

AN INTRODUCTION TO CYBERSECURITY INFORMATION SHARING

MISP - THREAT SHARING

CIRCL / TEAM MISP PROJECT

MISP PROJECT

<https://www.misp-project.org/>

13TH ENISA-EC3 WORKSHOP



MISP
Threat Sharing

AGENDA

- Agenda and details available
<https://tinyurl.com/EC3-LEA>

MISP AND STARTING FROM A PRACTICAL USE-CASE

- During a malware analysis workgroup in 2012, we discovered that we worked on the analysis of the same malware.
- We wanted to share information in an easy and automated way **to avoid duplication of work**.
- Christophe Vandeplas (then working at the CERT for the Belgian MoD) showed us his work on a platform that later became MISP.
- A first version of the MISP Platform was used by the MALWG and **the increasing feedback of users** helped us to build an improved platform.
- MISP is now **a community-driven development**.

The Computer Incident Response Center Luxembourg (CIRCL) is a government-driven initiative designed to provide a systematic response facility to computer security threats and incidents. CIRCL is the CERT for the private sector, communes and non-governmental entities in Luxembourg and is operated by LHC g.i.e.

MISP AND CIRCL

- CIRCL is mandated by the Ministry of Economy and acting as the Luxembourg National CERT for private sector.
- CIRCL leads the development of the Open Source MISP threat intelligence platform which is used by many military or intelligence communities, private companies, financial sector, National CERTs and LEAs globally.
- **CIRCL runs multiple large MISP communities performing active daily threat-intelligence sharing.**



Co-financed by the European Union

Connecting Europe Facility

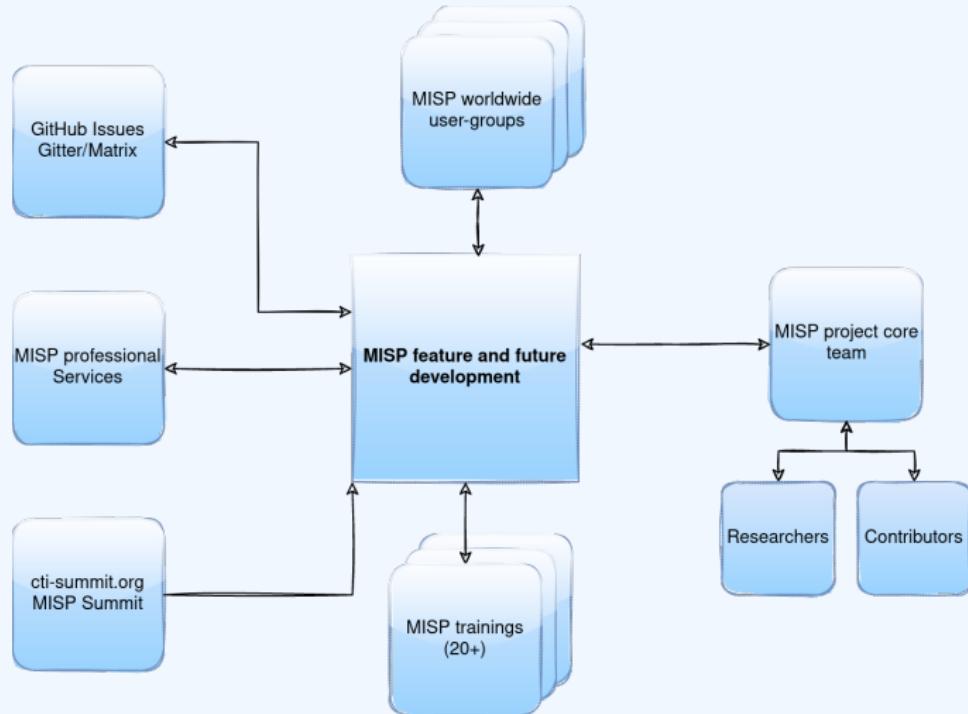
WHAT IS MISP?

- MISP is a **threat information sharing** platform that is free & open source software
- A tool that **collects** information from partners, your analysts, your tools, feeds
- Normalises, **correlates, enriches** the data
- Allows teams and communities to **collaborate**
- **Feeds** automated protective tools and analyst tools with the output

DEVELOPMENT BASED ON PRACTICAL USER FEEDBACK

- There are many different types of users of an information sharing platform like MISP:
 - ▶ **Malware reversers** willing to share indicators of analysis with respective colleagues.
 - ▶ **Security analysts** searching, validating and using indicators in operational security.
 - ▶ **Intelligence analysts** gathering information about specific adversary groups.
 - ▶ **Law-enforcement** relying on indicators to support or bootstrap their DFIR cases.
 - ▶ **Risk analysis teams** willing to know about the new threats, likelihood and occurrences.
 - ▶ **Fraud analysts** willing to share financial indicators to detect financial frauds.

MISP MODEL OF GOVERNANCE



MANY OBJECTIVES FROM DIFFERENT USER-GROUPS

- Sharing indicators for a **detection** matter.
 - ▶ 'Do I have infected systems in my infrastructure or the ones I operate?'
- Sharing indicators to **block**.
 - ▶ 'I use these attributes to block, sinkhole or divert traffic.'
- Sharing indicators to **perform intelligence**.
 - ▶ 'Gathering information about campaigns and attacks. Are they related? Who is targeting me? Who are the adversaries?'
- → These objectives can be conflicting (e.g. False-positives have different impacts)

COMMUNITIES USING MISP

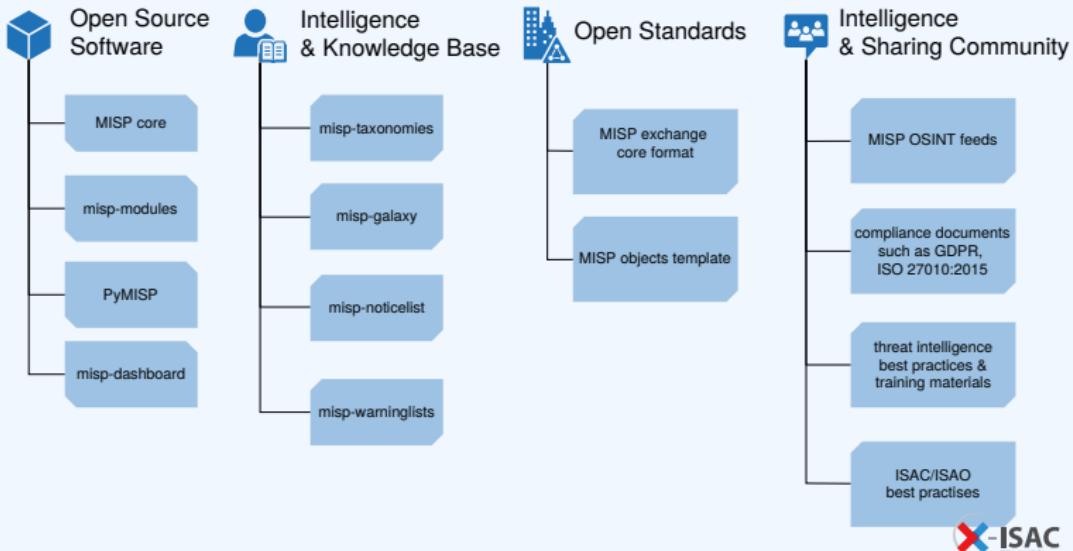
- Communities are groups of users sharing within a set of common objectives/values.
- CIRCL operates multiple MISP instances with a significant user base (more than 1200 organizations with more than 4000 users).
- **Trusted groups** running MISP communities in island mode (air gapped system) or partially connected mode.
- **Financial sector** (banks, ISACs, payment processing organizations) use MISP as a sharing mechanism.
- **Military and international organizations** (NATO, military CSIRTs, n/g CERTs,...).
- **Security vendors** running their own communities (e.g. Fidelis) or interfacing with MISP communities (e.g. OTX).
- **Topical communities** set up to tackle individual specific issues (COVID-19 MISP)

SHARING DIFFICULTIES

- Sharing difficulties are not really technical issues but often it's a matter of **social interactions** (e.g. **trust**).
- Legal restriction¹
 - ▶ "Our legal framework doesn't allow us to share information."
 - ▶ "Risk of information-leak is too high and it's too risky for our organization or partners."
- Practical restriction
 - ▶ "We don't have information to share."
 - ▶ "We don't have time to process or contribute indicators."
 - ▶ "Our model of classification doesn't fit your model."
 - ▶ "Tools for sharing information are tied to a specific format, we use a different one."

¹<https://www.misp-project.org/compliance/>

MISP PROJECT OVERVIEW



SHARING IN MISP

- Sharing via distribution lists - **Sharing groups**
- **Delegation** for pseudo-anonymised information sharing
- **Proposals** and **Extended events** for collaborated information sharing
- Synchronisation, Feed system, air-gapped sharing
- User defined **filtered sharing** for all the above mentioned methods
- Cross-instance information **caching** for quick lookups of large data-sets
- Support for multi-MISP internal enclaves

INFORMATION QUALITY MANAGEMENT

- Correlating data
- Feedback loop from detections via **Sightings**
- **False positive management** via the warninglist system
- **Enrichment system** via MISP-modules
- **workflow** system to review and control information publication
- **Integrations** with a plethora of tools and formats
- Flexible **API** and support **libraries** such as PyMISP to ease integration
- **Timelines** and giving information a temporal context
- Full chain for **indicator life-cycle management**

CONCLUSION

- **Information sharing practices come from usage** and by example (e.g. learning by imitation from the shared information).
- MISP is just a tool. What matters is your sharing practices. The tool should be as transparent as possible to support you.
- Enable users to customize MISP to meet their community's use-cases.
- MISP project combines open source software, open standards, best practices and communities to make information sharing a reality.

AN INTRODUCTION TO CYBERSECURITY INFORMATION SHARING

MISP - THREAT SHARING

CIRCL / TEAM MISP PROJECT

MISP PROJECT

<https://www.misp-project.org/>

13TH ENISA-EC3 WORKSHOP



MISP
Threat Sharing

AGENDA

- Agenda and details available
<https://tinyurl.com/EC3-LEA>

MISP AND STARTING FROM A PRACTICAL USE-CASE

- During a malware analysis workgroup in 2012, we discovered that we worked on the analysis of the same malware.
- We wanted to share information in an easy and automated way **to avoid duplication of work**.
- Christophe Vandeplas (then working at the CERT for the Belgian MoD) showed us his work on a platform that later became MISP.
- A first version of the MISP Platform was used by the MALWG and **the increasing feedback of users** helped us to build an improved platform.
- MISP is now **a community-driven development**.

ABOUT CIRCL

The Computer Incident Response Center Luxembourg (CIRCL) is a government-driven initiative designed to provide a systematic response facility to computer security threats and incidents. CIRCL is the CERT for the private sector, communes and non-governmental entities in Luxembourg and is operated by securitymadein.lu g.i.e.

- CIRCL is mandated by the Ministry of Economy and acting as the Luxembourg National CERT for private sector.
- CIRCL leads the development of the Open Source MISP threat intelligence platform which is used by many military or intelligence communities, private companies, financial sector, National CERTs and LEAs globally.
- **CIRCL runs multiple large MISP communities performing active daily threat-intelligence sharing.**



Co-financed by the European Union
Connecting Europe Facility

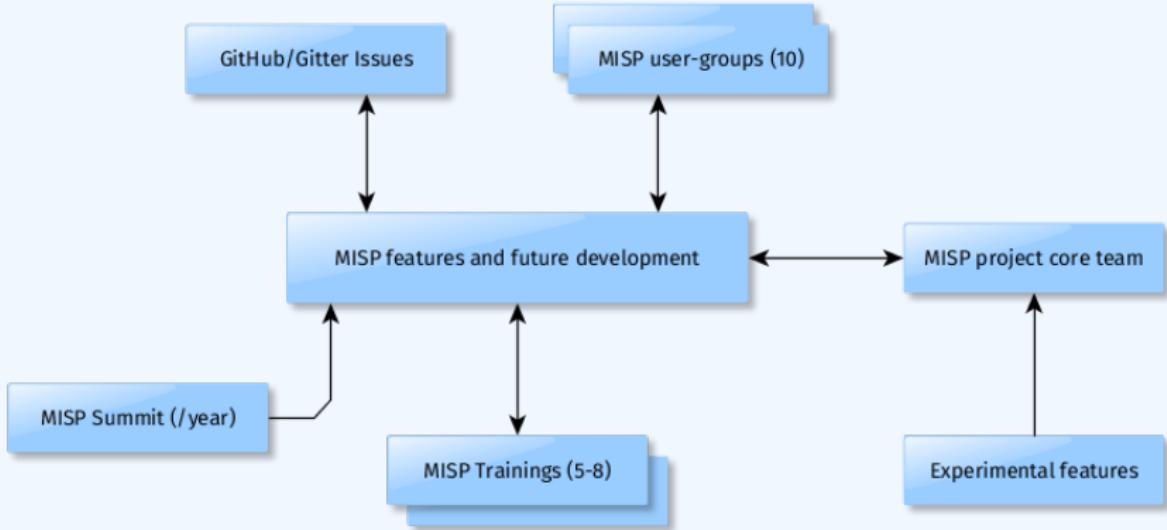
WHAT IS MISP?

- MISP is a **threat information sharing** platform that is free & open source software
- A tool that **collects** information from partners, your analysts, your tools, feeds
- Normalises, **correlates, enriches** the data
- Allows teams and communities to **collaborate**
- **Feeds** automated protective tools and analyst tools with the output

DEVELOPMENT BASED ON PRACTICAL USER FEEDBACK

- There are many different types of users of an information sharing platform like MISP:
 - ▶ **Malware reversers** willing to share indicators of analysis with respective colleagues.
 - ▶ **Security analysts** searching, validating and using indicators in operational security.
 - ▶ **Intelligence analysts** gathering information about specific adversary groups.
 - ▶ **Law-enforcement** relying on indicators to support or bootstrap their DFIR cases.
 - ▶ **Risk analysis teams** willing to know about the new threats, likelihood and occurrences.
 - ▶ **Fraud analysts** willing to share financial indicators to detect financial frauds.

MISP MODEL OF GOVERNANCE



MANY OBJECTIVES FROM DIFFERENT USER-GROUPS

- Sharing indicators for a **detection** matter.
 - ▶ 'Do I have infected systems in my infrastructure or the ones I operate?'
- Sharing indicators to **block**.
 - ▶ 'I use these attributes to block, sinkhole or divert traffic.'
- Sharing indicators to **perform intelligence**.
 - ▶ 'Gathering information about campaigns and attacks. Are they related? Who is targeting me? Who are the adversaries?'
- → These objectives can be conflicting (e.g. False-positives have different impacts)

COMMUNITIES USING MISP

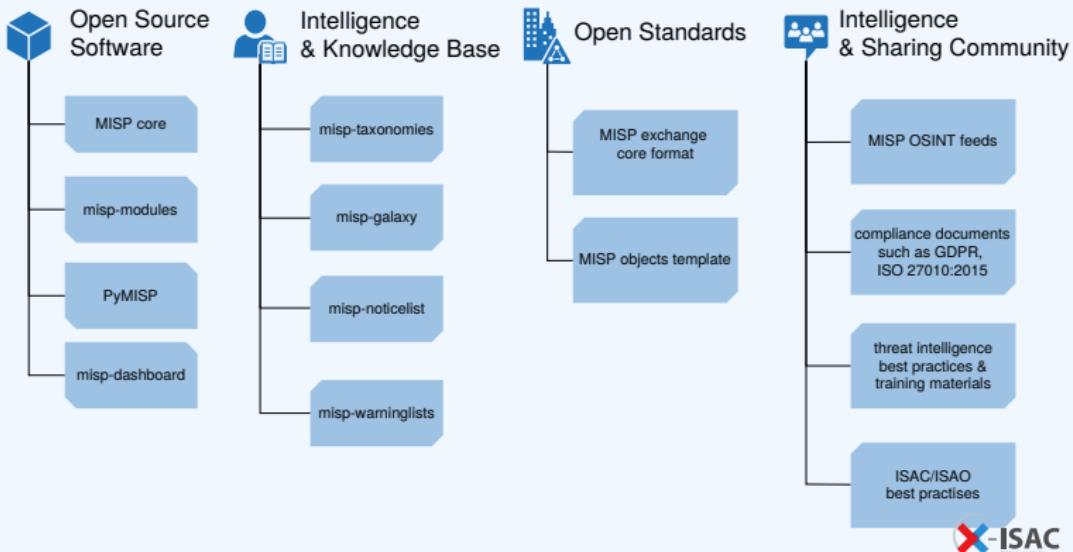
- Communities are groups of users sharing within a set of common objectives/values.
- CIRCL operates multiple MISP instances with a significant user base (more than 1200 organizations with more than 4000 users).
- **Trusted groups** running MISP communities in island mode (air gapped system) or partially connected mode.
- **Financial sector** (banks, ISACs, payment processing organizations) use MISP as a sharing mechanism.
- **Military and international organizations** (NATO, military CSIRTs, n/g CERTs,...).
- **Security vendors** running their own communities (e.g. Fidelis) or interfacing with MISP communities (e.g. OTX).
- **Topical communities** set up to tackle individual specific issues (COVID-19 MISP)

SHARING DIFFICULTIES

- Sharing difficulties are not really technical issues but often it's a matter of **social interactions** (e.g. **trust**).
- Legal restriction¹
 - ▶ "Our legal framework doesn't allow us to share information."
 - ▶ "Risk of information-leak is too high and it's too risky for our organization or partners."
- Practical restriction
 - ▶ "We don't have information to share."
 - ▶ "We don't have time to process or contribute indicators."
 - ▶ "Our model of classification doesn't fit your model."
 - ▶ "Tools for sharing information are tied to a specific format, we use a different one."

¹<https://www.misp-project.org/compliance/>

MISP PROJECT OVERVIEW



GETTING SOME NAMING CONVENTIONS OUT OF THE WAY...

■ Data layer

- ▶ **Events** are encapsulations for contextually linked information
- ▶ **Attributes** are individual data points, which can be indicators or supporting data
- ▶ **Objects** are custom templated Attribute compositions
- ▶ **Object references** are the relationships between other building blocks
- ▶ **Sightings** are time-specific occurrences of a given data-point detected

■ Context layer

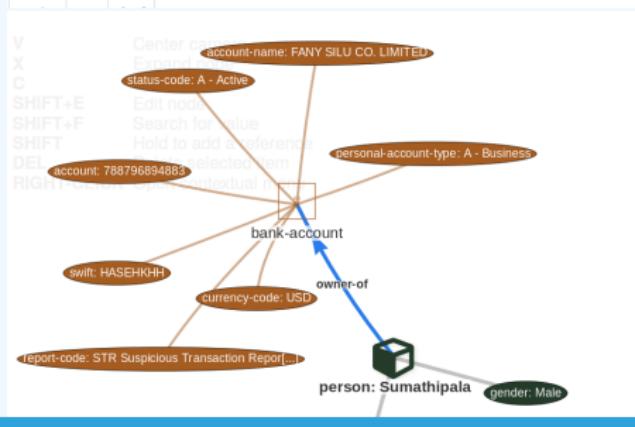
- ▶ **Tags** are labels attached to events/attributes and can come from **Taxonomies**
- ▶ **Galaxy-clusters** are knowledge base items used to label events/attributes and come from **Galaxies**
- ▶ **Cluster relationships** denote pre-defined relationships between clusters

TERMINOLOGY ABOUT INDICATORS

- Indicators²
 - ▶ Indicators contain a pattern that can be used to detect suspicious or malicious cyber activity.
- Attributes in MISP can be network indicators (e.g. IP address), system indicators (e.g. a string in memory) or even bank account details.
 - ▶ **A type (e.g. MD5, url) is how an attribute is described.**
 - ▶ An attribute is always in a category (e.g. Payload delivery) which puts it in a context.
 - **A category is what describes** an attribute.
 - ▶ An IDS flag on an attribute allows to determine if **an attribute can be automatically used for detection.**

²IoC (Indicator of Compromise) is a subset of indicators

A RICH DATA-MODEL: TELLING STORIES VIA RELATIONSHIPS



CONTEXTUALISATION AND AGGREGATION

- MISP integrates at the event and the attribute levels MITRE's Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK).

