability="almost-certain"	✓	edit delete
estimative-language.likelihood-probability="almost-no-chance"	Likelihood or probability: Almost no chance - remote - 01-05%	0	0	0	estimative-language:likelihood-probability="almost-no-chance"	✓	edit delete
estimative-language.likelihood-probability="likely"	Likelihood or probability: Likely - probable (probably) - 55-80%	55	4	5	estimative-language:likelihood-probability="likely"	✓	edit delete
estimative-language.likelihood-probability="roughly-even-chance"	Likelihood or probability: Roughly even change - roughly even odds - 45-55%	45	4	2	estimative-language:likelihood-probability="roughly-even-chance"	✓	edit delete
estimative-language.likelihood-probability="unlikely"	Likelihood or probability: Unlikely - Improbable (improbably) - 20-45%	20	0	1	estimative-language:likelihood-probability="unlikely"	✓	edit delete
estimative-language.likelihood-probability="very-likely"	Likelihood or probability: Very likely - highly probable - 80-95%	80	23	18	estimative-language:likelihood-probability="very-likely"	✓	edit delete
estimative-language.likelihood-probability="very-unlikely"	Likelihood or probability: Very unlikely - highly improbable - 05-20%	5	0	1	estimative-language:likelihood-probability="very-unlikely"	✓	edit delete

Figure 7: taxonomy

Country :: luxembourg

Name	luxembourg
Parent Galaxy	Country
Description	Luxembourg
Version	1
UUID	84668357-5a8c-4bdd-9f0f-6b50b24c5558
Source	MISP Project
Authors	geonames.org
Distribution	All communities
Creator Organisation	MISP
Connector tag	misp-galaxy:country="luxembourg"
Events	11 events

« previous next »

Tabular view JSON view

Key	Value	Actions
Capital	Luxembourg	
Continent	EU	
CurrencyCode	EUR	
CurrencyName	Euro	
ISO	LU	
ISO3	LUX	
Languages	lb,de-LU,fr-LU	
Population	497538	
tld	.lu	

Figure 8: cluster-country

Initial access	Execution	Persistence	Privilege escalation	Defense evasion	Credential access	Discovery	Lateral movement	Collection	Exfiltration	Command and control
Spearphishing Attachment	Scripting	Screensaver	File System Permissions Weakness	Process Hollowing	SecurityId Memory	Password Policy Discovery	AppleScript	Data from Information Repositories	Exfiltration Over Alternative Protocol	Standard Application Layer Protocol
Spearphishing via Service	Command-Line Interface	Login Item	AppCert DLLs	Code Signing	Input Capture	System Network Configuration Discovery	Distributed Component Object Model	Data from Removable Media	Exfiltration Over Command and Control Channel	Communication Through Removable Media
Trusted Relationship	User Execution	Trap	Application Shimming	Rootkit	Bash History	Process Discovery	Pass the Hash	Man in the Browser	Data Compressed	Custom Command and Control Protocol
Replication Through Removable Media	Regsvcs/Regasm	System Firmware	Scheduled Task	NTFS File Attributes	Exploitation for Credential Access	Network Share Discovery	Exploitation of Remote Services	Data Staged	Automated Exfiltration	Multi-Stage Channels
Exploit Public-Facing Application	Trusted Developer Utilities	Registry Run Keys / Start Folder	Startup Items	Exploitation for Defense Evasion	Private Keys	Peripheral Device Discovery	Remote Desktop Protocol	Screen Capture	Scheduled Transfer	Remote Access Tools
Spearphishing Link	Windows Management Instrumentation	LC_LOAD_DYLIB Addition	New Service	Network Share Connection Removal	Brute Force	Account Discovery	Pass the Ticket	Email Collection	Data Encrypted	Uncommonly Used Port
Valid Accounts	Service Execution	LSASS Driver	Sudo Caching	Process Doppelgänging	Password Filter DLL	System Information Discovery	Windows Remote Management	Clipboard Data	Exfiltration Over Other Network Medium	Multi-layer Encryption
Supply Chain Compromise	CMSTP	Rc.common	Process Injection	Disabling Security Tools	Two-Factor Authentication Interception	System Network Connections Discovery	Windows Admin Shares	Video Capture	Exfiltration Over Physical Medium	Domain Fronting
Drive-by Compromise	Control Panel Items	Authentication Package	Bypass User Account Control	Timestamp	LLMNR/NBT-NS Poisoning	Network Service Scanning	Remote Services	Audio Capture	Data Transfer Size Limits	Data Obfuscation
Hardware Additions	Dynamic Data Exchange	Component Firmware	Extra Window Memory Injection	Modify Registry	Credentials in Files	File and Directory Discovery	Taint Shared Content	Data from Network Shared Drive		Connection Proxy
	Source	Windows Management Instrumentation Event Subscription	Setuid and Setgid	Indicator Removal from Tools	Forced Authentication	Security Software Discovery	Application Deployment Software	Data from Local System		Commonly Used Port
	Space after Filename	Change Default File	Launch Daemon	Hidden Window	Keychain	System Service Discovery	Third-party Software	Automated Collection		Data Encoding

Figure 9: cluster-country

Failed spear-phishing attempt

UUID 28b1cd2e-46a7-4ee2-a364-c3d26451b089

Date 2021-12-09

Creator Org. CIRCL.lu

Distribution Connected Communities

Published ✓



> Intelligence Visualization Widgets

Event report: Email from source

We have had a failed spear-phishing attempt targeting our GSO recently with the following details:

The GSO received an E-mail on 03/02/2021 15:58 containing a personalized message about a report card for their child. The attacker pretended to be someone from the school of the GSO's daughter, sending a link from a spoofed email address to the GSO's child. After clicking on the link, the user was redirected to a website of the attacker. The email was received from from@example-mail-provider.com (197.211.196.104).

The mail contained a malicious file (not the attachments) that tried to download a secondary payload from <https://evilprovider.com/this-is-not-malicious.exe>. It looks like the sample is trying to exploit [vulnerability CVE-2019-5465](#).

After a brief investigation, the secondary payload has a hardcoded C2 at <https://evilprovider.com/pwnme.com?1>. This is a known exploit for the Microsoft Edge browser. Please be informed that this is an ongoing investigation. We would like to send information about the attack when we are ready and ask you to only use the confirmed information to protect your constituents.

Best regards,



> Attributes

2021-11-25 Payload delivery ip-src 118.217.182.3

2021-11-25 Payload delivery url <https://evilprovider.com/this-is-not-malicious.exe>

> Objects

2021-12-09	Object name: file	References: 1	Referenced by: 1
2021-12-09	Payload delivery	malware-sample: malicious.exe	malicious.exe f1a3e2d2e12fece0e82b44599cc11dd0
2021-12-09	Payload delivery	filename: filename	malicious.exe
2021-12-09	Payload delivery	md5: md5	f1a3e2d2e12fece0e82b44599cc11dd0
2021-12-09	Payload delivery	sha1: sha1	d936f2ee449b74913d1ef0d15eebd5bb5eaf791
2021-12-09	Payload delivery	sha256: sha256	d90401420908dbbfb3488a306467ef8ff75770e9d5ee016578f85a3a3da1
2021-12-09	Other	size-in-bytes: size-in-bytes	751328

Representation of an incident in MISP

Event: Encapsulates contextually linked information.

Events also have basic information including ownership and access-control
Here: Contains all the information related to the spear-phishing incident.

Taxonomies: Simple label standardised on common set of vocabularies.

Here: Usage of labels to classify the current completeness of the Event, what recipient can do with the information and the category of the incident.

Galaxies & Galaxy-Clusters: Advanced label containing meta-data

Here: The sector affected by the incident as well as the country. The kill-chain of the attack can be described using the MITRE ATT&CK framework

Event Graph: Visualization of the relationships between entities contained in the Event.

Here: The whole story of the attack can be described with relationships defined between Attributes and Objects

Event Timeline: Visualization of the temporality of the data contained in the event.

Here: A timeline of the steps performed during the attack. The time data is taken directly from the Attributes and Objects belonging to the Event.

Event Report: Markdown-aware supporting text document to describe events or incidents

Here: The report describe the steps taken by the attacker and provide additional contextual information. It also contains references to Attributes and Object encoded in the Event

Attributes: Basic building block to represent information.

They can have context such as taxonomy and express if they are supportive data or meant for automation. An Event can have multiple Attributes

Here: Two Attributes representing payload delivery. One is an IP address, the other is an URL.

Objects: Advanced building block allowing Attribute composition via predefined templates.