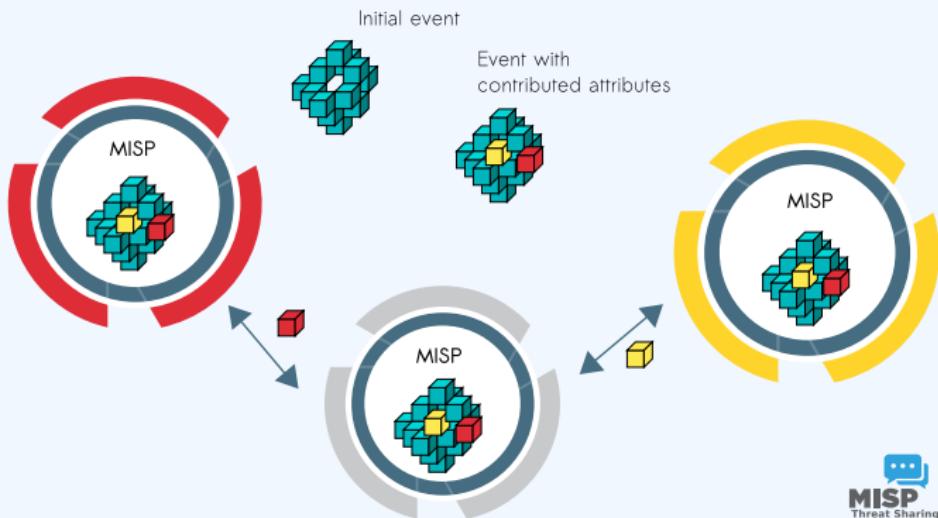
Pro Attack - Attack Pattern	Enterprise Attack - Attack Pattern	Mobile Attack - Attack Pattern									
Initial access	Execution	Persistence	Privilege escalation	Defense evasion	Credential access	Discovery	Lateral movement	Collection	Exfiltration	Command and control	
Phishing Attachment	Scripting	Screensaver	File System Permissions Weakness	Process Hollowing	Securityd Memory	Password Policy Discovery	AppleScript	Data from Information Repositories	Exfiltration Over Alternative Protocol	Standard Application Layer Protocol	
Speachphishing 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	Regsvr/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	
Speachphishing Link	Windows Management Instrumentation	LG_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 Doppelganging	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 Oblfuscation	
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			

SHARING IN MISP

- Sharing via distribution lists - **Sharing groups**
- **Delegation** for pseudo-anonymised information sharing
- **Proposals** and **Extended events** for collaborated information sharing
- Synchronisation, Feed system, air-gapped sharing
- User defined **filtered sharing** for all the above mentioned methods
- Cross-instance information **caching** for quick lookups of large data-sets
- Support for multi-MISP internal enclaves

MISP CORE DISTRIBUTED SHARING FUNCTIONALITY

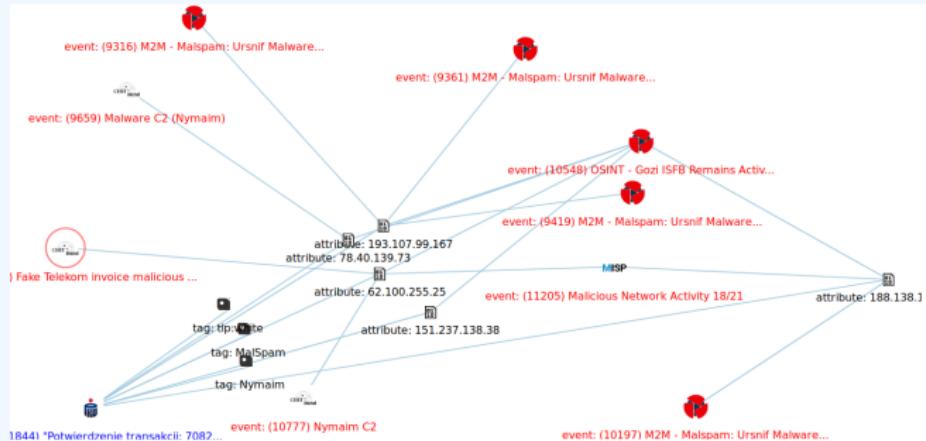
- MISP's core functionality is sharing where everyone can be a consumer and/or a contributor/producer."
- Quick benefit without the obligation to contribute.
- Low barrier access to get acquainted to the system.



INFORMATION QUALITY MANAGEMENT

- Correlating data
- Feedback loop from detections via **Sightings**
- **False positive management** via the warninglist system
- **Enrichment system** via MISP-modules
- **Integrations** with a plethora of tools and formats
- Flexible **API** and support **libraries** such as PyMISP to ease integration
- **Timelines** and giving information a temporal context
- Full chain for **indicator life-cycle management**

CORRELATION FEATURES: A TOOL FOR ANALYSTS



- To corroborate a finding (e.g. is this the same campaign?), reinforce an analysis (e.g. do other analysts have the same hypothesis?), confirm a specific aspect (e.g. are the sinkhole IP addresses used for one campaign?) or just find if this threat is new or unknown in your community.

SIGHTINGS SUPPORT

Events

<input checked="" type="checkbox"/>	No	Sightings CIRCL: 2 (2017-03-19 16:17:59)
<input checked="" type="checkbox"/>	No	INHERIT (2/0/0)
<input checked="" type="checkbox"/>	No Inherit	0/0/0

Tags

Date: 2016-02-24

Threat Level: High

Analysis: Initial

Distribution: Connected communities, free text test

Sighting Details: No

MISP: 2
CIRCL: 2

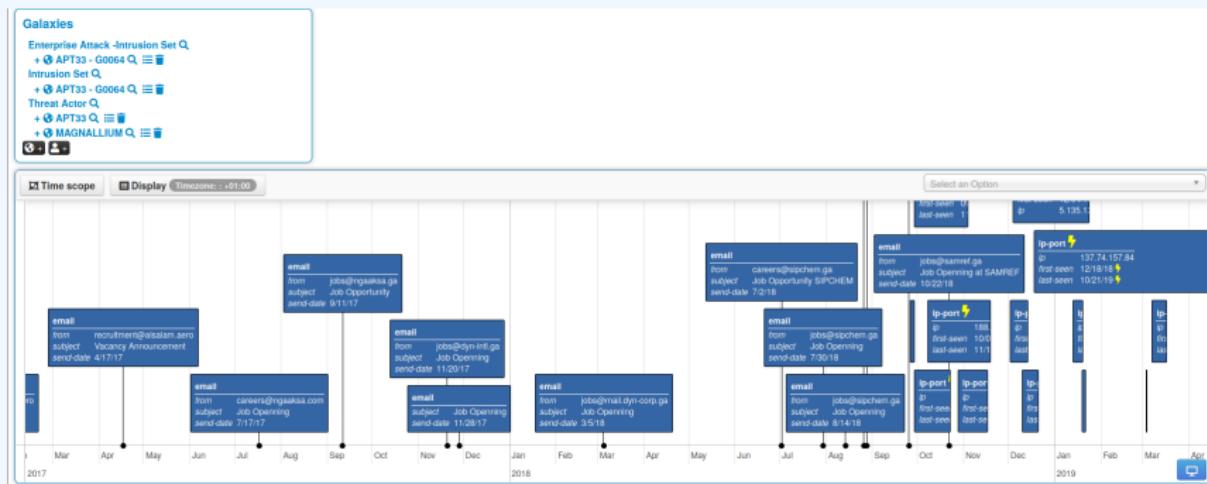
4 (2) - restricted to own organisation only.

- Discussion

- Has a data-point been **sighted** by me or the community before?
- Additionally, the sighting system supports negative sightings (FP) and expiration sightings.
- Sightings can be performed via the API or the UI.
- Many use-cases for **scoring indicators** based on users sighting.
- For large quantities of data, **SightingDB** by Devo

TIMELINES AND GIVING INFORMATION A TEMPORAL CONTEXT

- Recently introduced **first_seen** and **last_seen** data points
- All data-points can be placed in time
- Enables the **visualisation** and **adjustment** of indicators timeframes



LIFE-CYCLE MANAGEMENT VIA DECAYING OF INDICATORS

Pivots Galaxy Event graph Correlation graph ATT&CK matrix Attributes Discussion

x 45 Decays...

Galaxies

[+ Add](#) [Edit](#) [Delete](#) [Decay score](#) [Context](#) [Related Tags](#) [Filtering tool \(1\)](#)

Enter value to search

Date	Org	Category	Type	Value	Tags	Galaxies	Comment	Correlate	Related Events	Feed	IDS Distribution	Sightings	Activity	Score	Actions	
2019-09-12		Network activity	ip-src	5.5.5.5	+ Add			<input checked="" type="checkbox"/>		Inherit						
2019-08-13		Network activity	ip-src	8.8.8.8	+ Add			<input checked="" type="checkbox"/>	1 2 2 2	S1:1	<input checked="" type="checkbox"/>	Inherit				
2019-08-13		Network activity	ip-src	9.9.9.9	+ Add			<input checked="" type="checkbox"/>	1 3 19	S1:1	<input checked="" type="checkbox"/>	Inherit				
2019-08-13		Network activity	ip-src	7.7.7.7	+ Add			<input checked="" type="checkbox"/>	41		<input checked="" type="checkbox"/>	Inherit				
2019-07-18		Network activity	ip-src	6.6.6.6	+ Add			<input checked="" type="checkbox"/>	41		<input checked="" type="checkbox"/>	Inherit				

- Decay score toggle button
 - ▶ Shows Score for each *Models* associated to the *Attribute* type

DECAYING OF INDICATORS: FINE TUNING TOOL

Home Event Actions Databases Input Filters Global Actions Sync Actions Administration Audit NEP AI

Import Decaying Model
Add Decaying Model
Decaying Tool
List Decaying Models

Decaying Of Indicator Fine Tuning Tool

Show All Types Show MISP Objects Search Attribute Type

Attribute Type	Category	Model ID
abs-r11	Financial fraud	
authentihash	Payload delivery	
bank-account-qr	Financial fraud	
btc	Financial fraud	
bin	Financial fraud	
bro	Network activity	ID 11
btc	Financial fraud	11
cc-number	Financial fraud	
cphash	Payload delivery	
community-id	Network activity	
domain	Network activity	
domainip	Network activity	10-84
email-attachment	Payload delivery	
email-dst	Network activity	11
email-src	Payload delivery	
filename	Payload delivery	
filenameauthentihash	Payload delivery	
filenameimpfuzzy	Payload delivery	
filenamejephash	Payload delivery	
filenamejres	Payload delivery	13
filenamejshash	Payload delivery	13
filenamejs1	Payload delivery	13

Polynomial

Lifetime: 3 days
Decay speed: 2.3
Cut-off threshold: 30
Adjust base score: Simulate this model:

Phishing model: Simple model to rapidly decay Take

All available models My models Default models

ID	Model Name	Org ID	Description	Formula	Lifetime	Decay speed	Threshold	Default basescore	Basescore config	Settings	# Types	Enabled	Action
29	Phishing model	1	Simple model to rapidly decay	Polynomial	3	2.3	30	80	estimative-language-phishing website.	0.5	9	<input checked="" type="checkbox"/>	<input type="button" value="Load model"/>

Create, modify, visualise, perform mapping

DECAYING OF INDICATORS: SIMULATION TOOL

NIDS Simple Decaying Model

RestSearch Specific ID

Attribute RestSearch*

```
{"includeDecayScore": 1, "includeFullModel": 0, "score": 30, "excludeDecayed": 0, "decayingModel": [85], "to_ids": 1, "tags": ["estimative-language%", "priority-level%", "interference%", "targeted-threat"], "confidence_level": "usually-confident", "map-confidence-level": "fairly-confident", "adversary-scale-source-reliability": "a", "retention_expired": 0}
```

Base score: Base score configuration not set. But default value sets.

Tag	Computation	Result
map:confidence-level="usually-confident"	0 × 75.00 0	
map:confidence-level="fairly-confident"	0 × 50.00 0	
adversary-scale-source-reliability="a"	0 × 100.00 0	
retention_expired	0 × Non 0	
base_score		80.00

Sighting: Wed Sep 4 12:18:09 2019 | Current score: 54.60

Score: 54.60

ID	Event T	Date	Org	Category	Type	Value	Tags	Event Tags	Galaxies	Comment	IDS	Sightings	Score
36759	45	2019-08-13	ORIONAME	Network activity	ip-src	7.7.7.7	adversary-scale-information-confidence="C" retention_id	map:confidence-level="usually-confident" map:confidence-level="fairly-confident"			✓		NIDS Simple Decaying ... 37.41
36757	45	2019-08-13	ORIONAME	Network activity	ip-src	8.8.8.8	adversary-scale-source-reliability="a" retention_expired	map:confidence-level="usually-confident" map:confidence-level="fairly-confident"			✓		NIDS Simple Decaying ... 54.6

Page 1 of 1, showing 2 records out of 2 total, starting on record 1, ending on 2

< previous next >

Simulate Attributes with different Models

BOOTSTRAPPING YOUR MISP WITH DATA

- We maintain the default CIRCL OSINT feeds (TLP:WHITE selected from our communities) in MISP to allow users to ease their bootstrapping.
- The format of the OSINT feed is based on standard MISP JSON output pulled from a remote TLS/HTTP server.
- Additional content providers can provide their own MISP feeds. (<https://botvrij.eu/>)
- Allows users to **test their MISP installations and synchronisation with a real dataset.**
- Opening contribution to other threat intel feeds but also allowing the analysis of overlapping data³.

³A recurring challenge in information sharing

CONCLUSION

- **Information sharing practices come from usage** and by example (e.g. learning by imitation from the shared information).
- MISP is just a tool. What matters is your sharing practices. The tool should be as transparent as possible to support you.
- Enable users to customize MISP to meet their community's use-cases.
- MISP project combines open source software, open standards, best practices and communities to make information sharing a reality.

MISP USER TRAINING - GENERAL US- AGE OF MISP

MISP - THREAT SHARING

CIRCL / TEAM MISP PROJECT

[HTTP://WWW.MISP-PROJECT.ORG/](http://www.misp-project.org/)

TWITTER: @MISPPROJECT

13TH ENISA-EC3 WORKSHOP



MISP
Threat Sharing

- Credentials
 - ▶ MISP admin: admin@admin.test/admin
 - ▶ SSH: misp/Password1234
- Available at the following location (VirtualBox and VMWare):
 - ▶ <https://www.circl.lu/misp-images/latest/>

- It is a bit broken.

- ▶ sudo -s
- ▶ cd /var/www/MISP/
- ▶ sudo pear install
 INSTALL/dependencies/Console_CommandLine/package.xml
- ▶ sudo pear install
 INSTALL/dependencies/Crypt_GPG/package.xml
- ▶ cd /usr/local/src/misp-modules
- ▶ pip3 install -r REQUIREMENTS
- ▶ pip3 install .
- ▶ reboot

MISP - GENERAL USAGE

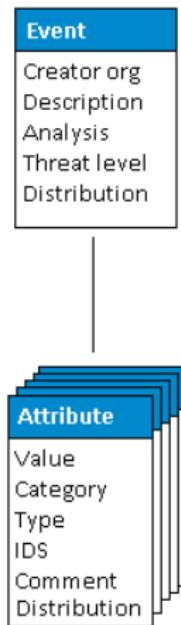
Plan for this part of the training

- Data model
- Viewing data
- Creating data
- Co-operation
- Distribution
- Exports

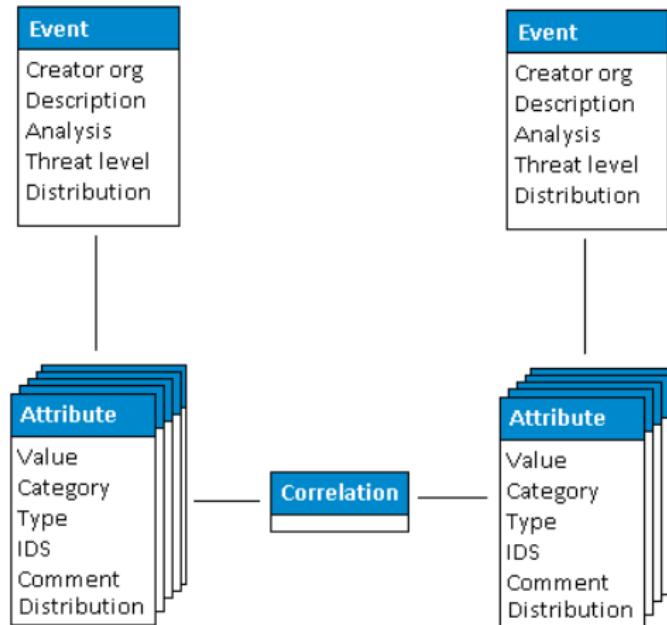
MISP - EVENT (MISP'S BASIC BUILDING BLOCK)

Event
Creator org
Description
Analysis
Threat level
Distribution

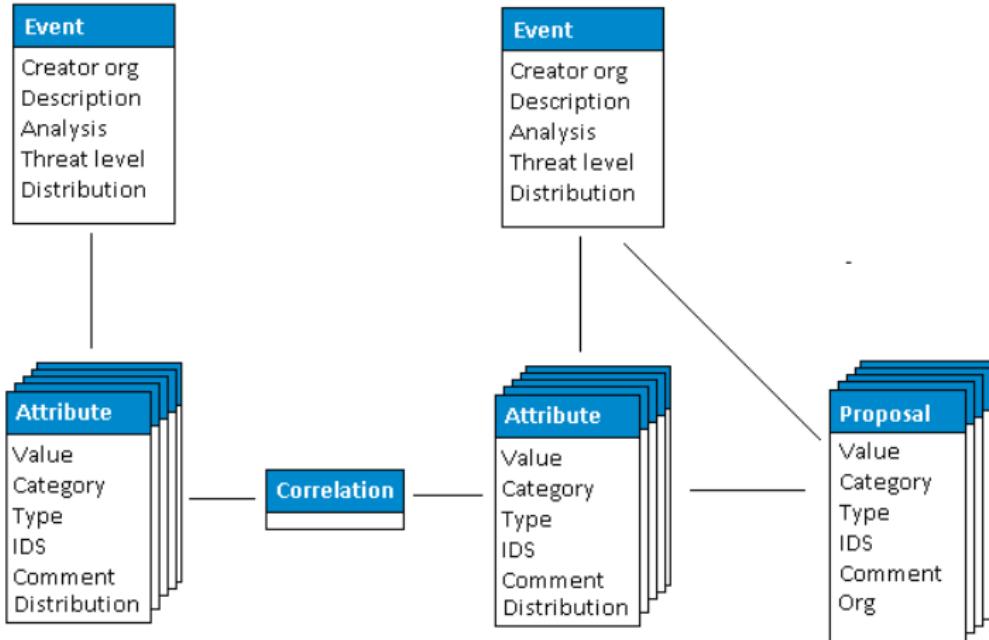
MISP - EVENT (ATTRIBUTES, GIVING MEANING TO EVENTS)



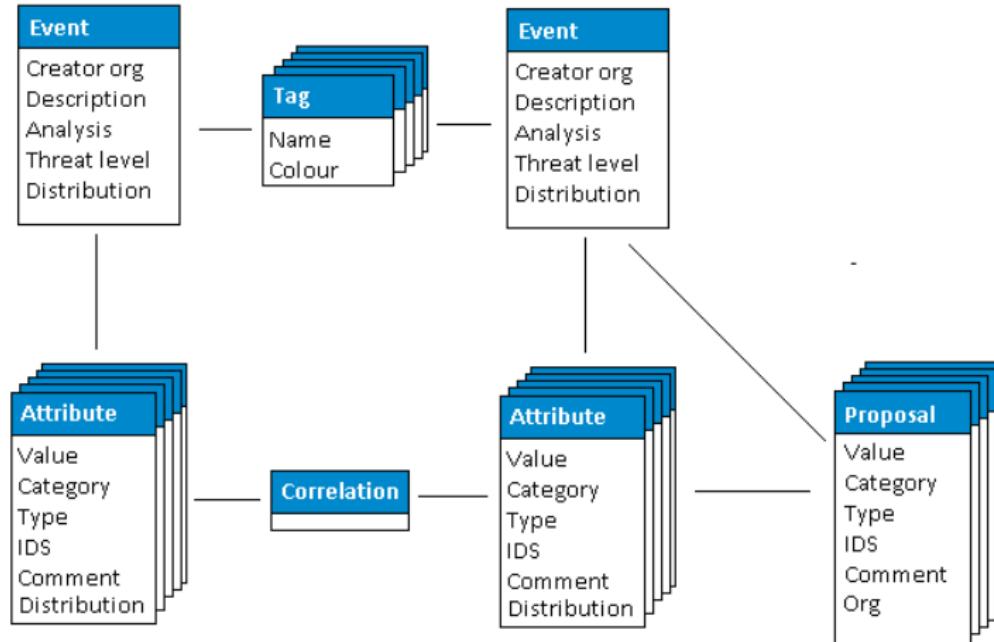
MISP - EVENT (CORRELATIONS ON SIMILAR ATTRIBUTES)



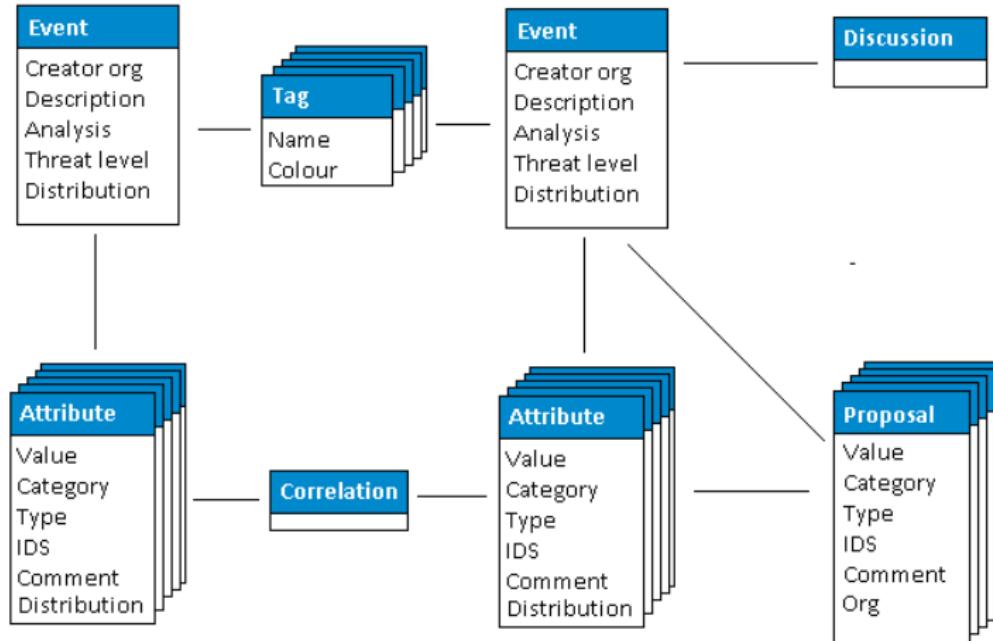
MISP - EVENT (PROPOSALS)



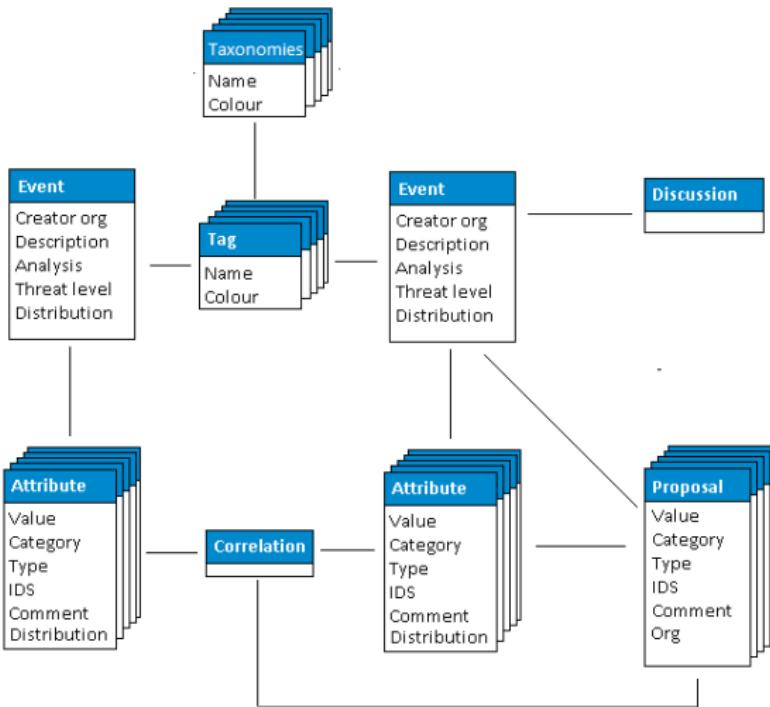
MISP - EVENT (TAGS)



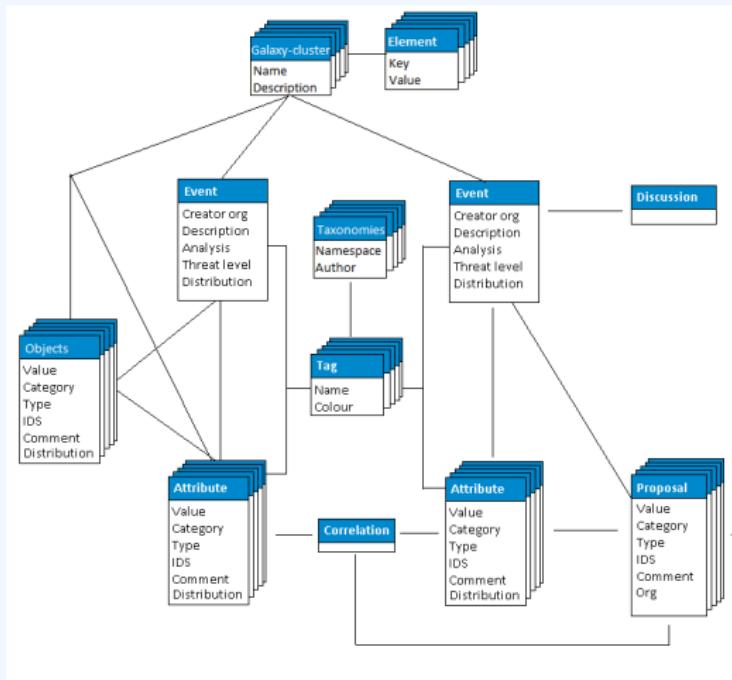
MISP - EVENT (DISCUSSIONS)



MISP - EVENT (TAXONOMIES AND PROPOSAL CORRELATIONS)



MISP - EVENT (THE STATE OF THE ART MISP DATAMODEL)



MISP - VIEWING THE EVENT INDEX

■ Event Index

- ▶ Event context
- ▶ Tags
- ▶ Distribution
- ▶ Correlations

■ Filters

MISP - VIEWING AN EVENT

- Event View
 - ▶ Event context
 - ▶ Attributes
 - Category/type, IDS, Correlations
 - ▶ Objects
 - ▶ Galaxies
 - ▶ Proposals
 - ▶ Discussions
- Tools to find what you are looking for
- Correlation graphs

MISP - CREATING AND POPULATING EVENTS IN VARIOUS WAYS (DEMO)

■ The main tools to populate an event

- ▶ Adding attributes / batch add
- ▶ Adding objects and how the object templates work
- ▶ Freetext import
- ▶ Import
- ▶ Templates
- ▶ Adding attachments / screenshots
- ▶ API

MISP - VARIOUS FEATURES WHILE ADDING DATA

- What happens automatically when adding data?
 - ▶ Automatic correlation
 - ▶ Input modification via validation and filters (regex)
 - ▶ Tagging / Galaxy Clusters
- Various ways to publish data
 - ▶ Publish with/without e-mail
 - ▶ Publishing via the API
 - ▶ Delegation

MISP - USING THE DATA

- Correlation graphs
- Downloading the data in various formats
- API (explained later)
- Collaborating with users (proposals, discussions, emails)

MISP - SYNC EXPLAINED (IF NO ADMIN TRAINING)

- Sync connections
- Pull/push model
- Previewing instances
- Filtering the sync
- Connection test tool
- Cherry pick mode

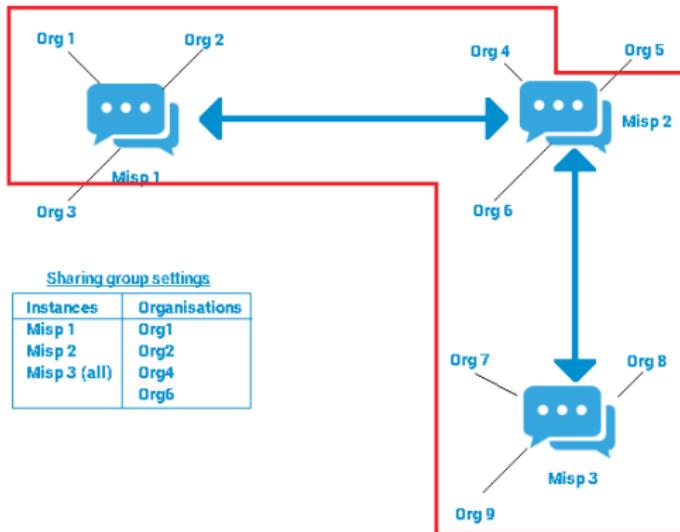
MISP - FEEDS EXPLAINED (IF NO ADMIN TRAINING)

- Feed types (MISP, Freetext, CSV)
- Adding/editing feeds
- Previewing feeds
- Local vs Network feeds

MISP - DISTRIBUTIONS EXPLAINED

- Your Organisation Only
- This Community Only
- Connected Communities
- All Communities
- Sharing Group

MISP - DISTRIBUTION AND TOPOLOGY



MISP - EXPORTS AND API

- Download an event
- Quick glance at the APIs
- Download search results
- ReST API and query builder

MISP - SHORTHAND ADMIN (IF NO ADMIN TRAINING)

- Settings
- Troubleshooting
- Workers
- Logs

MISP TRAINING: MISP DEPLOYMENT AND INTEGRATION

CIRCL / TEAM MISP PROJECT

[HTTP://WWW.MISP-PROJECT.ORG/](http://www.misp-project.org/)

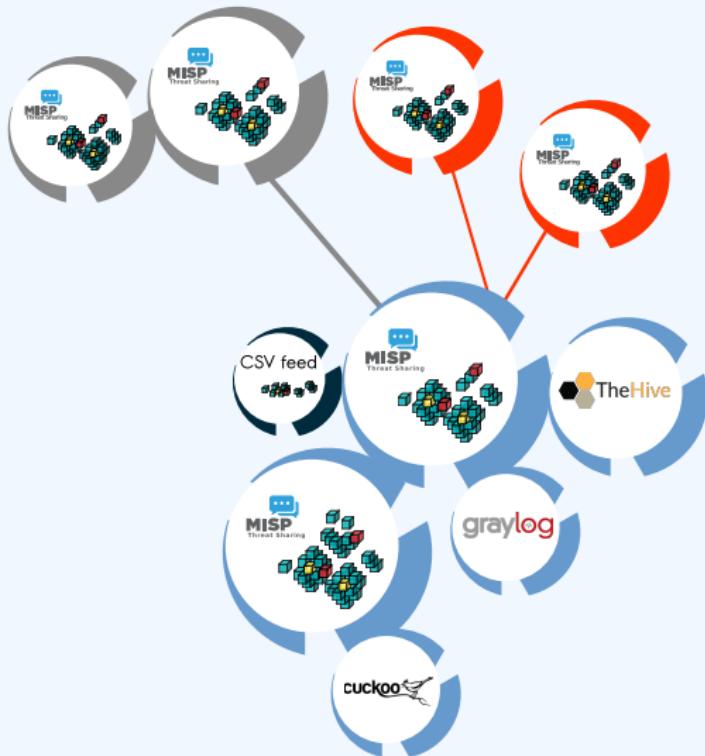
TWITTER: @MISPPROJECT

13TH ENISA-EC3 WORKSHOP



MISP
Threat Sharing

A COMMON INTEGRATION



RECOMMENDED MISP SETUP

- Provisioning your MISP infrastructure depends heavily on the **number of attributes/events** (whether your dataset is below or above 50 million attributes).
- Number of MISP instances and the overall design depends on the following factors:
 - ▶ Is your community private? Are you gathering MISP events from other communities? Are you **publishing events to external** (trusted/untrusted) communities.
 - ▶ Do you plan to have **automatic tools** (e.g. sandbox analysis or low-value information needing correlation or an analyst workbench) feeding MISP?

VENDORS AND FORMATS

- There is a **jungle of formats** with some vendors having little to no interest in keeping their users autonomous.
- Attacks and threats require a **dynamic format** to be efficiently shared (e.g. from financial indicators to personal information).
- **Review your current list of formats/vendors** to ensure a limited loss of information, especially when exporting from MISP to other formats (e.g. STIX not supporting financial indicators or taxonomies/galaxies).

USE CASE: NORMALIZING OSINT AND PRIVATE FEEDS

- Normalizing external input and feed into MISP (e.g. feed importer).
- Comparing feeds before import (how many similarities? false-positives?).
- Evaluating quality of information before import (warning-list lookup at feed evaluation).

CONNECTING DEVICES AND TOOLS TO MISP

- One of the main goals of MISP is to feed protective or detection tools with data
 - ▶ IDSSes / IPSses (e.g. Suricata, Bro, Snort format as included in Cisco products)
 - ▶ SIEMs (e.g. CEF, CSV or real-time ZMQ pub-sub or Sigma)
 - ▶ Host scanners (e.g. OpenIOC, STIX, yara rule-set, CSV)
 - ▶ Various analysis tools (e.g. Maltego)
 - ▶ DNS policies (e.g. RPZ)
- Various ways of exporting this data (downloads of the selected data, full exports, APIs)
- The idea was to leave the selection process of the subset of data to be pushed to these up to the user using APIs.

SIEM AND MISP INTEGRATION

- SIEMs and MISP can be integrated with different techniques depending on the processes at your SOC or IR:
 - ▶ Pulling events (via the API) or indicator lists at **regular intervals** in a given time frame to perform lookups.
 - ▶ Subscribing to the MISP ZMQ **pub-sub channel** to directly get the published events and use these in a lookup process.
 - ▶ **Lookup expansion module** in MISP towards the SIEM to have a direct view of the attributes matched against the SIEM.
- The above options can be combined, depending on your organisation or requirements to increase coverage and detection.

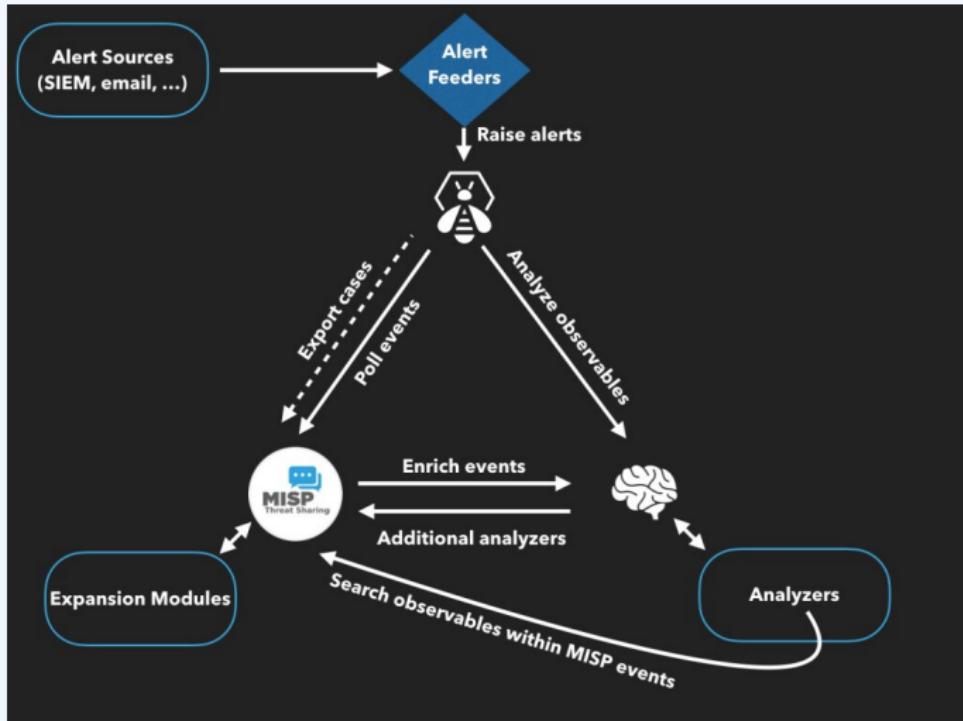
ZMQ INTEGRATION: MISP-DASHBOARD

- A dashboard showing live data and statistics from the ZMQ pub-sub of one or more MISP instances.
- Building **low-latency software** by consuming pub-sub channel provides significant advantages over standard API use.
- Process information in **real-time** when it's updated, created, published or gathered in MISP.
- Demo!

NEW INTEGRATIONS: IR AND THREAT HUNTING USING MISP

- Close co-operation with **the Hive project** for IR
 - ▶ Interact with MISP directly from the Hive
 - ▶ Use both the MISP modules and the **Cortex** analysers in MISP or the Hive directly
- Using MISP to support your threat hunting via **McAfee OpenDXL**
- (<https://securingtomorrow.mcafee.com/business/optimize-operations/expanding-automated-threat-hunting-response-open-dxl/>)

THE HIVE INTEGRATION



REPORTING BACK FROM YOUR DEVICES, TOOLS OR PROCESSES

As **Sightings** can be positive, negative or even based on expiration, different use cases are possible:

- **Sightings** allow users to notify a MISP instance about the activities related to an indicator.
- Activities can be from a SIEM (e.g. Splunk lookup validation or **false-positive feedback**), a NIDS or honeypot devices¹.
- Sighting can affect the API to limit the NIDS exports and improve the NIDS rule-set directly.

¹<https://www.github.com/MISP/misp-sighting-tools>

Q&A

- info@circl.lu (if you want to join the CIRCL MISP sharing community)
- <https://github.com/MISP/> -
<http://www.misp-project.org/>
- We welcome any contributions to the project, be it pull requests, ideas, github issues,...

VIPER - USING MISP FROM YOUR TERMINAL

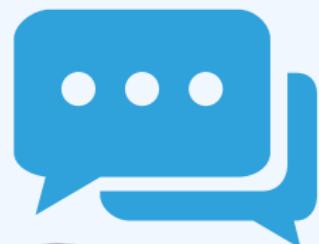
MISP - THREAT SHARING

CIRCL / TEAM MISP PROJECT

MISP PROJECT

<https://www.misp-project.org/>

13TH ENISA-EC3 WORKSHOP



MISP
Threat Sharing

VIPER - MAIN IDEAS

*Viper is a **binary analysis and management framework**. Its fundamental objective is to provide a solution to easily **organize** your collection of **malware** and **exploit samples** as well as your collection of **scripts** you created or found over the time to facilitate your daily research. Think of it as a **Metasploit for malware researchers**: it provides a terminal interface that you can use to **store, search and analyze** arbitrary files with and a framework to **easily create** **plugins** of any sort.*

- **Solid CLI**
- Plenty of modules (PE files, *office, ELF, APK, ...)
- Connection to **3rd party services** (MISP, VirusTotal, cuckoo)
- Connectors to **3rd party tools** (IDA, radare)
- **Locale storage** of your own zoo
- Django interface is available (I've been told)

Command	Description
apk	Parse Android Applications
clamav	Scan file from local ClamAV daemon
cuckoo	Submit the file to Cuckoo Sandbox
debug	Parse McAfee BUP Files
editdistance	Edit distance on the filenames
elf	Extract information from ELF headers
email	Parse eml and msg email files
exif	Extract Exif MetaData
fuzzy	Search for similar files through fuzzy hashing
html	Parse html files and extract content
ida	Start IDA Pro
idx	Parse Java IDX files
image	Perform analysis on images
jar	Parse Java JAR archives
koodous	Interact with Koodous
lastline	Submit files and retrieve reports from LastLine (default will print short summary)
macho	Get Macho OSX Headers
misp	Upload and query IOCs to/from a MISP instance
office	Office Document Parser
pdf	Parse and analyze PDF documents
pdns	Query a Passive DNS server
pe	Extract information from PE32 headers
pssl	Query a Passive SSL server
pst	Process PST Files for Attachment
r2	Start Radare2
rat	Extract information from known RAT families
reports	Online Sandboxes Reports
shellcode	Search for known shellcode patterns
size	Size command to show/scan/cluster files
strings	Extract strings from file
swf	Parse, analyze and decompress Flash objects
triage	Perform some initial triaging and tagging of the file

- Full featured **CLI for MISP**
- **Remote storage** of your zoo
- Search / **Cross check with VirusTotal**
- Create / Update / Show / Publish Event
- Download / Upload Samples
- Mass export / Upload / Download
- Get Yara rules

MISP MODULE

```
viper > misp -h
usage: misp [-h] [--url URL] [-k KEY] [-v]
           {upload,download,search,check_hashes,yara,pull,create_event,add,show,open,
publish,version,store}
           ...

Upload and query IOCs to/from a MISP instance

positional arguments:
  {upload,download,search,check_hashes,yara,pull,create_event,add,show,open,publish,ve
rsion,store}
    upload          Send malware sample to MISP.
    download        Download malware samples from MISP.
    search          Search in all the attributes.
    check_hashes   Crosscheck hashes on VT.
    yara            Get YARA rules of an event.
    pull             Initialize the session with an existing MISP event.
    create_event   Create a new event on MISP and initialize the session
                   with it.
    add              Add attributes to an existing MISP event.
    show             Show attributes to an existing MISP event.
    open             Open a sample from the temp directory.
    publish          Publish an existing MISP event.
    version          Returns the version of the MISP instance.
    store            Store the current MISP event in the current project.

optional arguments:
  -h, --help      show this help message and exit
  --url URL      URL of the MISP instance
  -k KEY, --key KEY Your key on the MISP instance
  -v, --verify    Disable certificate verification (for self-signed)
```

- Searches for hashes/ips/domains/URLs from the current MISP event, or download the samples
- Download samples from current MISP event
- Download all samples from all the MISP events of the current session

VIRUSTOTAL MODULE

```
Lookup the file on VirusTotal

optional arguments:
  -h, --help            show this help message and exit
  --search SEARCH      Search a hash.
  -c COMMENT [COMMENT ...], --comment COMMENT [COMMENT ...]
                        Comment to add to the file
  -d, --download        Hash of the file to download
  -dl, --download_list  List the downloaded files
  -do DOWNLOAD_OPEN, --download_open DOWNLOAD_OPEN
                        Open a file from the list of the DL files (ID)
  -don DOWNLOAD_OPEN_NAME, --download_open_name DOWNLOAD_OPEN_NAME
                        Open a file by name from the list of the DL files
                        (NAME)
  -dd DOWNLOAD_DELETE, --download_delete DOWNLOAD_DELETE
                        Delete a file from the list of the DL files can be an
                        ID or all.
  -s, --submit          Submit file or a URL to VirusTotal (by default it only
                        looks up the hash/url)
  -i IP, --ip IP        IP address to lookup in the passive DNS
  -dm DOMAIN, --domain DOMAIN
                        Domain to lookup in the passive DNS
  -u URL, --url URL    URL to lookup on VT
  -v, --verbose         Turn on verbose mode.
  -m {hashes,ips,domains,urls,download,download_all}, --misp {hashes,ips,domains,urls,
download,download_all}          Searches for the hashes, ips, domains or URLs from the
                                current MISP event, or download the samples if
                                possible. Be carefull with download_all: it will
                                download *all* the samples of all the MISP events in
                                the current project.
```

EXTRA FEATURES

- Link to a MISP event
- Local storage of the MISP event
- On the fly cross-check of MISP attributes with 3rd party services
- Never leaving your CLI!