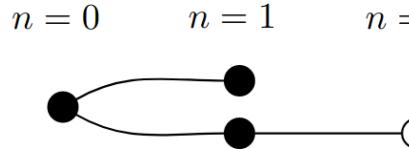
As an Object is an instantiation of its template, it is composed of Attributes that make sense together. They can also have relationship to other entity contained in the Event

Here: A file object composed of Attributes such as the filename, size and hashes. It also have a relationship

Figure 10: event-anatomy

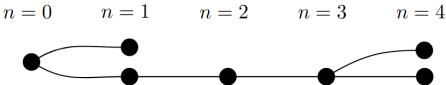
There are 5 distribution levels controlling who can see and how it should be shared:

- **Organisation only:** Only members of your organisation
- **This Community:** Organisations on one MISP instance
- **Connected Community:** Organisations on one MISP instance and those on MISP instances synchronising with this one. Upon receiving data, the distribution will be downgraded to



This community to avoid further propagation

- **All Community:** Anyone having access. Data will be freely propagated in the network of connected MISP instances



- **Sharing Groups:** Distribution list that exhaustively keeps track of which organisa-

Sharing Group configuration	
Organisations	Org. α Org. ω Org. γ
Instances*	MISP 1 MISP 2 MISP 3

*Or enable roaming mode instead

tions can access the data and to which server it should be synchronised

1.5 Synchronisation

In MISP, a synchronisation is the act of sharing data from one MISP to another. It can be done with two mechanisms, namely *push* and *pull*. The fact of an instance sending data to another is called *pushing*. If one instance retrieve data from another, it is called *pulling*.

The diagram below shows a one-way synchronisation link between two MISP instances. The Organisation α created a *sync_user* (denoted with a +) on MISP 2. A synchronisation link can be created on MISP 1 using the API Key and the organisation of the *sync_user*. At that point, MISP 1 can *pull* data from MISP 2 and can *push* data to MISP 2.

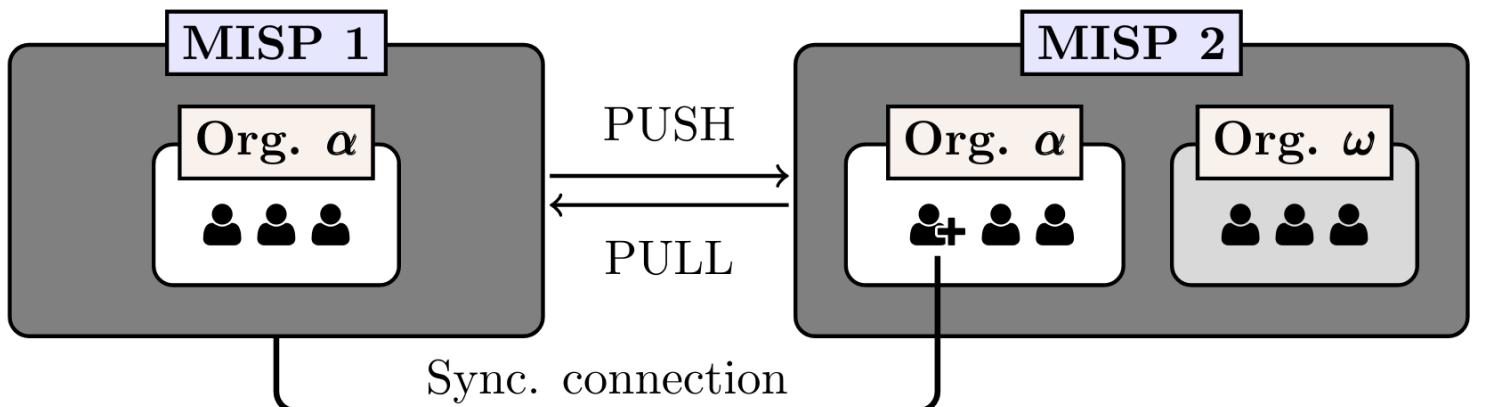


Figure 11: synchronisation

Once a synchronisation link exists *Events* can flow through that connection if and only if the distribution level of the *Event* allows it and if the *Event* is published.

1.6 Correlation

A *correlation* is a link between two *Attributes* that are created automatically. They allow interconnection between *Events* based on the correlation *Attribute*'s value. The system responsible to create these links is called the correlation engine and support not only strict string comparison but also more clever data type such as CIDR blocks and Fuzzy hashing like SSDEEP.

The correlation system is a tool meant for analysts to corroborate findings and gauge the trustiness of the data. It allows to confirm certain aspect of a report or to find new or unknown threats.

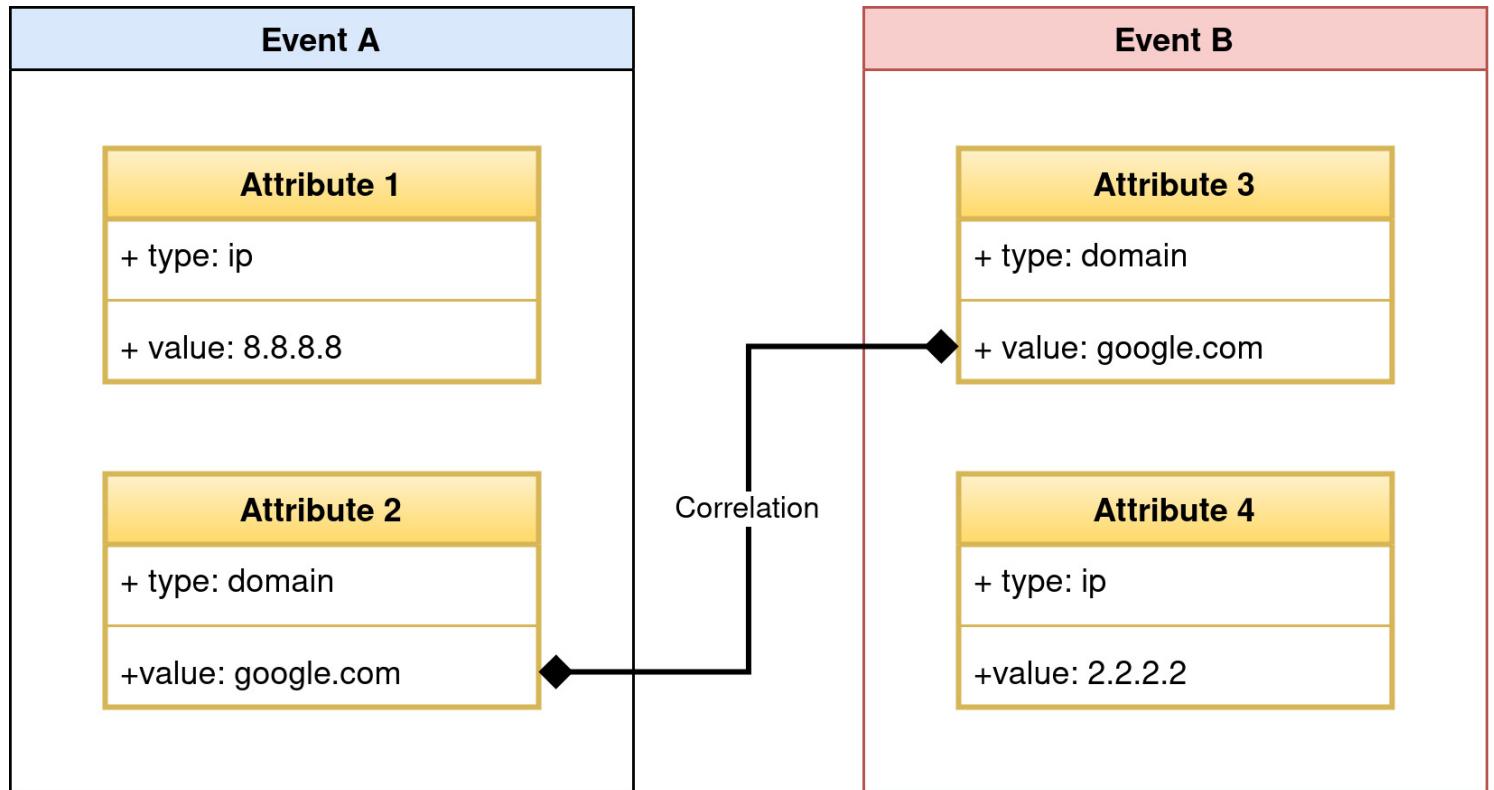


Figure 12: correlation

How-to

Create an Event

1. On the top-bar, click on Event Action then Add Event
2. Choose the correct distribution
3. Fill the Event info field with a concise summary of what this Event is about
4. Fill the remaining optional fields
5. Click on Submit

The screenshot displays two main pages of the ThreatConnect platform:

- Event List Page:** Shows a grid of event records. One record is highlighted in green, indicating it is selected. The columns include: ID, Date, Distribution, and various event details like Source IP, Target IP, and Status.
- Add Event Page:** A form for creating a new event. It includes fields for Date (set to 2023-03-08), Distribution (set to "This community only"), Threat Level (set to "Info"), and a large text area for Event Info containing placeholder text: "Quick Event Description or Tracking Info".