OTHER MODULES

- Fully featured CLI for **Passive SSL**
- Fully featured CLI for **Passive DNS**
- Can launch Radare2 or IDA

PASSIVE SSL

```
viper > pssl -h
usage: pssl [-h] [--url URL] [-u USER] [-p PASSWORD] [-i IP] [-c CERT]
            [-f FETCH] [-v] [-m {ips}]

Query a Passive SSL server

optional arguments:
  -h, --help            show this help message and exit
  --url URL            URL of the Passive SSL server (No path)
  -u USER, --user USER  Username on the PSSL instance
  -p PASSWORD, --password PASSWORD
                        Password on the PSSL instance
  -i IP, --ip IP        IP to query (can be a block, max /23).
  -c CERT, --cert CERT  SHA1 of the certificate to search.
  -f FETCH, --fetch FETCH
                        SHA1 of the certificate to fetch.
  -v, --verbose         Turn on verbose mode.
  -m {ips}, --misp {ips} Searches for the ips from the current MISP event
```

PASSIVE DNS

```
viper > pdns -h
usage: pdns [-h] [--url URL] [-u USER] [-p PASSWORD] [-v] [-m {ips,domains}]
            [query]

Query a Passive DNS server

positional arguments:
  query                  Domain or IP address to query

optional arguments:
  -h, --help              show this help message and exit
  --url URL              URL of the Passive DNS server
  -u USER, --user USER   Username on the PDNS instance
  -p PASSWORD, --password PASSWORD
                        Password on the PDNS instance
  -v, --verbose           Turn on verbose mode.
  -m {ips,domains}, --misp {ips,domains}
                        Searches for the ips or domains from the current MISP
                        event
```

Q&A



- <https://github.com/MISP/PyMISP>
- <https://github.com/MISP/>
- <https://github.com/viper-framework/viper>
- We welcome new functionalities and pull requests.

MAIL_TO_MISP

CONNECT YOUR MAIL INFRASTRUCTURE TO MISP TO

CIRCL / TEAM MISP PROJECT

[HTTP://WWW.MISP-PROJECT.ORG/](http://www.misp-project.org/)

TWITTER: @MISPPROJECT

13TH ENISA-EC3 WORKSHOP



MISP
Threat Sharing

CONTEXT

- You receive emails with IoC's inside
- How to create an event out of it?
- Create event manually and copy paste
- → This works once or twice
- Forwarding the email would be nice
- → mail_to_misp

FEATURES: EMAIL HANDLING

- Extraction of URLs and IP addresses and port numbers
- Extraction of hostnames from URLs
- Extraction of hashes (MD5, SHA1, SHA256)
- DNS expansion
- Subject filters
- Refanging of URLs ('hxxp://...')
- ... and more

FEATURES: SUPPORT MISP FEATURES

- Add tags automatically
- Ignore 'whitelisted' domains
- Configurable list of attributes not to enable the IDS flag
- DNS expansion
- Automatically create 'external analysis' links based on filter list (e.g. VirusTotal, malwr.com)
- Automatically filter out attributes that are on a server side warning list
- Support for value sighting
- ... and more

IMPLEMENTATION

■ Legacy

- ▶ Email → Apple Mail → Mail rule → AppleScript
→ AppleScript → mail_to_misp → PyMISP → MISP

- ▶ Email → Thunderbird → Mail rule → filterscript →
thunderbird_wrapper → mail_to_misp → PyMISP → MISP

■ Postfix and others

- ▶ Email → mail_to_misp

INSTALLATION

■ mail_to_misp

1. git clone

```
git://github.com/MISP/mail_to_misp.git
```

2. Install dependencies - See Github site

■ MTA (Postfix or alike)

1. Setup a new email address in the aliases file (e.g.
`/etc/aliases`)

```
misp_handler:  "|/path/to/mail_to_misp.py -"
```

2. Rebuild the DB

```
sudo newaliases
```

3. Configure `mail_to_misp_config.py`

```
misp_url = 'http://127.0.0.1/'  
misp_key = 's5jPWClud36Z8XHgsiCVI7SaL1XsMTyfEsN45tTe'  
misp_verifycert = True  
body_config_prefix = 'm2m'  
...  
...
```

EXERCISE: MAIL_2_MISP.PY

■ Bonus:

https://github.com/MISP/mail_to_misp_test

```
./mail_to_misp.py -r mail_to_misp_test/simple_forward.eml
```

■ Bonus: Fake-SMTPD spamtrap

```
./fake_smtp.py
```

```
telnet 127.0.0.1 2526
Trying 127.0.0.1...
Connected to 127.0.0.1.
Escape character is '^>'.
220 misp Python SMTP 1.1
helo misp
250 misp
mail from: mikel
250 OK
rcpt to: m2m
250 OK
data
354 End data with <CR><LF>.<CR><LF>
```

MISP USER TRAINING - ADMINISTRATION OF MISP 2.4

MISP THREAT SHARING

CIRCL / TEAM MISP PROJECT

[HTTP://WWW.MISP-PROJECT.ORG/](http://www.misp-project.org/)

TWITTER: @MISPPROJECT

13TH ENISA-EC3 WORKSHOP



MISP
Threat Sharing

- VM can be downloaded at
<https://www.circl.lu/misp-training/>
- Credentials
 - ▶ MISP admin: admin@admin.test/admin
 - ▶ SSH: misp/Password1234
- 2 network interfaces
 - ▶ NAT
 - ▶ Host only adapter
- Start the enrichment system by typing:
 - ▶ cd /home/misp/misp-modules/bin
 - ▶ python3 misp-modules.py

■ Plan for this part of the training

- ▶ User and Organisation administration
- ▶ Sharing group creation
- ▶ Templates
- ▶ Tags and Taxonomy
- ▶ Whitelisting and Regexp entries
- ▶ Setting up the synchronisation
- ▶ Scheduled tasks
- ▶ Feeds
- ▶ Settings and diagnostics
- ▶ Logging
- ▶ Troubleshooting and updating

MISP - CREATING USERS

- Add new user (`andras.iklody@circl.lu`)
- NIDS SID, Organisation, disable user
- Fetch the PGP key
- Roles
 - ▶ Re-using standard roles
 - ▶ Creating a new custom role
- Send out credentials

MISP - CREATING ORGANISATIONS

- Adding a new organisation
- UUID
- Local vs External organisation
- Making an organisation self sustaining with Org Admins
- Creating a sync user

MISP - SHARING GROUPS

- The concept of a sharing group
- Creating a sharing group
- Adding extending rights to an organisation
- Include all organisations of an instance
- Not specifying an instance
- Making a sharing group active
- Reviewing the sharing group

- Why templating?
- Create a basic template
- Text fields
- Attribute fields
- Attachment fields
- Automatic tagging

MISP - TAGS AND TAXONOMIES

- git submodule init && git submodule update
- Loading taxonomies
- Enabling taxonomies and associated tags
- Tag management
- Exportable tags

MISP - OBJECT TEMPLATES

- git submodule init && git submodule update
- Enabling objects (and what about versioning)

MISP - WHITELISTING, REGEXP ENTRIES, WARNINGLISTS

- Block from exports - whitelisting
- Block from imports - blacklisting via regexp
- Modify on import - modification via regexp
- Maintaining the warninglists

MISP - SETTING UP THE SYNCHRONISATION

- Requirements - versions
- Pull/Push
- One way vs Two way synchronisation
- Exchanging sync users
- Certificates
- Filtering
- Connection test tool
- Previewing an instance
- Cherry picking and keeping the list updated

MISP - SCHEDULED TASKS

- How to schedule the next execution
- Frequency, next execution
- What happens if a job fails?

MISP - SETTING UP THE SYNCHRONISATION

- MISP Feeds and their generation
- PyMISP
- Default free feeds
- Enabling a feed
- Previewing a feed and cherry picking
- Feed filters
- Auto tagging

■ Settings

- ▶ Settings interface
- ▶ The tabs explained at a glance
- ▶ Issues and their severity
- ▶ Setting guidance and how to best use it

MISP - SETTINGS AND DIAGNOSTICS CONTINUED

- Basic instance setup
- Additional features released as hotfixes
- Customise the look and feel of your MISP
- Default behaviour (encryption, e-mailing, default distributions)
- Maintenance mode
- Disabling the e-mail alerts for an initial sync

MISP - SETTINGS AND DIAGNOSTICS CONTINUED

- Plugins
 - ▶ Enrichment Modules
 - ▶ RPZ
 - ▶ ZeroMQ

MISP - SETTINGS AND DIAGNOSTICS CONTINUED

■ Diagnostics

- ▶ Updating MISP
- ▶ Writeable Directories
- ▶ PHP settings
- ▶ Dependency diagnostics

■ Workers

- ▶ What do the background workers do?
- ▶ Queues
- ▶ Restarting workers, adding workers, removing workers
- ▶ Worker diagnostics (queue size, jobs page)
- ▶ Clearing worker queues
- ▶ Worker and background job debugging

■ Seeking help

- ▶ Dump your settings to a file!
- ▶ Make sure to sanitise it
- ▶ Send it to us together with your issue to make our lives easier
- ▶ Ask Github (<https://github.com/MISP/MISP>)
- ▶ Have a chat with us on gitter (<https://gitter.im/MISP/MISP>)
- ▶ Ask the MISP mailing list
- ▶ If this is security related, drop us a PGP encrypted email to <mailto:info@circl.lu>

MISP - LOGGING

- Audit logs in MISP
- Enable IP logging / API logging
- Search the logs, the fields explained
- External logs
 - ▶ `/var/www/MISP/app/tmp/logs/error.log`
 - ▶ `/var/www/MISP/app/tmp/logs/resque-worker-error.log`
 - ▶ `/var/www/MISP/app/tmp/logs/resque-scheduler-error.log`
 - ▶ `/var/www/MISP/app/tmp/logs/resque-[date].log`
 - ▶ `/var/www/MISP/app/tmp/logs/error.log`
 - ▶ apache access logs

MISP - UPDATING MISP

- git pull
- git submodule init && git submodule update
- reset the permissions if it goes wrong according to the INSTALL.txt
- when MISP complains about missing fields, make sure to clear the caches
 - ▶ in /var/www/MISP/app/tmp/cache/models remove myapp*
 - ▶ in /var/www/MISP/app/tmp/cache/persistent remove myapp*
- No additional action required on hotfix level
- Read the migration guide for major and minor version changes

MISP - ADMINISTRATIVE TOOLS

- Upgrade scripts for minor / major versions
- Maintenance scripts

INFORMATION SHARING AND TAXONOMIES

PRACTICAL CLASSIFICATION OF THREAT INDICATORS US-

CIRCL / TEAM MISP PROJECT

[HTTP://WWW.MISP-PROJECT.ORG/](http://www.misp-project.org/)

TWITTER: @MISPPROJECT

13TH ENISA-EC3 WORKSHOP



MISP
Threat Sharing

FROM TAGGING TO FLEXIBLE TAXONOMIES

OSINT - Fancy Bear Source Code

Event ID	5703
Uuid	58724cbf-5508-4425-ab89-4f61950d210f
Org	CIRCL
Owner org	CIRCL
Contributors	
Email	alexandre.dulaunoy@circl.lu
Tags	<code>tip:white</code> <code>osint:certainty="75"</code> <code>osint:source-type="source-code-repository"</code> <code>circl:osint-feed</code> <code>ms-caro-malware:malware-platform="Python"</code>
Date	2017-01-08
Threat Level	Medium
Analysis	Initial
Distribution	All communities
Info	OSINT - Fancy Bear Source Code
Published	<code>Yes</code>
Sightings	0 (0)
Activity	

- Tagging is a simple way to attach a classification to an event or an attribute.
- In the early version of MISP, tagging was local to an instance.
- **Classification must be globally used to be efficient.**
- After evaluating different solutions of classification, we built a new scheme using the concept of machine tags.

MACHINE TAGS

- Triple tag, or machine tag, format was introduced in 2004 to extend geotagging on images.

admiralty-scale:source-reliability="c"

The diagram illustrates the structure of a triple tag. It consists of three horizontal bars: a blue bar labeled "namespace", a purple bar labeled "predicate", and a green bar labeled "value". The text "admiralty-scale:source-reliability="c"" is positioned above these bars, with each part aligned under its respective color-coded bar. The "c" at the end is enclosed in double quotes.

namespace predicate value

- A machine tag is just a tag expressed in way that allows systems to parse and interpret it.
- Still have a human-readable version:
 - ▶ admiralty-scale:source-reliability="Fairly reliable"

MISP TAXONOMIES

- Taxonomies are implemented in a simple JSON format.
- Anyone can create their own taxonomy or reuse an existing one.
- The taxonomies are in an independent git repository¹.
- These can be freely reused and integrated into other threat intel tools.
- Taxonomies are licensed under Creative Commons (public domain) except if the taxonomy author decided to use another license.

¹<https://www.github.com/MISP/misp-taxonomies/>

EXISTING TAXONOMIES

- NATO - **Admiralty Scale**
- CIRCL Taxonomy - **Schemes of Classification in Incident Response and Detection**
- eCSIRT and IntelMQ incident classification
- EUCL **EU classified information marking**
- Information Security Marking Metadata from DNI (Director of National Intelligence - US)
- NATO Classification Marking
- OSINT **Open Source Intelligence - Classification**
- TLP - **Traffic Light Protocol**
- Vocabulary for Event Recording and Incident Sharing - **VERIS**
- And many more like ENISA, Europol, or the draft FIRST SIG Information Exchange Policy.

WANT TO WRITE YOUR OWN TAXONOMY? 1/2

```
1 {
2   "namespace": "admiralty-scale",
3   "description": "The Admiralty Scale (also called the NATO System
4                  ) is used to rank the reliability of a source and the
5                  credibility of an information.",
6   "version": 1,
7   "predicates": [
8     {
9       "value": "source-reliability",
10      "expanded": "Source Reliability"
11    },
12    {
13      "value": "information-credibility",
14      "expanded": "Information Credibility"
15    }
16  ],
17  ....
```

WANT TO WRITE YOUR OWN TAXONOMY? 2/2

```
1  {
2      "values": [
3          {
4              "predicate": "source-reliability",
5              "entry": [
6                  {
7                      "value": "a",
8                      "expanded": "Completely reliable"
9                  },
10                 ...
11             ]
12         }
13     ]
14 }
```

- Publishing your taxonomy is as easy as a simple git pull request on misp-taxonomies².

²<https://github.com/MISP/misp-taxonomies>

HOW ARE TAXONOMIES INTEGRATED IN MISP?

18	✓	✗	admiralty-scale:information-credibility-="1"	admiralty-scale	4	0		<input type="checkbox"/>		
19	✓	✗	admiralty-scale:information-credibility-="2"	admiralty-scale	15	1		<input type="checkbox"/>		
20	✓	✗	admiralty-scale:information-credibility-="3"	admiralty-scale	12	4		<input type="checkbox"/>		
21	✓	✗	admiralty-scale:information-credibility-="4"	admiralty-scale	1	0		<input type="checkbox"/>		
22	✓	✗	admiralty-scale:information-credibility-="5"	admiralty-scale	1	0		<input type="checkbox"/>		
23	✓	✗	admiralty-scale:information-credibility-="6"	admiralty-scale	2	0		<input type="checkbox"/>		
12	✓	✗	admiralty-scale:source-reliability-="a"	admiralty-scale	0	0		<input type="checkbox"/>		
13	✓	✗	admiralty-scale:source-reliability-="b"	admiralty-scale	15	53		<input type="checkbox"/>		
14	✓	✗	admiralty-scale:source-reliability-="c"	admiralty-scale	5	2		<input type="checkbox"/>		
15	✓	✗	admiralty-scale:source-reliability-="d"	admiralty-scale	1	0		<input type="checkbox"/>		
16	✓	✗	admiralty-scale:source-reliability-="e"	admiralty-scale	0	0		<input type="checkbox"/>		
17	✓	✗	admiralty-scale:source-reliability-="f"	admiralty-scale	4	2		<input type="checkbox"/>		
1203	✓	✗	adversary:infrastructure-action-="monitoring-active"	adversary	1	0		<input type="checkbox"/>		
1201	✓	✗	adversary:infrastructure-action-="passive-only"	adversary	0	0		<input type="checkbox"/>		

- MISP administrator can just import (or even cherry pick) the namespace or predicates they want to use as tags.
- Tags can be exported to other instances.
- Tags are also accessible via the MISP REST API.

FILTERING THE DISTRIBUTION OF EVENTS AMONG MISP INSTANCES

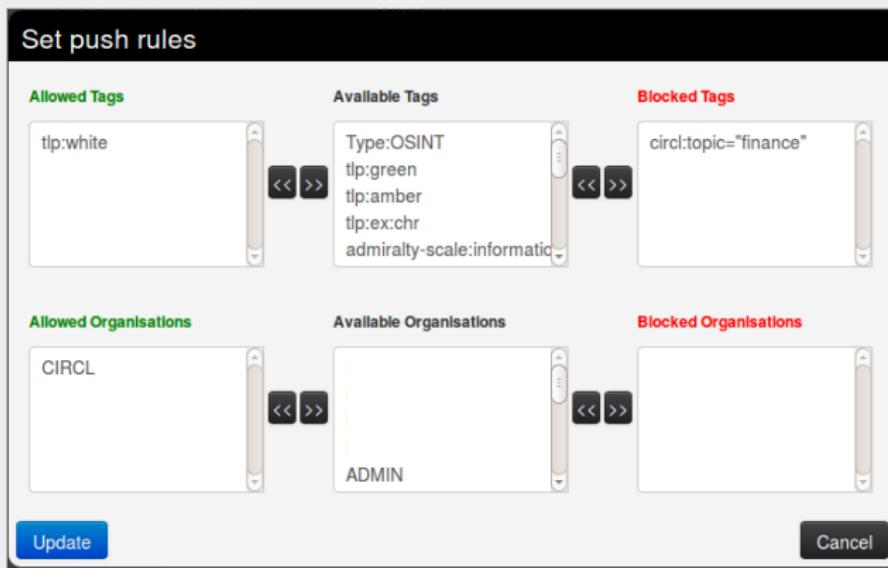
■ Applying rules for distribution based on tags:

Set push rules

Allowed Tags	Available Tags	Blocked Tags
tlp:white	Type:OSINT tlp:green tlp:amber tlp:ex:chr admiralty-scale:informatic	circl:topic="finance"

Allowed Organisations	Available Organisations	Blocked Organisations
CIRCL	ADMIN	

Update **Cancel**

The screenshot shows a 'Set push rules' dialog box. It has two main sections: 'Tags' and 'Organizations'.

Tags Section:

- Allowed Tags:** Contains the tag "tlp:white".
- Available Tags:** Contains "Type:OSINT", "tlp:green", "tlp:amber", "tlp:ex:chr", and "admiralty-scale:informatic".
- Blocked Tags:** Contains "circl:topic='finance'".

Organizations Section:

- Allowed Organisations:** Contains the organization "CIRCL".
- Available Organisations:** Contains "ADMIN".
- Blocked Organisations:** Contains nothing.

At the bottom left is a blue 'Update' button, and at the bottom right is a black 'Cancel' button.

OTHER USE CASES USING MISP TAXONOMIES

- Tags can be used to set events or attributes for **further processing by external tools** (e.g. VirusTotal auto-expansion using Viper).
- Ensuring a classification manager **classifies the events before release** (e.g. release of information from air-gapped/classified networks).
- **Enriching IDS export** with tags to fit your NIDS deployment.
- Using **IntelMQ** and MISP together to process events (tags limited per organization introduced in MISP 2.4.49).

FUTURE FUNCTIONALITIES RELATED TO MISP TAXONOMIES

- **Sighting** support (thanks to NCSC-NL) is integrated in MISP allowing to auto expire IOC based on user detection.
- Adjusting taxonomies (adding/removing tags) based on their score or visibility via sighting.
- Simple taxonomy editors to **help non-technical users** to create their taxonomies.
- **Filtering mechanisms** in MISP to rename or replace taxonomies/tags at pull and push synchronisation.
- More public taxonomies to be included.