Create an Attribute

1. When viewing an *Event*, click on **Add Attribute**
2. Fill the required Category, Type and Value field
3. Check **For Intrusion Detection System** checkbox if you consider this *Attribute* to be an indicator
4. Fill the remaining optional fields
5. Click on **Submit**

Firefox web browser

Event #11 - MISP

https://localhost:443/university/changing/11

Home Event Actions Dashboard Issues Alert Pages Global Actions Open Actions Administration Log API

Event Report

Add Attribute

Event ID: 11
Event URL: https://localhost:443/university/changing/11
Event Type: Training
Event Status: Unpublished
Event Name: Event Report Example
Event Description: Event report example
Event Category: Event Report Example
Event Start Date: 2021-11-28
Event End Date: 2021-11-28
Event Location: Online
Event Duration: 0 hours
Event Classification: User organization only
Event Report: Event report example
Event Report URL: https://localhost:443/university/changing/11
Event Report Status: Published
Event Report Last Change: 2021-11-28 10:26:27
Last Change: 2021-01-01 00:00:00
Modification Map:
Signature: 0.00 - associated to user organization only, JP

Event Actions

Event Information

Event Details

Add Attribute

Category i Type i

Network activity ▾ ip-src ▾

Value

8.8.8.8

General Options

For Intrusion Detection System

Block connection
 Disable connection

First seen date: 2018-01-01 00:00:00 Last seen date: 2018-01-01 00:00:00

First seen time: 00:00:00 Last seen time: 00:00:00

Associated threat: Unknown threat Associated threat: Unknown threat

Submit

Create an Object

1. When viewing an *Event*, click on **Add Object**
2. If you know the category of the *Object*, select it, otherwise pick **All Objects**
3. To add a “File” *Object*, search the entry in the dropdown or start typing **file** then select the entry
4. Fill out at least the requirements for this *Object* and additional other *Attributes*
5. Click on **Submit**
6. Review the *Object* you are about to create then it **Create new object**

Event report example

The screenshot shows a search dialog titled "All Objects" with the query "file". The results list includes "cytomic-orion-file" (Cytomic Orion File Detection), "file" (selected), "network-profile", "original-imported-file", and "ripperper-software-hive-userprofile-winlogon".

Add File Object

Object Template: File object

Description: The object describing all the file object information.

Requirements: Required one of: filename, size-in-bytes, authentihash, ssdeep, md5, sha1, sha224, sha256, sha384, sha512, sha512/224, sha512/256, sha3-224, sha3-256, sha3-384, sha3-512, tish, telfhash, imphash, pattern-in-file, certificate, malware-sample, attachment, path, fullpath

File category: File

Distribution: Default account

Comment:

Last seen date: Last seen date

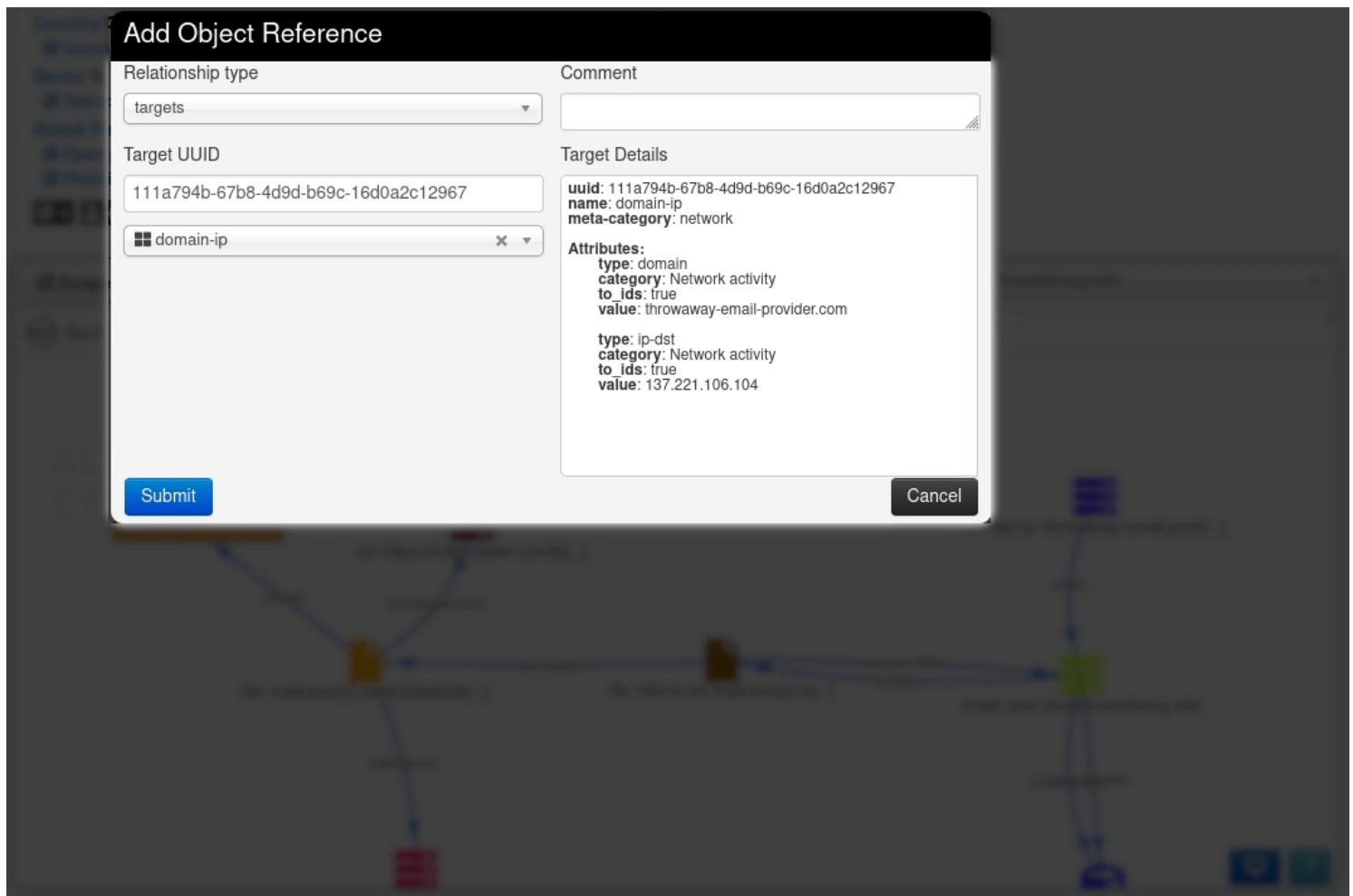
Last seen time: Last seen time

Save	Name :: type	Description	Category	Value	IDS	Disable Correlation
<input type="checkbox"/>	Attachment attachment	A non-malicious file.	External analysis	<input type="button" value="Browse..."/> No file selected.	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	Malware-sample malware-sample	The file itself (binary)	Payload delivery	<input type="button" value="Browse..."/> No file selected.	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	Text text	Free text value to attach to the file	Other	<input type="text"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Create an Relationship

1. To create a relationship or *Reference*, a user can either click on the plus button from the *Object* table or do it directly from the *Event Graph*
2. On the *Event Graph*, click on **Edit** then drag an arrow from the first *Object* to another entity
3. On the **Add Object Reference** box, select which verb should be used to describe the relationship in the **Relationship type** input
 - Note: If you want to use a verb not present in the list, use the **custom** entry
4. Click on **Submit**

References: 3 [+] ▾



Create an Event Report

1. When viewing an *Event*, click on the toggle button **Event reports**
2. Click on **Add Event Report** and enter the name of the report. As its content can be written with more ease in the dedicated editor, leave it empty and click on **Submit**
3. Once the list has reloaded, click on the *Event Report* that was created, then on the **Edit report** button
4. Write the report in the editor
 - Note: The **Help** button contains documentation about the supported markdown syntax and how to reference *Attributes*, *Objects* and context.
5. Once you are done, click the **Save** button