- **Python module** to handle the taxonomies
- **Offline** and online mode (fetch the newest taxonomies from GitHub)
- Simple **search** to make tagging easy
- Totally independent from MISP
- **No external dependencies** in offline mode
- Python3 only
- Can be used to create & **dump a new taxonomy**

PYTAXONOMIES

```
from pytaxonomies import Taxonomies
taxonomies = Taxonomies()
taxonomies.version
# => '20160725'
taxonomies.description
# => 'Manifest file of MISP taxonomies available.'
list(taxonomies.keys())
# => ['tlp', 'eu-critical-sectors', 'de-vs', 'osint', 'circl', 'veris',
#      'ecsirt', 'dhs-ciip-sectors', 'fr-classif', 'misp', 'admiralty-scale', ...]
taxonomies.get('enisa').description
# 'The present threat taxonomy is an initial version that has been developed on
# the basis of available ENISA material. This material has been used as an ENISA-internal
# structuring aid for information collection and threat consolidation purposes.
# It emerged in the time period 2012-2015.'
print(taxonomies.get('circl'))
# circl:incident-classification="vulnerability"
# circl:incident-classification="malware"
# circl:incident-classification="fastflux"
# circl:incident-classification="system-compromise"
# circl:incident-classification="sql-injection"
# ....
print(taxonomies.get('circl').machinetags_expanded())
# circl:incident-classification="Phishing"
# circl:incident-classification="Malware"
# circl:incident-classification="XSS"
# circl:incident-classification="Copyright issue"
# circl:incident-classification="Spam"
# circl:incident-classification="SQL Injection"
```

THE DILEMMA OF FALSE-POSITIVES

- False-positives are a **common issue** in threat intelligence sharing.
- It's often a contextual issue:
 - ▶ False-positives might be different per community of users sharing information.
 - ▶ Organizations might have their **own view** on false-positives.
- Based on the success of the MISP taxonomy model, we built misp-warninglists.

MISP WARNING LISTS

- misp-warninglists are lists of well-known indicators that can be associated to potential false positives, errors, or mistakes.
- Simple JSON files

```
1 {  
2     "name": "List of known public DNS resolvers",  
3     "version": 2,  
4     "description": "Event contains one or more public DNS resolvers  
5         as attribute with an IDS flag set",  
6     "matching_attributes": [  
7         "ip-src",  
8         "ip-dst"  
9     ],  
10    "list": [  
11        "8.8.8.8",  
12        "8.8.4.4", ...]  
13 }
```

MISP WARNING LISTS

- The warning lists are integrated in MISP to display an info/warning box at the event and attribute level.
- Enforceable via the API where all attributes that have a hit on a warninglist will be excluded.
- This can be enabled at MISP instance level.
- Default warning lists can be enabled or disabled like **known public resolver**, **multicast IP addresses**, **hashes for empty values**, **rfc1918**, **TLDs** or **known Google domains**.
- The warning lists can be expanded or added in JSON locally or via pull requests.
- Warning lists can be also used for **critical or core infrastructure warning**, **personally identifiable information...**

Q&A



- <https://github.com/MISP/MISP>
- <https://github.com/MISP/misp-taxonomies>
- <https://github.com/MISP/PyTaxonomies>
- <https://github.com/MISP/misp-warninglists>
- info@circl.lu (if you want to join one of the MISP community operated by CIRCL)
- PGP key fingerprint: CA57 2205 C002 4E06 BA70 BE89 EAAD CFFC 22BD 4CD5

EXTENDING MISP WITH PYTHON MODULES

MISP - THREAT SHARING

CIRCL / TEAM MISP PROJECT

[HTTP://WWW.MISP-PROJECT.ORG/](http://www.misp-project.org/)

TWITTER: @MISPPROJECT

13TH ENISA-EC3 WORKSHOP



MISP
Threat Sharing

WHY WE WANT TO GO MORE MODULAR...

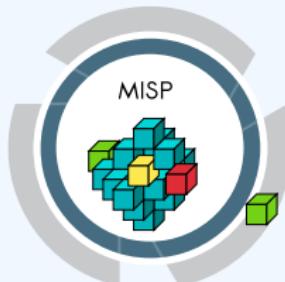
■ Ways to extend MISP before modules

- ▶ APIs (PyMISP, MISP API)
 - Works really well
 - **No integration with the UI**
- ▶ Change the core code
 - Have to change the core of MISP, diverge from upstream
 - Needs a deep understanding of MISP internals
 - Let's not beat around the bush: **Everyone hates PHP**

GOALS FOR THE MODULE SYSTEM

- Have a way to extend MISP without altering the core
- Get started **quickly** without a need to study the internals
- Make the **modules as light weight as possible**
 - ▶ Module developers should only have to worry about the data transformation
 - ▶ Modules should have a simple and clean skeleton
- In a friendlier language - **Python**

MISP MODULES - EXTENDING MISP WITH PYTHON SCRIPTS



- MISP expansion modules
 - IP address expansion
 - VirusTotal
 - VIPER modules
 - Your module

- Extending MISP with expansion modules with zero customization in MISP.
- A simple ReST API between the modules and MISP allowing auto-discovery of new modules with their features.
- Benefit from existing Python modules in Viper or any other tools.
- MISP modules functionnality introduced in MISP 2.4.28.
- MISP import/export modules introduced in MISP 2.4.50.

MISP MODULES - INSTALLATION

- MISP modules can be run on the same system or on a remote server.
- Python 3 is required to run MISP modules.
 - ▶ sudo apt-get install python3-dev python3-pip libpq5
 - ▶ cd /usr/local/src/
 - ▶ sudo git clone https://github.com/MISP/misp-modules.git
 - ▶ cd misp-modules
 - ▶ sudo pip3 install -I -r REQUIREMENTS
 - ▶ sudo pip3 install -I .
 - ▶ sudo vi /etc/rc.local, add this line: 'sudo -u www-data misp-modules -s &'

MISP MODULES - SIMPLE REST API MECHANISM

- <http://127.0.0.1:6666/modules> - introspection interface to get **all modules available**
 - ▶ returns a JSON with a description of each module
- <http://127.0.0.1:6666/query> - interface to **query a specific module**
 - ▶ to send a JSON to query the module
- MISP **autodiscovers** the available modules and the MISP site administrator can enable modules as they wish.
- If a configuration is required for a module, **MISP adds automatically the option** in the server settings.

FINDING AVAILABLE MISP MODULES

■ curl -s http://127.0.0.1:6666/modules | jq .

```
1   {
2     "type": "expansion",
3     "name": "dns",
4     "meta": {
5       "module-type": [
6         "expansion",
7         "hover"
8       ],
9       "description": "Simple DNS expansion service
10      to resolve IP address from MISP
11      attributes",
12      "author": "Alexandre Dulaunoy",
13      "version": "0.1"
14    },
15    "mispattributes": {
16      "output": [
17        "ip-src",
18        "ip-dst"
19      ],
20      "input": [
21        "hostname",
22        "domain"
23      ]
24    }
25 }
```

MISP MODULES - CONFIGURATION IN THE UI

Server settings

Overview MISP settings (18) GnuPG settings (3) Proxy settings (5) Security settings (2) Misc settings (1) Plugin settings (22)				Diagnostics	Workers
Enrichment					
Priority	Setting	Value	Description		
Critical	Plugin.Enrichment_services_enable	true	Enable/disable the enrichment module		
Recommended	Plugin.Enrichment_services_url	http://127.0.0.1	The url used to access the enrichment service		
Recommended	Plugin.Enrichment_services_port	6666	The port used to access the enrichment service		
Recommended	Plugin.Enrichment_cve_enabled	false	Enable or disable the cve module		
Recommended	Plugin.Enrichment_dns_enabled	true	Enable or disable the dns module		
Recommended	Plugin.Enrichment_sourcecache_enabled	false	Enable or disable the sourcecache module		
Recommended	Plugin.Enrichment_sourcecache_archivepath		Set this required module specific path		
Recommended	Plugin.Enrichment_passivetotal_enabled	true	Enable or disable the passivetotal module		
Recommended	Plugin.Enrichment_passivetotal_username	alexandre.dulaunoy@circl.lu	Set this required module specific username		
Recommended	Plugin.Enrichment_passivetotal_password		Set this required module specific password		

MISP MODULES - HOW IT'S INTEGRATED IN THE UI?

Filters: All File Network Financial Proposal Correlation				
Value	Comment	Related Events	ID \$	Distribution
microsoft.com			No	Inherit
google.com	25		No	Inherit
circl.lu			No	Inherit

Modules → Discussion

Choose the enrichment module that you wish to use for the expansion

dns

Cancel

Filters: All File Network Financial Proposal Correlation				
Org	Category	Type	Value	Comment
3	Network activity	domain	microsoft.com	
3	Network activity	domain	google.com	25
3	Network activity	domain	circl.lu	

Enrichment 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.

Value	Category	Type	ID \$	Comment	Actions
23.100.122.175	Network activity	ip-src		Imported via the freetext import.	x

Submit

ip-src → ip-dst Change all

Update all comment fields Change all

MISP MODULES - MAIN TYPES OF MODULES

- Expansion modules - enrich data that is in MISP
 - ▶ Hover type - showing the expanded values directly on the attributes
 - ▶ Expansion type - showing and adding the expanded values via a proposal form
- Import modules - import new data into MISP
- Export modules - export existing data from MISP

QUERYING A MODULE

- curl -s http://127.0.0.1:6666/query -H "Content-Type: application/json" -data @body.json -X POST

body.json

```
1 {"module": "dns", "hostname": "www.circl.lu"}
```

- and the response of the dns module:

```
1 {"results": [{"values": ["149.13.33.14"],  
2 "types": ["ip-src", "ip-dst"]}]}
```

CREATING YOUR MODULE - DNS MODULE

```
import json
import dns.resolver
misperrors = {'error': 'Error'}
mispattributes = {'input': ['hostname', 'domain', 'domain|ip'], 'output': ['ip-src','ip-dst']}
moduleinfo = {'version': '0.3', 'author': 'Alexandre Dulaunoy', 'description': 'Simple DNS expansion service to resolve IP address from MISP attributes', 'module-type': ['expansion', 'hover']}
moduleconfig = ['nameserver']

def handler(q=False):
    if q is False:
        return False
    request = json.loads(q)
    if request.get('hostname'):
        toquery = request['hostname']
    elif request.get('domain'):
        toquery = request['domain']
    elif request.get('domain|ip'):
        toquery = request['domain|ip'].split('|')[0]
    else:
        return False
    r = dns.resolver.Resolver()
    r.timeout = 2
    r.lifetime = 2

    if request.get('config'):
        if request['config'].get('nameserver'):
            nameservers = []
            nameservers.append(request['config'].get('nameserver'))
            r.nameservers = nameservers
        else:
            r.nameservers = ['8.8.8.8']

    try:
        answer = r.resolve(tquery, 'A')
    except dns.resolver.NXDOMAIN:
        misperrors['error'] = "NXDOMAIN"
        return misperrors
    except ...
        pass

    return {'results': [{}{'types': mispattributes['output'], 'values':str(answer[0])}]}

def introspection():
    return mispattributes

def version():
    moduleinfo['config'] = moduleconfig
    return moduleinfo
```

TESTING YOUR MODULE

- Copy your module dns.py in modules/expansion/
- Restart the server misp-modules.py

```
[adulau:~/git/misp-modules/bin]$ python3 misp-modules.py
2016-03-20 19:25:43,748 - misp-modules - INFO - MISP modules passivetotal imported
2016-03-20 19:25:43,787 - misp-modules - INFO - MISP modules sourcecache imported
2016-03-20 19:25:43,789 - misp-modules - INFO - MISP modules cve imported
2016-03-20 19:25:43,790 - misp-modules - INFO - MISP modules dns imported
2016-03-20 19:25:43,797 - misp-modules - INFO - MISP modules server started on TCP port 6666
```

- Check if your module is present in the introspection
- curl -s http://127.0.0.1:6666/modules
- If yes, test it directly with MISP or via curl

CODE SAMPLES (CONFIGURATION)

```
# Configuration at the top
moduleconfig = ['username', 'password']

# Code block in the handler
if not request.get('config'):
    return {'error': 'CIRCL Passive SSL authentication is missing.'}

if not request['config'].get('username') or not request['config'].get('password'):
    return {'error': 'CIRCL Passive SSL authentication is incomplete, please provide your username and password.'}
authentication = (request['config']['username'], request['config']['password'])

if not request.get('attribute') or not check_input_attribute(request['attribute']):
    return {'error': f'{standard_error_message}, which should contain at least a type, a value and an uuid.'}
attribute = request['attribute']

pssl_parser = PassiveSSLPParser(attribute, authentication)
```

DEFAULT EXPANSION MODULE SET

- asn history
- CIRCL Passive DNS
- CIRCL Passive SSL
- Country code lookup
- CVE information expansion
- DNS resolver
- DomainTools
- eupi (checking url in phishing database)
- ipasn
- PassiveTotal -
<http://blog.passivetotal.org/misp-sharing-done-differently>
- sourcecache
- Virustotal
- Whois
- ...

IMPORT MODULES

- Similar to expansion modules
- Input is a file upload or a text paste
- Output is a list of parsed attributes to be editend and verified by the user
- Some examples
 - ▶ Cuckoo JSON import
 - ▶ email import
 - ▶ OCR module
 - ▶ Open IoC import

EXPORT MODULES

- Not the preferred way to export data from MISP
- Input is currently only a single event
- Output is a file in the export format served back to the user
- Will be moved / merged with MISP built-in export modules
 - ▶ Allows export of event / attribute collections

NEW EXPANSION & IMPORT MODULES FORMAT

- Backward compatible - an additional field to extend the format

```
misp_attributes = {'input': [...], 'output': [...],  
                    'format': 'misp_standard'}
```

- Takes a standard MISP attribute as input

- Returns MISP format

- ▶ Attributes
- ▶ Objects (with their references)
- ▶ Tags

```
results = {'Attribute': [...], 'Object': [...],  
           'Tag': [...]}
```

- First modules supporting this new export format

- ▶ urlhaus expansion module
- ▶ Joe Sandbox import & query module

NEW EXPANSION & IMPORT MODULES VIEW (MISP 2.4.110)

Enrichment Results

Below you can see the attributes and objects that are to be created from the results of the enrichment module.

Event ID	1229	UUID	Tags	ID5	Disable Correlation	Comment	Distribution
Event UUID	5cc3042c-8bb4-4837-9564-47aca964451a						
Event creator org	ORDNAME						
Event info	virustotal test						
#Resolved Attributes	14 (2 Objects)						
Category	Type	Value					
Name: virustotal-report	+						Inherit event
References:	0						
Other	detection-ratio: text	10 / 66	ad:32:de-4651-41a1-a55b-5a1b39fe4be1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	[2b701d43a43315105d649612b2]	Inherit event
External analysis	permalink: link	https://www.virustotal.com/file/d3fd6f911b00e1d64eb08a29febc0dc2fa73017b6bdcf78579ef47552ed552ed/analysis/1554403108/	40b3d105-5e01-48c7-94e7-be2b289427b	<input type="checkbox"/>	<input type="checkbox"/>	[2b701d43a43315105d649612b2]	Inherit event
ID: 12700	Name: file						Inherit event
References:	11						
Payload delivery	sha256: sha256	d3fd6f911b00e1d64eb08a29febc0dc2fa73017b6bdcf78579ef47552ed	5026ab08-8fc8-49e4-a485-b69e92d02950	<input checked="" type="checkbox"/>	<input type="checkbox"/>	[2b701d43a43315105d649612b2]	Inherit event
Other	size-in-bytes: size-in-bytes	98304	9eeff4454-fa8f-4210-a88a-e401569047f1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	[2b701d43a43315105d649612b2]	Inherit event
Network activity	url	http://automotivedreamteam.com/v.exe	e197650e-b872-405f-9be9-2d39459d5e0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	[2b701d43a43315105d649612b2]	Inherit event
Network activity	url	http://shopalldoggsoop.com/v.exe	a3996a11-4e60-4f05-ba40-999664a02cbc	<input checked="" type="checkbox"/>	<input type="checkbox"/>	[2b701d43a43315105d649612b2]	Inherit event
Network activity	url	http://pooperscooperfranchise.com/v.exe	3778dbbd-7f86-4186-9052-74a389569e0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	[2b701d43a43315105d649612b2]	Inherit event
Network activity	url	http://cheryllipooperscoopers.com/v.exe	b834e874-a827-407-abef-a068781411e	<input checked="" type="checkbox"/>	<input type="checkbox"/>	[2b701d43a43315105d649612b2]	Inherit event
Network activity	url	http://alldoggsoop.net/v.exe	08d072d8-822b-4659-9c11-5315bf226d44	<input checked="" type="checkbox"/>	<input type="checkbox"/>	[2b701d43a43315105d649612b2]	Inherit event
Network activity	url	http://alldoggsoop.mob/v.exe	4baea866-d739-47a0-94c1-d583b294e4ee	<input checked="" type="checkbox"/>	<input type="checkbox"/>	[2b701d43a43315105d649612b2]	Inherit event
Network activity	url	http://alldoggsoop.info/v.exe	0f5ad15b-47ed-4772-acb8-d2240afed8c3	<input checked="" type="checkbox"/>	<input type="checkbox"/>	[2b701d43a43315105d649612b2]	Inherit event
Network activity	url	http://alldoggsoop.lt/v.exe	90b29d18-d778-4415-8544-5a2fcf53d4f7	<input checked="" type="checkbox"/>	<input type="checkbox"/>	[2b701d43a43315105d649612b2]	Inherit event

NEW - STANDALONE FUNCTIONALITY

- Flexibility, no need to install MISP
- User friendly interface
- Easiest way to test new modules

WEB INTERFACE - QUERY

- Add multiple entries
- Choose different modules

The screenshot shows the MISP Query interface. On the left is a sidebar with a navigation menu:

- Home
- History
- History Session
- History Tree
- Config
- External tools

A blue button labeled "Query" is highlighted. The main area is titled "MISP Modules". It displays a search bar with the query "circ.lu", a "Add new entry" button, and a "Delete entry" button. Below this is a section titled "Input Attributes" with a dropdown menu set to "domain". A section titled "Modules" contains a list box with the item "circL_passivedns". At the bottom is a checkbox labeled "Configure all modules".

WEB INTERFACE - RESULTS

■ Multiple tabs for visualization in different formats

The screenshot shows the MISP web interface with the following details:

- Left Sidebar:** Home, History, History Session, History Tree, Config, External tools.
- Header:** MISP, circl.lu, + New query, Query, Refresh.
- Input Attribute:** domain
- Modules:** cird_passivedns
- Timeline:** 100% (blue bar), Stopped | 1 Success, 0 Errors, 1 Total, 2024-07-08 13:34.
- Visual:** Selected tab.
- Json:** Available tab.
- Markdown:** Available tab.
- External tools:** circl.lu, Errors, circl.lu.
- Content Area:** Shows the results for the cird_passivedns module, including fields like rrtype, rname, rdata, count, origin, and time_first, each with a 'query' link.
- Bottom Right:** [Go Back Top] button.

WEB INTERFACE - HISTORY

- Save your researches and pivot from them

The screenshot shows the MISP web interface with the 'History' tab selected in the sidebar. The main content area is titled 'History' and contains a message: 'All histories present here will be deleted at the end of the session'. Below this, a history entry is displayed with the identifier '# 1'. The entry consists of a row of tabs: 'circl.lu' (highlighted in red), 'Input Attributes' (highlighted in red), 'Modules', and 'circl_passivedns'. The 'Input Attributes' tab is active, showing the value 'domain'. A blue 'Save' button is located to the right of the entry.

WEB INTERFACE - EXTERNAL TOOLS (DEV)

■ Export results to other tools. (Still in dev)

The screenshot shows the MISP web interface with the following details:

- Left sidebar:** Home, History, History Session, History Tree, Config, External tools (selected).
- Header:** MISP Threat Hunting
- Page Title:** External tools
- Search Bar:** Search tools
- Tool List:** flowintel (selected, indicated by a checked checkbox and a red circle with an 'x').
- Tool Configuration Panel:**
 - Name:** flowintel
 - Url:** http://localhost:7006/analyzer/receive_result
 - Buttons:** Save (blue), Delete (red)
- Page Bottom:** [Go Back Top]

FUTURE OF THE MODULES SYSTEM

- Enrichment on full events
- Move the modules to background processes with a messaging system
- Have a way to skip the results preview
 - ▶ Preview can be very heavy
 - ▶ Difficulty is dealing with uncertain results (without the user having final say)

Q&A



- <https://github.com/MISP/misp-modules>
- <https://github.com/MISP/>
- We welcome new modules and pull requests.
- MISP modules can be designed as standalone application.

MISP GALAXY

CIRCL / TEAM MISP PROJECT

[HTTP://WWW.MISP-PROJECT.ORG/](http://www.misp-project.org/)

TWITTER: @MISPPROJECT

13TH ENISA-EC3 WORKSHOP



MISP
Threat Sharing

MISP GALAXIES

- MISP started out as a platform for technical indicator sharing
- The need for a way to describe threat actors, tools and other commonalities became more and more pressing
- **Taxonomies quickly became essential for classifying events**
- The weakness of the tagging approach is that it's not very descriptive
- We needed a way to attach **more complex structures to data**
- Also, with the different naming conventions for the same "thing" attribution was a mess
- This is where the Galaxy concept came in

SOLUTION

- Pre-crafted galaxy "clusters" via GitHub project
- Attach them to an event and attribute(s)
- The main design principle was that these higher level informations are meant for human consumption
- This means flexibility - key value pairs, describe them dynamically
- Technical indicators remain strongly typed and validated, galaxies are loose key value lists

THE GALAXY OBJECT STACK

- **Galaxy:** The type of data described (Threat actor, Tool, ...)
- **Cluster:** An individual instance of the galaxy (Sofacy, Turla, ...)
- **Element:** Key value pairs describing the cluster (Country: RU, Synonym: APT28, Fancy Bear)
- **Reference:** Referenced galaxy cluster (Such as a threat actor using a specific tool)

(SOME) EXISTING GALAXIES

- **Exploit-Kit:** An enumeration of known exploitation kits used by adversaries
- **Microsoft activity group:** Adversary groups as defined by Microsoft
- **Preventive measure:** Potential preventive measures against threats
- **Ransomware:** List of known ransomwares
- **TDS:** Traffic Direction System used by adversaries
- **Threat-Actor:** Known or estimated adversary groups
- **Tool:** Tools used by adversaries (from Malware to common tools)
- **MITRE ATT&CK:** Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK™)

WHAT A CLUSTER LOOKS LIKE

Galaxies	
Threat Actor	  
- Sofacy	  
Description	The Sofacy Group (also known as APT28, Pawn Storm, Fancy Bear and Sednit) is a cyber espionage group believed to have ties to the Russian government. Likely operating since 2007, the group is known to target government, military, and security organizations. It has been characterized as an advanced persistent threat.
Synonyms	APT 28 APT28 Pawn Storm Fancy Bear Sednit TsarTeam TG-4127 Group-4127 STRONTIUM Grey-Cloud
Source	MISP Project
Authors	Alexandre Dulaunoy Florian Roth Thomas Schreck Timo Steffens Various
Country	 RU
Refs	https://en.wikipedia.org/wiki/Sofacy_Group

Add new cluster

ATTACHING CLUSTERS TO EVENTS

- Internally simply using a taxonomy-like tag to attach them to events
- Example: misp-galaxy:threat-actor="Sofacy"
- **Synchronisation works out of the box** with older instances too. They will simply see the tags until they upgrade.
- Currently, as mentioned we rely on the community's contribution of galaxies

ATTACHING CLUSTERS

- Use a searchable synonym database to find what you're after

The screenshot shows a user interface for searching threat actors. At the top, there are four tabs: "All namespaces", "deprecated", "misp", and "mitre-attack". Below these tabs is a search bar containing the text "Threat Actor". Underneath the search bar, there are several suggestions: "Attack Pattern", "Election guidelines", "attack4fraud", and "o365-exchange-techniques". A detailed result for "Sofacy" is shown in a box, listing its synonyms: "APT 28, APT28, Pawn Storm, PawnStorm, Fancy Bear, Sednit, SNAKEMACKEREL, TsarTeam, Tsar Team, TG-4127, Group-4127, STRONTIUM, TAG_0700, Swallowtail, IRON TWILIGHT, Group 74". A "Submit" button is located at the bottom right of this result box.

CREATING YOUR OWN GALAXY

- Creating galaxy clusters has to be straightforward to get the community to contribute
- Building on the prior success of the taxonomies and warninglists
- Simple JSON format in similar fashion
- Just drop the JSON in the proper directory and let MISP ingest it
- We always look forward to contributions to our galaxies repository

GALAXY JSON

- If you want to create a completely new galaxy instead of enriching an existing one

```
1 {  
2     "name" : "Threat Actor",  
3     "type" : "threat-actor",  
4     "description": "Threat actors are characteristics of malicious  
      actors (or adversaries) representing a cyber attack threat  
      including presumed intent and historically observed  
      behaviour.",  
5     "version": 1,  
6     "uuid": "698774c7-8022-42c4-917f-8d6e4fo6ada3"  
7 }
```

CLUSTER JSON

- Clusters contain the meat of the data

- Skeleton structure as follows
-

```
1 {  
2   "values": [  
3     {  
4       "meta": {},  
5       "description": "",  
6       "value": "",  
7       "related_clusters": [{}],  
8     }  
9   ]  
10 }
```

CLUSTER JSON VALUE EXAMPLE

```
1  {
2      "meta": {
3          "synonyms": [
4              "APT 28", "APT28", "Pawn Storm", "Fancy Bear",
5              "Sednit", "TsarTeam", "TG-4127", "Group-4127",
6              "STRONTIUM", "Grey-Cloud"
7          ],
8          "country": "RU",
9          "refs": [
10              "https://en.wikipedia.org/wiki/Sofacy_Group"
11          ]
12      },
13      "description": "The Sofacy Group (also known as APT28,
14                      Pawn Storm, Fancy Bear and Sednit) is a cyber
15                      espionage group believed to have ties to the
16                      Russian government. Likely operating since 2007,
17                      the group is known to target government, military,
18                      and security organizations. It has been
19                      characterized as an advanced persistent threat.",
20      "value": "Sofacy"
21  },
```

- Reusing existing values such as **complexity, effectiveness, country, possible_issues, colour, motive, impact, refs, synonyms, derived_from, status, date, encryption, extensions, ransomnotes, cfr-suspected-victims, cfr-suspected-state-sponsor, cfr-type-of-incident, cfr-target-category, kill_chain**.
- Or adding your own meta fields.

META BEST PRACTICES - A SAMPLE

```
1  {
2      "description": "Putter Panda were the subject of an
3          extensive report by CrowdStrike, which stated: 'The
4          CrowdStrike Intelligence team has been tracking this
5          particular unit since 2012, under the codename PUTTER
6          PANDA, and has documented activity dating back to 2007.
7          The report identifies Chen Ping, aka cpyy, and the
8          primary location of Unit 61486.'",
9
10     "meta": {
11         "cfr-suspected-state-sponsor": "China",
12         "cfr-suspected-victims": [
13             "U.S. satellite and aerospace sector"
14         ],
15         "cfr-target-category": [
16             "Private sector",
17             "Government"
18         ],
19         "cfr-type-of-incident": "Espionage",
20         "country": "CN",
21         "refs": [
22             "http://cdn0.vox-cdn.com/assets/4589853/crowdstrike-
23                 intelligence-report-putter-panda.original.pdf",
24             "https://www.cfr.org/interactive/cyber-operations/putter-
25                 -panda"
26         ]
27     }
28 }
```

GALAXY JSON MATRIX-LIKE

Propose Attribute	Analysis	Initial
P example-of-threats	Setup party/candidate registration (3 items)	Setup electoral rolls (3 items)
F DoS or overload of party/campaign registration, causing them to miss the deadline	Deleting or tampering with voter data	Hacking campaign websites (defacement, DoS)
C Fabricated signatures from sponsor	DoS or overload of voter registration system, suppressing voters	Hacking candidate laptops or email accounts
L A Tampering with registrations	Identity fraud during voter registration	Leak of confidential information
		Misconfiguration of a website

Select Some Options

Can

GALAXY JSON MATRIX-LIKE

```
1      {
2      "description": "Universal Development and Security Guidelines as
3          Applicable to Election Technology." ,
4      "icon": "map",
5      "kill_chain_order": {           \\\bTab in the matrix
6          "example-of-threats": [       \\\bColumn in the matrix
7              "setup | party/candidate-registration",
8              "setup | electoral-rolls",
9              "campaign | campaign-IT",
10             "all-phases | governement-IT",
11             "voting | election-technology",
12             "campaign/public-communication | media/press"
13         ]
14     },
15     "name": "Election guidelines",
16     "namespace": "misp",
17     "type": "guidelines",
18     "uuid": "c1dc03b2-89b3-42a5-9d41-782ef726435a",
19     "version": 1
}
```

CLUSTER JSON MATRIX-LIKE

```
1  {
2      "description": "DoS or overload of party/campaign
3          registration, causing them to miss the deadline",
4      "meta": {
5          "date": "March 2018.",
6          "kill_chain": [ \Define in which column the cluster should be placed
7              "example-of-threats:setup | party/candidate-registration"
8          ],
9          "refs": [
10             "https://www.ria.ee/sites/default/files/content-editors/kuberturve/cyber\_security\_of\_election\_technology.pdf
11         ]
12     },
13     "uuid": "154c6186-a007-4460-a029-ea23163448fe",
14     "value": "DoS or overload of party/campaign registration,
15         causing them to miss the deadline"
16 }
```

EXPRESSING RELATION BETWEEN CLUSTERS

- Cluster can be related to one or more clusters using default relationships from MISP objects and a list of tags to classify the relation.

```
1   "related": [
2     {
3       "dest-uuid": "5ce5392a-3a6c-4e07-9df3-9b6a9159ac45",
4       "tags": [
5         "estimative-language:likelihood-probability=\\\"likely
6           \\\""
7         ],
8         "type": "similar"
9       }
10      ],
11      "uuid": "0ca45163-e223-4167-b1af-f088ed14a93d",
12      "value": "Putter Panda"
```

PyMISPGALAXIES

```
from pymispgalaxies import Clusters
c = Clusters()
list(g.keys())
# ['threat-actor', 'ransomware', 'exploit-kit', 'tds', 'tool', 'rat', 'mitre-attack-pattern',
# 'mitre-tool', 'microsoft-activity-group', 'mitre-course-of-action', 'mitre-malware',
# 'mitre-intrusion-set', 'preventive-measure']
print(c.get("rat"))
# misp-galaxy:rat="Brat"
# misp-galaxy:rat="Loki RAT"
# misp-galaxy:rat="join.me"
# misp-galaxy:rat="Setro"
# misp-galaxy:rat="drat"
# misp-galaxy:rat="Plasma RAT"
# misp-galaxy:rat="NanoCore"
# misp-galaxy:rat="DarkTrack"
# misp-galaxy:rat="Theef"
# misp-galaxy:rat="Greame"
# misp-galaxy:rat="Nuclear RAT"
# misp-galaxy:rat="DameWare Mini Remote Control"
# misp-galaxy:rat="ProRat"
# misp-galaxy:rat="death"
# misp-galaxy:rat="Dark DDoSeR"
# ....
print(c.get("rat").description)
# remote administration tool or remote access tool (RAT), also called sometimes remote
# access trojan, is a piece of software or programming that allows a remote "operator"
# to control a system as if they have physical access to that system.
```

Q&A

- info@circl.lu (if you want to join the CIRCL MISP sharing community)
- OpenPGP fingerprint: 3B12 DCC2 82FA 2931 2F5B 709A 09E2 CD49 44E6 CBCD
- <https://github.com/MISP/> -
<http://www.misp-project.org/>
- We welcome any contributions to the project, be it pull requests, ideas, github issues,...

MISP OBJECT TEMPLATE

BUILDING CUSTOM AND OPEN DATA MODELS

CIRCL / TEAM MISP PROJECT

[HTTP://WWW.MISP-PROJECT.ORG/](http://www.misp-project.org/)

TWITTER: @MISPPROJECT

13TH ENISA-EC3 WORKSHOP



MISP
Threat Sharing

OBJECTS - OR HOW WE LEARNED TO STOP WORRYING AND LOVE THE TEMPLATES

- Attributes are a simple but powerful tool to describe data
- Lacking the capability to create containers around attributes describing a common concept
- The goal was to develop something semi-standardised, with the option to **dynamically build templates**
- We have considered a list of different solutions such as simple boolean operators, but found that the current implementation was superior.
- The result is a simple template that uses the basic attribute types as building blocks along with some meta data
- The template does **not have to be known** in order to use the constructed objects
- What we maintain now is a set of common objects, but similarly to our other JSON formats, users can extend it with their own ideas.

MISP OBJECT TEMPLATES

- Using a similar JSON format as the taxonomies, galaxies, warninglists.
- You can find the default set of object templates in the git repository¹.
- Some of the object templates capture objects from other standards or mimic the output of tools
- We tried to capture the most common use-cases coming from our own use-case as well as those of various partners that got involved
- Improvements or pull requests for new object templates are of course always welcome

¹<https://www.github.com/MISP/misp-objects/>

EXISTING OBJECT EXAMPLES

- AIL-leak - **AIL object, an example for an object catering to the output of another tool**
- Android permission - **An object used to further contextualise another object**
- Bank account
- File **Generic object to describe a file**
- Passive DNS
- Regex
- Sandbox report
- Vulnerability **Enabling new use-cases such as pre-sharing of vulnerability information**
- X509
- Yara **Verbatim sharing of rule sets along with meta-data**

OBJECT TEMPLATE SKELETON

```
1 {
2   "requiredOneOf": [],
3   "required": [],
4   "attributes": {},
5   "version": 1,
6   "description": "My description",
7   "meta-category": "Chosen meta category",
8   "uuid": "Object template uuid",
9   "name": "Object template name"
10 }
```

ADDING ELEMENTS TO AN OBJECT TEMPLATE

```
1 "regexp-type": {  
2     "description": "Type of the regular expression syntax.",  
3     "disable_correlation": true,  
4     "ui-priority": 0,  
5     "misp-attribute": "text",  
6     "values_list": [  
7         "PCRE",  
8         "PCRE2",  
9         "POSIX BRE",  
10        "POSIX ERE"  
11    ],  
12 },
```

ATTRIBUTE KEYS

- Primary key: Object relation
- description: A description of the attribute in relation to the object
- disable_correlation: You can disable correlations for attributes in the resulting object
- ui-priority: Not implemented yet, but the idea is to have a "quick view" of objects only showing certain prio levels
- misp-attribute: The misp attribute type used as the building block
- values_list: an optional list of values from which the user **must** choose instead of entering a value manually
- sane_defaults: an optional list of values from which the user **may** choose instead of entering a value
- multiple: Allow the user to add **more** than one of this attribute

ENFORCEMENT OF CERTAIN KEYS

- The template also defines which of the added attributes are mandatory
- Requirements are pointed to via their **object relations names**
- We differentiate between two types of rule sets:
 - ▶ Required: Everything in this list has to be set in order for the object to validate
 - ▶ Required One Of: Any of the attributes in this list will satisfy the requirements

WHAT WILL THE TEMPLATE ACTUALLY DO?

- Templates create a form that can be used to populate an event
- When using templates, MISP will enforce everything according to the template rules
- However, these are only optional, users can avoid using the templates when creating events via the API
- The reason for this is that you do not need to have the template in order to create an object
- The limitation of this system: You **cannot modify** objects that were created with unknown templates

TEMPLATES AS RENDERED IN THE UI

Add File Object

Object Template	File v10
Description	File object describing a file with meta-information
Requirements	Required one of: filename, size-in-bytes, authentihash, ssdeep, imphash, pehash, md5, sha1, sha224, sha256, sha384, sha512, sha512/224, sha512/256, tlsh, pattern-in-file, x509-fingerprint-sha1, malware-sample

Meta category

File

Distribution

Inherit event

Comment

Save	Name :: type	Description	Category	Value
<input checked="" type="checkbox"/>	Md5 :: md5	[Insecure] MD5 hash (128 bits)	Payload delivery	
<input checked="" type="checkbox"/>	Pattern-in-file :: pattern-in-file	Pattern that can be found in the file	Payload installation	
<input checked="" type="checkbox"/>	Sha256 :: sha256	Secure Hash Algorithm 2 (256 bits)	Payload delivery	
<input checked="" type="checkbox"/>	Sha512 :: sha512	Secure Hash Algorithm 2 (512 bits)	Payload delivery	

Filenames :: Filenames

Filenames :: Filenames

TEMPLATES AS RENDERED IN THE UI

2018-03-27 Name: %v.r*		
References: 1 ✓		
2018-03-27	Payload delivery	filename: filename:
2018-03-27	Other	size-in-bytes: size-in-bytes:
2018-03-27	Other	entropy: float:
2018-03-27	Payload delivery	md5: md5:
2018-03-27	Payload delivery	sha1: sha1:
2018-03-27	Payload delivery	sha256: sha256:
2018-03-27	Payload delivery	sha512: sha512:
2018-03-27	Payload delivery	malware-sample: putty.exe

Q&A



- <https://github.com/MISP/MISP>
- <https://github.com/MISP/misp-objects>
- info@circl.lu (if you want to join one of the MISP community operated by CIRCL)
- PGP key fingerprint: CA57 2205 C002 4E06 BA70 BE89 EAAD
CFFC 22BD 4CD5

MISP DASHBOARD

REAL-TIME OVERVIEW OF THREAT INTELLIGENCE FROM

CIRCL / TEAM MISP PROJECT

INFO@CIRCL.LU

SEPTEMBER 11, 2024



MISP
Threat Sharing

MISP ZEROMQ

MISP includes a flexible publish-subscribe model to allow real-time integration of the MISP activities:

- Event publication
- Attribute creation or removal
- Sighting
- User login

→ Operates at global level in MISP

MISP ZeroMQ functionality can be used for various model of integration or to extend MISP functionalities:

- Real-time search of indicators into a SIEM¹
- Dashboard activities
- Logging mechanisms
- Continuous indexing
- Custom software or scripting

¹Security Information & Event Management

MISP-DASHBOARD: AN INTRODUCTION

MISP-DASHBOARD - REALTIME ACTIVITIES AND THREAT INTELLIGENCE

MISP Live Dashboard - MISP Standard ZMQ

Network activity: 62.102.148.67 Rotation speed: 30 sec Zoom level: 15

The map displays network activity around the city center of Stockholm, Sweden. A blue dot marks the location of the IP address 62.102.148.67. A callout box indicates "Sweden null null". The map shows various neighborhoods like Södermalm, Norrmalm, and Kungsholmen.

Attribute.category overtime (hours)

A gauge chart showing the overtime for different attribute categories. The categories and their corresponding colors are: Network activity (yellow), Antivirus detection (blue), Persistence mechanism (red), Internal reference (green), and Financial fraud (purple). The chart shows that Network activity has the highest value, followed by Financial fraud, Internal reference, Antivirus detection, and Persistence mechanism.

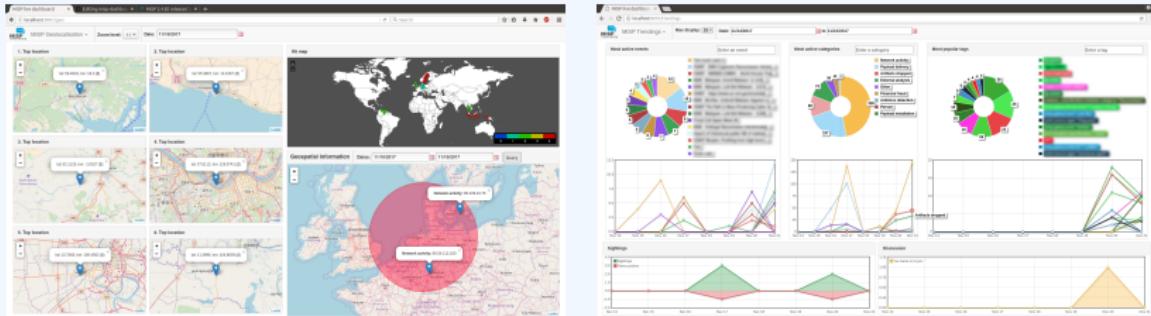
World Map

A world map where threat intelligence is visualized as colored dots. A color scale at the bottom ranges from 0 (dark red) to 10 (dark green). Most activity is concentrated in North America, Europe, and parts of Asia.