Event Reports

+ Add Event Report Generate report from Event All Default Deleted

ID	Name	Last update	Distribution	Actions
13	My report	2021-11-25 10:29:34	Your organisation only	
14	Report from - https://www.welivesecurity.com/2021/02/02/kobalos-complex-linux-threat-high-performance-computing-infrastructure (1637836339)	2022-01-18 14:00:50	Inherit event	

My report

The screenshot shows a web-based reporting interface. At the top, there are tabs for 'Event', 'Attribute', 'Relationship', and 'Custom report template'. Below these are sections for 'Event details', 'Attribute details', and 'Relationship details'. A toolbar at the top right includes 'Save' and 'Help' buttons. The main area has a code editor on the left and a preview on the right.

Code Editor (Left):

```
1 # Description of the incident
2 The incident took place ...
3
4 | Column 1 | Column 2 | Column 3 |
5 | ----- | ----- | ----- |
6 | Text     | Text     | Text     |
7
8
9 ***
10 def hello():
11     print('Hello World')
12 ***
13
14 - A reference to `filename` Attribute: @[attribute] (94b9aec0-1690-41d4-92b7-1370b2b7c5d9)
15 - A reference to a `file` Object @[object](16b535ba-c3f8-4984-9600-961aef943693)
```

Description of the incident (Right):

Description of the incident

The incident took place ...

Column 1	Column 2	Column 3
Text	Text	Text

```
def hello():
    print('Hello World')
```

- A reference to `filename` Attribute: `filename ControlIT1573.001Encrypted`
- A reference to a `file` Object `file cf5f24cea4cdb2a222670c6a7b18c966`

Add Tags

1. *Tags* can be attached to both *Events* and *Attributes* with the following buttons:
2. To tag the *Event* or the *Attribute* globally, click on the button with the globe icon
3. Select the *Taxonomy* in which the tag is part of or click on **All Tags**
4. Pick the tag then click on **Submit**

Event report example

The screenshot shows an event report interface with a 'Tags' section at the bottom. A 'Add a tag' dialog is open over the report content.

Tags (Bottom Left):

- tip:white
- osint:lifetime="perpetual"
- workflow:state="draft"
- smo:sync

Add a tag Dialog (Bottom Right):

Buttons: Tag Collections, Custom Tags, All Tags, Taxonomy Library:tip

Input field: tip:red

Submit button

Figure 13: tag

Add Galaxy Clusters

1. Similar to tags, *Galaxy Clusters* can be attached with the button with the globe icon
2. To tag the *Event* or the *Attribute* globally, click on the button with the globe icon
3. Select the namespace in the *Galaxy* is part of or click on **All namespaces**
4. Select the *Galaxy* in which the *Cluster* is part of or click on **All Clusters**
5. Pick the *Cluster* then click on **Submit**

The screenshot shows a threat intelligence application interface. On the left, there is a sidebar with various filters and search fields:

- Galaxies**
- Threat Actor**: APT 29
- Target Information**: Canada, China
- Sector**: Defense, Infrastructure
- Malpedia**: Kobalos
- Attack**: Add new cluster
- SS**
- So**

A modal dialog box titled "Add new cluster" is open in the center. It contains a dropdown menu labeled "All namespaces" and a list of options:

- Select an Option
- & Attack Pattern
- Bhadra Framework
- CONCORDIA Mobile Modelling Framework - Attack Pattern
- Election guidelines
- Misinformation Pattern
- SoD Matrix
- Tea Matrix
- attck4fraud
- o365-exchange-techniques
- rsit

At the bottom of the dialog, there is a text input field containing "Internal Spearphishing - T1534" and a "Submit" button.