Logs

Time	Event.id	Attribute.Tag	Attribute.category	Attribute.type	Attribute.value Attribute.comment
15:07:46	9356	circTopic="undefined" tip:white	Network activity	ip-src	99.99.99.99
15:08:36	9356	circIncident-classification="denial-of-service"	Network activity	ip-src	8.8.8.8
15:08:36	9356	circIncident-classification="malware" circIncident-classification="XSS"	Antivirus detection	comment	Comment
15:08:36	9356		Network activity	ip-src	9.9.9.9
15:08:36	9356		Persistence mechanism	text	Just a another test
15:08:36	9356		Internal reference	text	Another text
15:08:36	9356		Financial fraud	phone-number	+221721120220
15:08:36	9356		Network activity	ip-src	62.102.148.67
15:08:36	9356	circTopic="undefined" tip:white	Network activity	ip-src	99.99.99.99

MISP-DASHBOARD - FEATURES



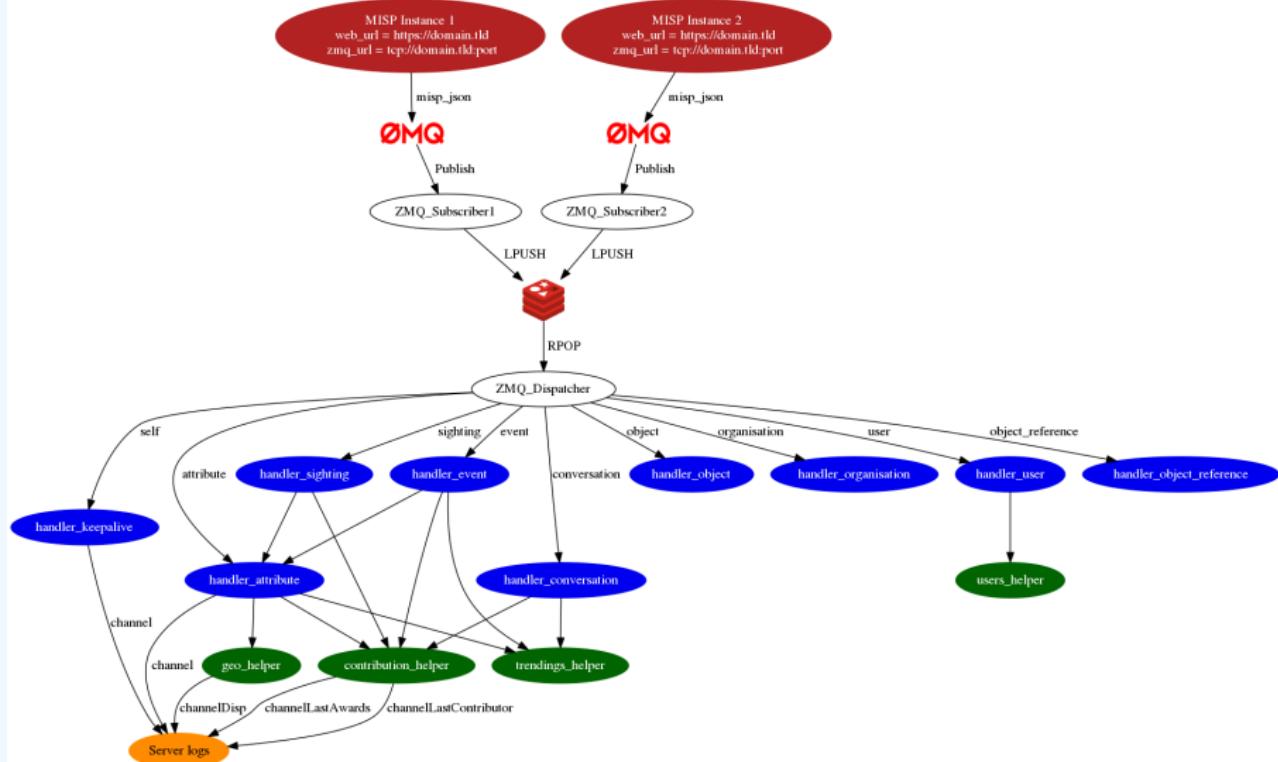
- Subscribe to multiple **ZMQ** MISP instances
- Provides historical geolocalised information
- Present an experimental **Gamification of the platform**
- Shows when and how MISP is used
- Provides real time information showing current threats and activity

MISP-DASHBOARD: ARCHITECTURE AND DEVELOPMENT

SETTING UP THE DASHBOARD

1. Be sure to have a running redis server: e.g.
 - ▶ `redis-server -p 6250`
2. Update your configuration in `config.cfg`
3. Activate your virtualenv:
 - ▶ `.. ./DASHENV/bin/activate`
4. Listen to the MISP feed by starting the `zmq_subscriber`:
 - ▶ `./zmq_subscriber.py`
5. Start the dispatcher to process received messages:
 - ▶ `./zmq_dispatcher.py`
6. Start the Flask server:
 - ▶ `./server.py`
7. Access the interface at `http://localhost:8001/`

MISP-Dashboard architecture



WRITING YOUR HANDLER

```
1 # Register your handler
2 dico_action = {
3     "misp_json":                      handler_dispatcher,
4     "misp_json_event":                 handler_event,
5     "misp_json_self":                  handler_keepalive,
6     "misp_json_attribute":             handler_attribute,
7     "misp_json_object":                handler_object,
8     "misp_json_sighting":              YOUR_CUSTOM_SIGHTINGS_HANDLER,
9     "misp_json_organisation":          handler_log,
10    "misp_json_user":                 handler_user,
11    "misp_json_conversation":         handler_conversation,
12    "misp_json_object_reference":     handler_log,
13 }
14 }
```

```
1 # Implement your handler
2
3 # e.g. user handler
4 def handler_user(zmq_name, jsondata):
5     # json action performed by the user
6     action = jsondata['action']
7     # user json data
8     json_user = jsondata['User']
9     # organisation json data
10    json_org = jsondata['Organisation']
11    # organisation name
12    org = json_org['name']
13    # only consider user login
14    if action == 'login':
15        timestamp = time.time()
16        # users_helper is a class to interact with the DB
17        users_helper.add_user_login(timestamp, org)
18
```

RECENT CHANGES IN THE MISP-DASHBOARD

- MISP authentication can now be used in the misp-dashboard
- Improved TLS/SSL support in the default misp-dashboard
- Self-test tool to debug and test ZMQ connectivity

FUTURE DEVELOPMENT

-  Optimizing contribution scoring and model to encourage sharing and contributions enrichment
-  Increasing geolocation coverage
-  Global filtering capabilities
 - Geolocation: Showing wanted attribute or only on specific region
 - Trendings: Showing only specified taxonomies
-  Tighter integration with MISP
 - Present in MISP by default
 - ACL enabled version

CONCLUSION

MISP-Dashboard can provide real-time information to support security teams, CSIRTs or SOC showing current threats and activity by providing:

- Historical geolocalised information
- Geospatial information from specific regions
- The most active events, categories, tags, attributes, ...

It also proposes a prototype of gamification of the platform providing incentive to share and contribute to the community

CONTRIBUTING TO THE MISP PROJECT

BECOME PART OF THE COMMUNITY TO DESIGN, DEVELOP

CIRCL / TEAM MISP PROJECT

[HTTP://WWW.MISP-PROJECT.ORG/](http://www.misp-project.org/)

TWITTER: @MISPPROJECT

13TH ENISA-EC3 WORKSHOP



MISP
Threat Sharing

CODE OF CONDUCT

- The MISP project has a Contributor Covenant Code of Conduct¹.
- The goal of the code of conduct is to foster an **open, fun and welcoming environment**.
- Another important aspect of the MISP projects is to welcome different areas of expertise in information sharing and analysis. The **diversity of the MISP community** is important to make the project useful for everyone.

¹https://github.com/MISP/MISP/code_of_conduct.md

REPORTING A BUG, AN ISSUE OR SUGGESTING FEATURES

- The most common way to contribute to the MISP project is to report a bug, issues or suggesting features.
- Each project (MISP core, misp-modules, misp-book, misp-taxonomies, misp-galaxy, misp-object or PyMISP) has their **own issue management**.
- Don't forget that you can **cross-reference issues** from other sub-projects.
- If you know an answer or could help on a specific issue, we welcome all contributions including **useful comments to reach a resolution**.

REPORTING SECURITY VULNERABILITIES

- **If you find security vulnerabilities (even minor ones) in MISP project, send an encrypted email** (info@circl.lu) with the details and especially how to reproduce the issues. Avoid to share publicly the vulnerability before a fix is available in MISP. PGP key fingerprint: CA57 2205 C002 4E06 BA70 BE89 EAAD CFFC 22BD 4CD5.
- We usually fix reported and confirmed security vulnerabilities in less than 48 hours.
- **We will request a CVE number** if the reporters didn't ask for one (don't forget to mention how you want to be credited).

AUTOMATIC INTEGRATION AND TESTING

- The majority of the repositories within the MISP GitHub organisation includes automatic integration via Github Actions.
- If you contribute and make a pull-request, **verify if your changes affect the result of the tests.**
- Automatic integration is not perfect including Travis but it's a quick win to catch new bugs or major issues in contribution.
- When you do a pull-request, the CI suite is automatically called².
 - ▶ If this fails, no worries, **review the output at Github actions** (it's not always you).
- We are working on additional automatic tests including security testing for the MISP core software (contributors are welcome).

²<https://github.com/MISP/MISP/actions>

JSON VALIDATION FOR MISP LIBRARIES

- All JSON format (**galaxy, taxonomies, objects or warning-lists**) are described in a JSON Schema³.
- The TravisCI tests are including JSON validation (via *jq*) and validated with the associated JSON schema.
- How to contribute a JSON library (objects, taxonomies, galaxy or warning-list):
 - ▶ If you update a JSON library, don't forget to run *jq_all_the_things.sh*. It's fast and easy. If it fails, review your JSON.
 - ▶ Commit your code and make a pull-request.
- Documentations (in PDF and HTML format) for the libraries are automatically generated from the JSON via asciidoctor⁴.

³schema_name.json

⁴example https://github.com/MISP/misp-galaxy/blob/master/tools/adoc_galaxy.py

DOCUMENTATION

- In addition to the automatic generation of documentations from JSON files, we maintain **misp-book**⁵ which is a generic documentation for MISP including usage, API documentation, best practices and specific configuration settings.
- The book is generated in HTML, PDF, epub and mobi using GitBook⁶ which is a framework to write documentation in MarkDown format.
- TravisCI is included in misp-book and **the book generation is tested at each commit.**
- The MISP book is regularly published on misp-project.org and circl.lu website.
- Contributors are welcome especially for new topics⁷ and also fixing our broken english.

⁵<https://github.com/MISP/misp-book>

⁶<https://github.com/GitbookIO>

⁷Topics of interest are analysts best-practices,

INTERNET-DRAFT - IETF FOR MISP FORMATS

- If you want to contribute to our IETF Internet-Draft for the MISP standard, misp-rfc⁸ is the repository where to contribute.
- **Update only the markdown file**, the XML and ASCII for the IETF I-D are automatically generated.
- If a major release or updates happen in the format, we will publish the I-D to the IETF⁹.
- The process is always MISP implementation → IETF I-D updates.

⁸<https://github.com/MISP/misp-rfc>

⁹https://datatracker.ietf.org/doc/search/?name=misp&active_drafts=on&rfc5=on

MISP CORE DEVELOPMENT CRASH COURSE

How I LEARNED TO STOP WORRYING AND LOVE THE PHP

CIRCL / TEAM MISP PROJECT



13TH ENISA-EC3 WORKSHOP



SOME THINGS TO KNOW IN ADVANCE...

- MISP is based on PHP 7.3+
- Using the MVC framework CakePHP 2.x
- What we'll look at now will be a quick glance at the structuring / layout of the code

MVC FRAMEWORKS IN GENERAL

- separation of business logic and views, interconnected by controllers
- main advantage is clear separation of the various components
- lean controllers, fat models (kinda...)
- domain based code reuse
- No interaction between Model and Views, ever

STRUCTURE OF MISP CORE APP DIRECTORIES

- Config: general configuration files
- Console: command line tools
- Controller: Code dealing with requests/responses, generating data for views based on interactions with the models
- Lib: Generic reusable code / libraries
- Model: Business logic, data gathering and modification
- Plugin: Alternative location for plugin specific codes, ordered into controller, model, view files
- View: UI views, populated by the controller

CONTROLLERS - SCOPE

- Each public function in a controller is exposed as an API action
- request routing (admin routing)
- multi-use functions (POST/GET)
- request/response objects
- contains the action code, telling the application what data fetching/modifying calls to make, preparing the resulting data for the resulting view
- grouped into controller files based on model actions
- Accessed via UI, API, AJAX calls directly by users
- For code reuse: behaviours
- Each controller bound to a model

CONTROLLERS - FUNCTIONALITIES OF CONTROLLERS

- pagination functionality
- logging functionality
- Controllers actions can access functionality / variables of Models
- Controllers cannot access code of other controller actions (kind of...)
- Access to the authenticated user's data
- beforeFilter(), afterFilter() methods
- Inherited code in AppController

CONTROLLERS - COMPONENTS

- Components = reusable code for Controllers
 - ▶ Authentication components
 - ▶ RestResponse component
 - ▶ ACL component
 - ▶ Cidr component
 - ▶ IOCIImport component (should be moved)

CONTROLLERS - ADDITIONAL FUNCTIONALITIES

- Handling API responses (RestResponseComponent)
- Handling API requests (IndexFilterComponent)
- auth/session management
- ACL management
- CRUD Component
- Security component
- important: queryString/PyMISP versions, MISP version handler
- future improvements to the export mechanisms

MODELS - SCOPE

- Controls anything that has to do with:
 - ▶ finding subsets of data
 - ▶ altering existing data
 - ▶ inherited model: AppModel
 - ▶ reusable code for models: Behaviours
 - ▶ regex, trim

MODELS - HOOKING SYSTEM

- Versatile hooking system
 - ▶ manipulate the data at certain stages of execution
 - ▶ code can be located in 3 places: Model hook, AppModel hook, behaviour

MODEL - HOOKING PIPELINE (ADD/EDIT)

■ Hooks / model pipeline for data creation / edits

- ▶ beforeValidate() (lowercase all hashes)
- ▶ validate() (check hash format)
- ▶ afterValidate() (we never use it)
- ▶ could be interesting if we ever validated without saving)
- ▶ beforeSave() (purge existing correlations for an attribute)
- ▶ afterSave() (create new correlations for an attribute / zmq)

MODELS - HOOKING PIPELINE (DELETE/READ)

■ Hooks for deletions

- ▶ `beforeDelete()` (purge correlations for an attribute)
- ▶ `afterDelete()` (zmq)

■ Hooks for retrieving data

- ▶ `beforeFind()` (modify the find parameters before execution, we don't use it)
- ▶ `afterFind()` (json decode json fields)

- code to handle version upgrades contained in AppModel
- generic cleanup/data migration tools
- centralised redis/pubsub handlers
- (Show example of adding an attribute with trace)

VIEWS - SCOPE AND STRUCTURE

- templates for views
- layouts
- reusable template code: elements
 - ▶ attribute list, rows (if reused)
- reusable code: helpers
 - ▶ commandhelper (for discussion boards), highlighter for searches, tag colour helper
- views per controller

VIEWS - TYPES OF VIEWS AND HELPERS

- ajax views vs normal views
- data views vs normal views vs serialisation in the controller
- sanitisation h()
- creating forms
 - ▶ sanitisation
 - ▶ CSRF

VIEWS - GENERATORS

- Mostly in genericElements
- Preparing the move to Cake4
- Important ones
 - ▶ Form - generate forms in a standardised way (/add, /edit, etc)
 - ▶ IndexTable - index lists using Field templates (/index, etc)
 - ▶ SingleViews - key-value lists with child elements (/view, etc)
 - ▶ Menues - to be refactored, see Cerebrate

GENERAL REUSABLE LIBRARIES

- Located in app/Lib
- Code that is to be reused across several layers
- Important ones
 - ▶ Dashboard - Dashboard widget backend code
 - ▶ EventReport - Report generation
 - ▶ Export - MISP -> external format converter modules
 - ▶ Tools - List of generic helper libraries - examples:
 - Attachment, JSON conversion, random generation, emailing, sync request generation
 - Kafka, ZMQ, AWS S3, Elastic integration, PGP encryption, CIDR operations

DISTRIBUTION

- algorithm for checking if a user has access to an attribute
- creator vs owner organisation
- distribution levels and inheritance (events -> objects -> attributes)
- shorthand inherit level
- sharing groups (org list, instance list)
- correlation distribution
- algorithms for safe data fetching (`fetchEvents()`,
`fetchAttributes()`,...)

TESTING YOUR CODE

- functional testing
- Github actions
- impact scope
 - ▶ view code changes: only impacts request type based views
 - ▶ controller code changes: Should only affect given action
 - ▶ model code changes: can have impact on entire application
 - ▶ lib changes: can have affect on the entire application
- Don't forget: queryACL, change querystring

DEEP-DIVE INTO PyMISP

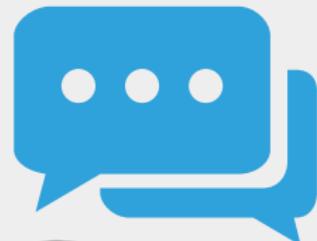
MISP - THREAT SHARING

CIRCL / TEAM MISP PROJECT

[HTTP://WWW.MISP-PROJECT.ORG/](http://www.misp-project.org/)

TWITTER: @MISPPROJECT

13TH ENISA-EC3 WORKSHOP



MISP
Threat Sharing

- MISP is a large project
- Your production environment is even more complex
- 3rd party services are even worse
- Querying MISP via CURL is doable, but get's painful fast
- Talking to MySQL directly can be dangerous
- POST a JSON blob, receive a JSON blob. You can do it manually(-ish)

BIG PICTURE

- Core goal: providing stable access to APIs, respect access control
- Simplifying handling & automation of indicators in 3rd party tools
- Hiding complexity of the JSON blobs
- Providing pre-cooked examples for commonly used operations
- Helping integration with existing infrastructure

COMMON QUERIES: RECENT CHANGES ON A TIMEFRAME

There are 4 main cases here:

- Metadata of the events that have been modified
 - ▶ **search_index** ⇒ timestamp (1h, 1d, 7d, ...), returns list of all the modified events
- Full events (metadata + attributes)
 - ▶ **search** ⇒ timestamp (1h, 1d, 7d, ...)
- Modified attributes
 - ▶ **search** ⇒ controller = attributes and timestamp (1h, 1d, 7d, ...)
- Other use case: get last **published** events by using the last parameter in the **search** method.

COMMON QUERIES: SEARCH THINGS

There are 3 main cases here:

- Easy, but slow: full text search with **search_all**
- Faster: use the **search** method and search by tag, type, enforce the warning lists, with(-out) attachments, dates interval, ...
- Get malware samples (if available on the instance).

COMMON QUERIES: CREATE THINGS

There are 3 main cases here:

- Add Event, edit its metadata
- Add attributes or objects to event
- (un)Tag event or attribute (soon object)
- Edit Attributes medatada
- Upload malware sample (and automatically expand it)

ADMINISTRATIVE TASKS

Assyming you have the right to do it on the instance.

- Managing users
- Managing organisations
- Managing sync servers

OTHER CAPABILITIES

- Upload/download samples
- **Proposals:** add, edit, accept, discard
- **Sightings:** Get, set, update
- Export **statistics**
- Manage **feeds**
- Get MISP server version, recommended PyMISP version
- And more, look at the api file

MISPEVENT - USECASE

```
from pymisp import MISPEvent, EncodeUpdate

# Create a new event with default values
event = MISPEvent()

# Load an existing JSON dump (optional)
event.load_file('Path/to/event.json')
event.info = 'My cool event' # Duh.

# Add an attribute of type ip-dst
event.add_attribute('ip-dst', '8.8.8.8')

# Mark an attribute as deleted (From 2.4.6o)
event.delete_attribute('<Attribute UUID>')

# Dump as json
event_as_jsondump = json.dumps(event, cls=EncodeUpdate)
```

- Python 3.5+ is recommended
- PyMISP is always inline with current version (`pip3 install pymisp`)
- Dev version: `pip3 install git+https://github.com/MISP/PyMISP.git`
- Get your auth key from:
<https://misppriv.circl.lu/events/automation>
 - ▶ Not available: you don't have "Auth key access" role. Contact your instance admin.
- Source available here: `git clone https://github.com/MISP/PyMISP.git`

EXAMPLES

- PyMISP needs to be installed (duh)
- Usage:
 - ▶ Create examples/keys.py with the following content

```
misp_url = "https://url-to-your-misp"
misp_key = "<API_KEY>"
misp_verifycert = True
```

- Proxy support:

```
proxies = {
    'http': 'http://127.0.0.1:8123',
    'https': 'http://127.0.0.1:8123',
}
PyMISP(misp_url, misp_key, misp_verifycert, proxies=proxies)
```

EXAMPLES

- Lots of ideas on how to use the API
- You may also want to look at the tests directory
- All the examples use argparse. Help usage is available:
script.py -h
 - ▶ **add_file_object.py**: Attach a file (PE/ELF/Mach-O) object to an event
 - ▶ **upload.py**: Upload a malware sample (use advanced expansion is available on the server)
 - ▶ **last.py**: Returns all the most recent events (on a timeframe)
 - ▶ **add_named_attribute.py**: Add attribute to an event
 - ▶ **sighting.py**: Update sightings on an attribute
 - ▶ **stats.py**: Returns the stats of a MISP instance
 - ▶ **{add,edit,create}_user.py** : Add, Edit, Create a user on MISP

USAGE

■ Basic example

```
from pymisp import PyMISP
api = PyMISP(url, apikey, verifycert=True, debug=False, proxies=None)
response = api.<function>
if response['error']:
    # <something went wrong>
else:
    # <do something with the output>
```

CONCEPT BEHIND ABSTRACTMISP

- JSON blobs are python dictionaries
- ... Accessing content can be a pain
- **AbstractMISP inherits collections.MutableMapping**, they are all dictionaries!
- ... Has helpers to load, dump, and edit JSON blobs
- **Important:** All the public attributes (not starting with a `_`) defined in a class are dumped to JSON
- **Tags:** Events and Attributes have tags, soon Objects. Tag handling is defined in this class.
- **edited:** When pushing a full MISPEvent, only the objects without a timestamp, or with a newer timestamp will be updated. This method recursively finds updated events, and removes the timestamp key from the object.

- **Pythonic** representation of MISP elements

- **Easy manipulation**

- ▶ Load an existing event
- ▶ Update te metadata, add attributes, objects, tags, mark an attribute as deleted, ...
- ▶ Set relations between objects
- ▶ Load and add attachments or malware samples as pseudo files

- **Dump to JSON**

MISPEVENT - MAIN ENTRYPOINTS

- `load_file(event_path)`
- `load(json_event)`
- `add_attribute(type, value, **kwargs)`
- `add_object(obj=None, **kwargs)`
- `add_attribute_tag(tag, attribute_identifier)`
- `get_attribute_tag(attribute_identifier)`
- `add_tag(tag=None, **kwargs)`
- `objects[], attributes[], tags[]`
- `edited, all other parameters of the MISPEvent element (info, date, ...)`
- `to_json()`

MISPOBJECT - MAIN ENTRYPOINTS

- `add_attribute(object_relation, **value)`
- `add_reference(referenced_uuid, relationship_type, comment=None, **kwargs)`
- `has_attributes_by_relation(list_of_relations)`
- `get_attributes_by_relation(object_relation)`
- `attributes[], relations[]`
- edited, all other parameters of the MISPObject element
(name, comment, ...)
- `to_json()`
- Can be validated against their template
- Can have default parameters applied to all attributes (i.e.
distribution, category, ...)