Figure 14: cluster

Publish

1. Whenever an *Event* is to be shared, it has to be Published
2. When viewing an *Event*, click on the Publish button located on the sidebar

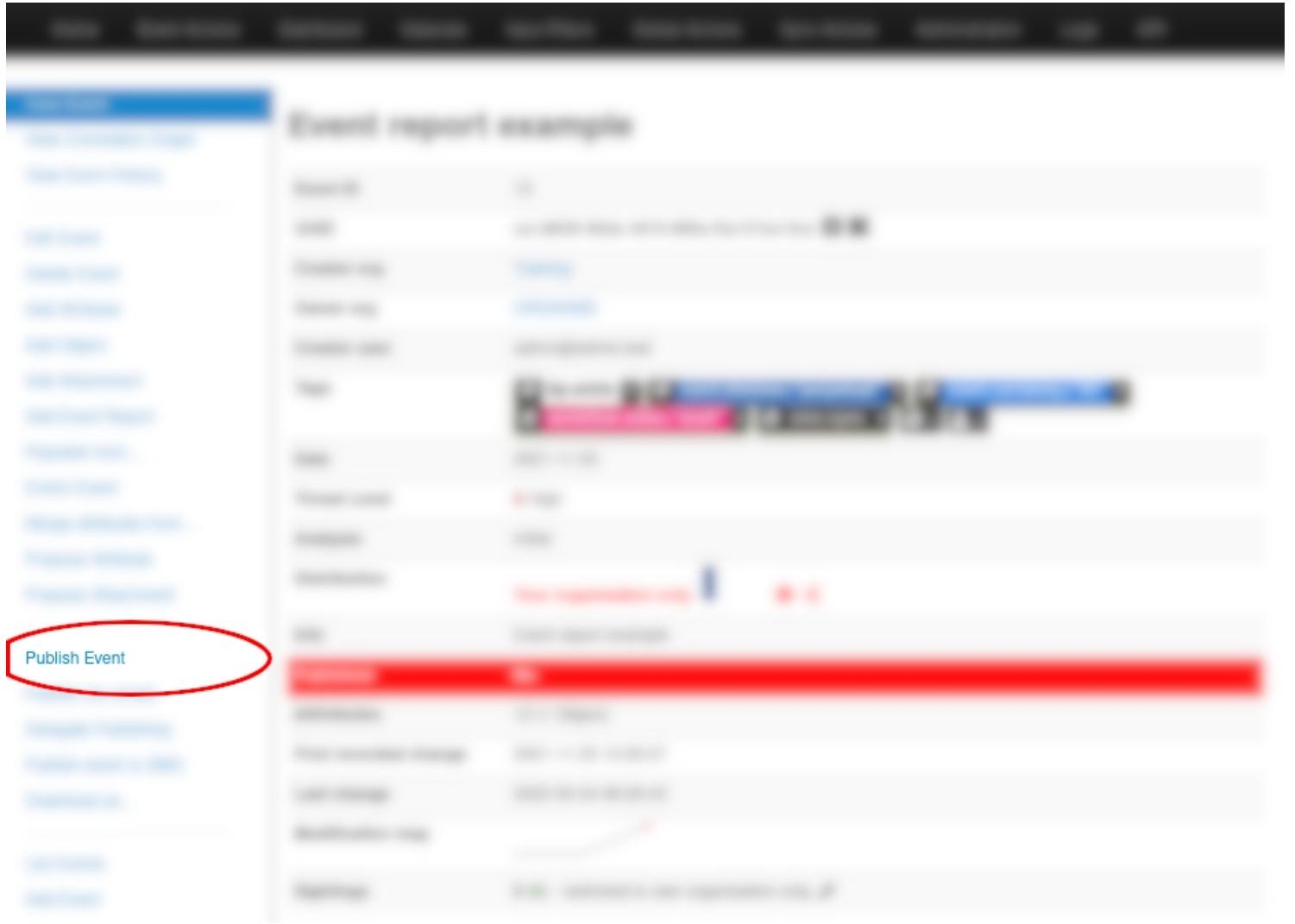


Figure 15: publish-event

Further document and reading references

The following references are not required to follow the training later. The documents and references below are provided for student willing to deep dive into MISP or have specific topic to understand.

- Neolea trainings
- Virtual machines (VirtualBox and VMWare format) if you want to explore a bit more MISP
 - <https://vm.misp-project.org/>
- Slide Deck (source file and compiled)
 - <https://github.com/MISP/misp-training>
 - <https://github.com/cerebrate-project/cerebrate-training>
- Cheatsheet
 - <https://www.misp-project.org/misp-training/cheatsheet.pdf>
- PyMISP
 - <https://github.com/MISP/PyMISP/>
- OpenAPI documentation
 - <https://www.misp-project.org/documentation/openapi.html>
- MISP Book
 - [User guide for MISP PDF](#)
- MISP data models and knowledge base available

- MISP taxonomies
- MISP object templates
- MISP galaxy