MISPATTRIBUTE - MAIN ENTRYPOINTS

- `add_tag(tag=None, **kwargs)`
- `delete()`
- `malware_binary (if relevant)`
- `tags[]`
- `edited, all other parameters of the MISPObjec`t element
`(value, comment, ...)`
- `to_json()`

- Libraries requiring specific 3rd party dependencies
- Callable via PyMISP for specific usecases
- Currently implemented:
 - ▶ **OpenIOC** to MISP Event
 - ▶ MISP to **Neo4J**

PyMISP - DEFAULT OBJECTS GENERATORS

- File - PE/ELF/MachO - Sections
- VirusTotal
- Generic object generator

PyMISP - LOGGING / DEBUGGING

- debug=True passed to the constructor enable debug to stdout
- Configurable using the standard logging module
- Show everything send to the server and received by the client

```
import pymisp
import logging

logger = logging.getLogger('pymisp')
logger.setLevel(logging.DEBUG) # enable debug to stdout

logging.basicConfig(level=logging.DEBUG, # Enable debug to file
                    filename="debug.log",
                    filemode='w',
                    format=pymisp.FORMAT)
```

Q&A



- <https://github.com/MISP/PyMISP>
- <https://github.com/MISP/>
- <https://pymisp.readthedocs.io/>
- We welcome new functionalities and pull requests.

MISP FEEDS - A SIMPLE AND SECURE APPROACH TO GENERATE, SELECT AND COLLECT INTELLIGENCE

PROVIDING READY-TO-USE THREAT INTELLIGENCE IN

CIRCL / TEAM MISP PROJECT

TLP:WHITE

[HTTP://WWW.MISP-PROJECT.ORG/](http://www.misp-project.org/)

TWITTER: @MISPPROJECT

13TH ENISA-EC3 WORKSHOP

MISP FEED - BASICS

MISP Feeds provide a way to

- **Exchange information via any transports** (e.g. HTTP, TLS, USB keys)
- Preview events along with their attributes, objects
- Select and import events
- **Correlate attributes using caching**

MISP Feeds have the following advantages

- Feeds work without the need of MISP synchronisation (reducing attack surface and complexity to a static directory with the events)
- **Feeds can be produced without a MISP instance** (e.g. security devices, honeypot sensors)

FEED - OVERVIEW

- By default, MISP is bundled with ~50 default feeds (MISP feeds, CSV or freetext feeds) which are not enabled by default and described in a simple JSON file¹.
- The feeds include CIRCL OSINT feed but also feeds like abuse.ch, Tor exit nodes or many more ²

Feeds

Generate feed lookup caches or fetch feed data (enabled feeds only)

[Cache all feeds](#) [Cache freetext/CSV feeds](#) [Cache MISP feeds](#) [Fetch and store all feed data](#)

[← previous](#) [next →](#)

Default feeds		Custom Feeds		All Feeds		Enabled Feeds												
	<input type="checkbox"/> Id	<input type="checkbox"/> Enabled	Name	Feed	Provider	Format	Input	Url	Headers	Target	Publish	Delta Merge	Override IDS	Distribution	Tag	Lookup	Caching	Actions
	<input type="checkbox"/>	<input checked="" type="checkbox"/>	CIRCL OSINT Feed <small>MISP</small>	MISP	CIRCL	Feed	network	https://www.circl.lu/doc/misp/feed-osint		All communities				CIRCL OSINT Feed	<small>x</small>	Age: 3m <small>▲</small>	<small>🔍 ⓘ 🔍</small>	<small>🔗</small>
	<input type="checkbox"/>	<input checked="" type="checkbox"/>	The Botvrij.eu Data <small>MISP</small>	MISP	Botvrij.eu	Feed	network	http://www.botvrij.eu/datafeed-osint		All communities				FEED-KOEN	<small>x</small>	Not cached <small>▲</small>	<small>🔍 ⓘ 🔍</small>	<small>🔗</small>
	<input type="checkbox"/>	<input checked="" type="checkbox"/>	InThreat OSINT Feed <small>MISP</small>	MISP	InThreat	Feed	network	https://feeds.inthreat.com/osint/misp/		Your organisation only				osint:source-type=block-or-filter-list*	<small>x</small>	Not cached	<small>🔍 ⓘ 🔍</small>	<small>🔗</small>

¹<https://github.com/MISP/MISP/blob/2.4/app/files/feed-metadata/defaults.json>

²<http://www.misp-project.org/feeds/>

FEED - OPERATIONS

Caching	Actions
Age: 12m	

- Cache feed attributes for correlation (not imported but visible in MISP)
- Disable feed
- Explore remote events
- Fetch all events (imported in MISP as event)
- Edit the feed configuration (e.g. authentication, URL,...)
- Remove feed
- Download feed metadata (to share feed details)

FEED - CREATION USING PYMISP feed generator

feed generator fetches events (matching some filtering) from a MISP instance and construct the manifest (defined in *MISP core format*) needed to export data.

Particularly,

- Used to generate the **CIRCL OSINT feed**
- Export events as json based on tags, organisation, events, ...
- Automatically update the dumps and the metadata file
- Comparable to a lightweight **TAXII interface**

Feed generator - CONFIGURATION FILE

```
1 url = 'your/misp/url'
2 key = 'YourAPIKey'
3 ssl = True
4 outputdir = 'output_directory'

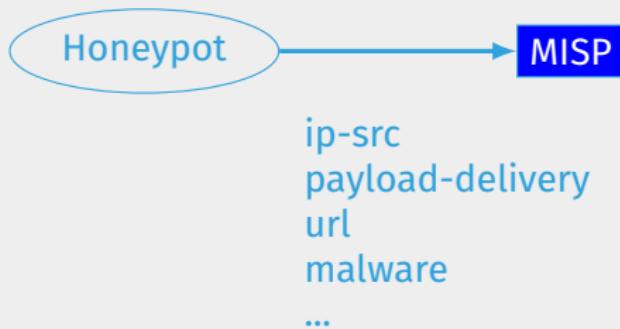
5
6 filters = {
7     'tag':'tlp:white|feed-export|!privint',
8     'org':'CIRCL'
9 }
10 # the above would generate a feed for all events created by CIRCL,
11     # tagged tlp:white and/or feed-export but exclude anything
12     # tagged privint

13 valid_attribute_distribution_levels = ['0', '1', '2', '3', '4', '5']
14 # 0: Your Organisation Only
15 # 4: Sharing Group
16 # 5: Inherit Event
```

Real-time FEED GENERATOR - PURPOSE

The PyMISP feed generator is great but may be inadequate or inefficient:

- Batch import of attributes/objects
- Data producer doesn't have a MISP instance at hand and only wants to **produce a directly consumable feed**:



Real-time FEED GENERATOR - USAGE

- generator.py exposes a class allowing to generate a MISP feed in real-time
- Each items can be appended on daily generated events

Example:

```
1 #  Init generator
2 generator = FeedGenerator()
3
4 #  Adding an attribute to the daily event
5 attr_type = "ip-src"
6 attr_value = "8.8.8.8"
7 additional_data = {}
8 generator.add_attribute_to_event(attr_type,
9                               attr_value,
10                             **additional_data)
```

Real-time FEED GENERATOR - USAGE (2)

```
1 # Adding a MISP object (cowrie) to the daily event
2 obj_name = "cowrie"
3 obj_data = {
4     "session": "session_id",
5     "username": "admin",
6     "password": "admin",
7     "protocol": "telnet"
8 }
9 generator.add_object_to_event(obj_name, **obj_data)
```

ADDING CUSTOM FEED TO MISP

List Feeds

Add Feed

Import Feeds from JSON

Feed overlap analysis matrix

Export Feed settings

Add MISP Feed

Add a new MISP feed source.

Enabled

Lookup Visible

Name

Provider

Source Format

Url

Source Format

Any headers to be passed with requests (for example: Authorization)

Add Basic Auth

Distribution

Default Tag

Filter rules:

- Enabled
- Lookup visible
- Name
- Provider
- Source Format
- Url
- Source Format
- Headers
- Distribution
- Default Tag
- Filter rules

Q&A



- <https://github.com/MISP/PyMISP>
- <https://github.com/MISP/>
- We welcome new functionalities and pull requests.

MISP WORKSHOP

INTRODUCTION INTO INFORMATION SHARING USING

TEAM CIRCL

TLP:WHITE

13TH ENISA-EC3 WORKSHOP



MISP
Threat Sharing

PLAN FOR THIS SESSION

- Explanation of the CSIRT use case for information sharing and what CIRCL does
- Building an information sharing community and best practices¹
- Quick demo of MISP capabilities

¹We published the complete guidelines in https://www.x-isac.org/assets/images/guidelines_to_set-up_an_ISAC.pdf

COMMUNITIES OPERATED BY CIRCL

- As a CSIRT, CIRCL operates a wide range of communities
- We use it as an **internal tool** to cover various day-to-day activities
- Whilst being the main driving force behind the development, we're also one of the largest consumers
- Different communities have different needs and restrictions

COMMUNITIES OPERATED BY CIRCL

- Private sector community (fall-back community)
 - ▶ Our largest sharing community
 - ▶ Over **+1500 organisations**
 - ▶ **+4000 users**
 - ▶ Functions as a central hub for a lot of sharing communities
 - ▶ Private organisations, Researchers, Various SoCs, some CSIRTs, etc
- CSIRT community
 - ▶ Tighter community
 - ▶ National CSIRTs, connections to international organisations, etc

COMMUNITIES OPERATED BY CIRCL

- Financial sector community
 - ▶ Banks, payment processors, etc.
 - ▶ Sharing of **mule accounts** and **non-cyber threat information**
- X-ISAC²
 - ▶ **Bridging the gap** between the various sectorial and geographical ISACs
 - ▶ Goal is to **bootstrap the cross-sectorial sharing** along with building the infrastructure to enable sharing when needed
 - ▶ Provide a basic set of threat intelligence for new ISACs

²<https://www.x-isac.org/>

COMMUNITIES OPERATED BY CIRCL

■ The ATT&CK EU community³

- ▶ Work on attacker modelling
- ▶ With the assistance of MITRE themselves
- ▶ Unique opportunity to **standardise on TTPs**
- ▶ Increasing the use of TTPs⁴ especially in sharing community like MITRE ATT&CK
- ▶ Major increase of MITRE ATT&CK context in sharing communities

³<https://www.attack-community.org/>

⁴Tactics, Techniques and Procedures

COMMUNITIES SUPPORTED BY CIRCL

- ISAC / specialised community MISP
 - ▶ Topical or community specific instances hosted or co-managed by CIRCL
 - ▶ Examples, GSMA, FIRST.org, CSIRTs network, etc
 - ▶ Often come with their **own taxonomies and domain specific object definitions**
- FIRST.org's MISP community
- Telecom and Mobile operators' such as GSMA T-ISAC community
- Various ad-hoc communities for cyber security exercises
 - ▶ The ENISA exercise (Cyber Europe)
 - ▶ NATO Locked Shields exercise

SHARING SCENARIOS IN MISP

- Sharing can happen for **many different reasons**. Let's see what we believe are the typical CSIRT scenarios
- We can generally split these activities into 4 main groups when we're talking about traditional CSIRT tasks:
 - ▶ Core services
 - ▶ Proactive services
 - ▶ Advanced services
 - ▶ Sharing communities managed by CSIRTs for various tasks

■ Incident response

- ▶ **Internal storage** of incident response data
- ▶ Sharing of indicators **derived from incident response**
- ▶ **Correlating data** derived and using the built in analysis tools
- ▶ **Enrichment** services
- ▶ **Collaboration** with affected parties via MISP during IR
- ▶ **Co-ordination** and collaboration
- ▶ **Takedown** requests

■ Alerting of information leaks (integration with AIL⁵)

⁵<https://www.ail-project.org/>

- **Contextualising** both internal and external data
- **Collection and dissimilation** of data from various sources (including OSINT)
- Storing, correlating and sharing own manual research (**reversing, behavioural analysis**)
- Aggregating automated collection (**sandboxing, honeypots, spamtraps, sensors**)
 - ▶ MISP allows for the creation of **internal MISP "clouds"**
 - ▶ Store **large specialised datasets** (for example honeypot data)
 - ▶ MISP has **interactions with** a large set of such **tools** (Cuckoo, Mail2MISP, etc)
- **Situational awareness** tools to monitor trends and adversary TTPs within my sector/geographical region (MISP-dashboard, built in statistics)

- Supporting **forensic analysts**
- Collaboration with **law enforcement**
- **Vulnerability** information sharing
 - ▶ **Notifications** to the constituency about relevant vulnerabilities
 - ▶ **Co-ordinating** with vendors for notifications (*)
 - ▶ Internal / closed community sharing of pentest results

CSIRTS' MANAGEMENT OF SHARING COMMUNITIES FOR CONSTITUENT ACTIONS:

- **Reporting** non-identifying information about incidents (such as outlined in NISD)
- **Seeking** and engaging in **collaboration** with CSIRT or other parties during an incident
- Pre-sharing information to **request for help** / additional information from the community
- **Pseudo-anonymised sharing** through 3rd parties to **avoid attribution** of a potential target
- Building processes for **other types of sharing** to get the community engaged and acquainted with the methodologies of sharing (mule account information, disinformation campaigns, border control, etc)

A QUICK NOTE ON LEGAL COMPLIANCE...

- Collaboration with legal advisors as part of a CEF project for creating compliance documents
 - ▶ Information sharing and cooperation **such as GDPR**
 - ▶ How MISP enables stakeholders identified by the **NISD** to perform key activities
 - ▶ **AIL** and MISP
- For more information:
<https://github.com/CIRCL/compliance about DORA, GDPR, ISO 27010 and MISP compliance>

BRINGING DIFFERENT SHARING COMMUNITIES TOGETHER

- We generally all **end up sharing with peers that face similar threats**
- Division is either **sectorial or geographical**
- So why even bother with trying to bridge these communities?

ADVANTAGES OF CROSS SECTORIAL SHARING

- Reuse of TTPs across sectors
- Being hit by something that **another sector has faced before**
- **Hybrid threats** - how seemingly unrelated things may be interesting to correlate
- Prepare other communities for the capability and **culture of sharing** for when the need arises for them to reach out to CSIRT
- Generally our field is ahead of several other sectors when it comes to information sharing, might as well **spread the love**



SHARING IS CARING!

GETTING STARTED WITH BUILDING YOUR OWN SHARING COMMUNITY

- Starting a sharing community is **both easy and difficult** at the same time
- Many moving parts and most importantly, you'll be dealing with a **diverse group of people**
- Understanding and working with your constituents to help them face their challenges is key

GETTING STARTED WITH BUILDING YOUR OWN SHARING COMMUNITY

- When you are starting out - you are in a unique position to drive the community and set best practices...



RUNNING A SHARING COMMUNITY USING MISP - HOW TO GET GOING?

- Different models for constituents
 - ▶ **Connecting to** a MISP instance hosted by a CSIRT
 - ▶ **Hosting** their own instance and connecting to CSIRT's MISP
 - ▶ **Becoming member** of a sectorial MISP community that is connected to CSIRT's community
- Planning ahead for future growth
 - ▶ Estimating requirements
 - ▶ Deciding early on common vocabularies
 - ▶ Offering expansion, analysis and intelligence services through MISP

RELY ON OUR INSTINCTS TO IMMITATE OVER EXPECTING ADHERENCE TO RULES

- **Lead by example** - the power of imitation
- Encourage **improving by doing** instead of blocking sharing with unrealistic quality controls
 - ▶ What should the information look like?
 - ▶ How should it be contextualise
 - ▶ What do you consider as useful information?
 - ▶ What tools did you use to get your conclusions?
- Side effect is that you will end up **raising the capabilities of your constituents**

WHAT COUNTS AS VALUABLE DATA?

- Sharing comes in many shapes and sizes
 - ▶ Sharing **results** / reports is the classical example
 - ▶ Sharing **enhancements** to existing data/intelligence
 - ▶ Validating data / flagging false positives (**sighting**)
 - ▶ Asking for **support and collaboration** from the community
- **Embrace all of them.** Even the ones that don't make sense right now, you never know when they come handy...

HOW TO DEAL WITH ORGANISATIONS THAT ONLY "LEECH"?

- From our own communities, only about **30%** of the organisations **actively share data**
- We have come across some communities with sharing requirements
- In our experience, this sets you up for failure because:
 - ▶ Organisations losing access are the ones who would possibly benefit the most from it
 - ▶ Organisations that want to stay above the thresholds will start sharing junk / fake data
 - ▶ You lose organisations that might turn into valuable contributors in the future

SO HOW DOES ONE CONVERT THE PASSIVE ORGANISATIONS INTO ACTIVELY SHARING ONES?

- Rely on **organic growth** and it takes time (+2 years is common)
- **Help** them increase their capabilities
- As mentioned before, lead by example
- Rely on the inherent value to one's self when sharing information (validation, enrichments, correlations)
- **Give credit** where credit is due, never steal the contributions of your community (that is incredibly demotivating)

DISPELLING THE MYTHS AROUND BLOCKERS WHEN IT COMES TO INFORMATION SHARING

- Sharing difficulties are not really technical issues but often it's a matter of **social interactions** (e.g. **trust**).
 - ▶ You can play a role here: organise regular workshops, conferences, have face to face meetings
- Legal restrictions
 - ▶ "Our legal framework doesn't allow us to share information."
 - ▶ "Risk of information leak is too high and it's too risky for our organization or partners."
- Practical restrictions
 - ▶ "We don't have information to share."
 - ▶ "We don't have time to process or contribute indicators."
 - ▶ "Our model of classification doesn't fit your model."
 - ▶ "Tools for sharing information are tied to a specific format, we use a different one."

CONTEXTUALISING THE INFORMATION

- Sharing **technical information** is a **great start**
- However, to truly create valuable information for your community, always consider the context:
 - ▶ Your IDS might not care why it should alert on a rule
 - ▶ But your analysts will be interested in the threat landscape and the "big picture"
- Classify data to make sure your partners understand why it is **important for you**, so they can see why it could be **useful to them**
- Massively important once an organisation has the maturity to filter the most critical **subsets of information for their own defense**

CHOICE OF VOCABULARIES

- MISP has a verify **versatile system** (taxonomies) for classifying and marking data
- However, this includes different vocabularies with obvious overlaps
- MISP allows you to **pick and choose vocabularies** to use and enforce in a community
- Good idea to start with this process early
- If you don't find what you're looking for:
 - ▶ Create your own (JSON format, no coding skills required)
 - ▶ If it makes sense, share it with us via a pull request for redistribution

SHARED LIBRARIES OF META- INFORMATION (GALAXIES)

- The MISProject in co-operation with partners provides a **curated list of galaxy information**
- Can include information packages of different types, for example:
 - ▶ Threat actor information (event different models or approaches)
 - ▶ Specialised information such as Ransomware, Exploit kits, etc
 - ▶ Methodology information such as preventative actions
 - ▶ Classification systems for methodologies used by adversaries - ATT&CK
- Consider improving the default libraries or contributing your own (simple JSON format)
- If there is something you cannot share, run your own galaxies and **share it out of bound** with partners
- Pull requests are always welcome

FALSE-POSITIVE HANDLING

- You might often fall into the trap of discarding seemingly "junk" data
- Besides volume limitations (which are absolutely valid, fear of false-positives is the most common reason why people discard data) - Our recommendation:
 - ▶ Be lenient when considering what to keep
 - ▶ Be strict when you are feeding tools
- MISP allows you to **filter out the relevant data on demand** when feeding protective tools
- What may seem like **junk to you** may be absolutely **critical to other users**

MANY OBJECTIVES FROM DIFFERENT USER-GROUPS

- Sharing indicators for a **detection** matter.
 - ▶ 'Do I have infected systems in my infrastructure or the ones I operate?'
- Sharing indicators to **block**.
 - ▶ 'I use these attributes to block, sinkhole or divert traffic.'
- Sharing indicators to **perform intelligence**.
 - ▶ 'Gathering information about campaigns and attacks. Are they related? Who is targeting me? Who are the adversaries?'
- → These objectives can be conflicting (e.g. False-positives have different impacts)

FALSE-POSITIVE HANDLING

- Analysts will often be interested in the **modus operandi** of threat actors over **long periods of time**
- Even cleaned up infected hosts might become interesting again (embedded in code, recurring reuse)
- Use the tools provided to eliminate obvious false positives instead and limit your data-set to the most relevant sets

Warning: Potential false positives

List of known IPv4 public DNS resolvers

MANAGING SUB-COMMUNITIES

- Often within a community **smaller bubbles of information sharing will form**
- For example: Within a national private sector sharing community, specific community for financial institutions
- Sharing groups serve this purpose mainly
- As a CSIRT running a national community, consider bootstrapping these sharing communities
- Organisations can of course self-organise, but you are the ones with the know-how to get them started

MANAGING SUB-COMMUNITIES

- Consider compartmentalisation - does it make sense to move a secret squirrel club to their own sharing hub to avoid accidental leaks?
- Use your **best judgement** to decide which communities should be separated from one another
- Create sharing hubs with **manual data transfer** if needed
- Some organisations will even have their data air-gapped - Feed system
- **Create guidance** on what should be shared outside of their bubbles - organisations often lack the insight / experience to decide how to get going. Take the initiative!

GET IN TOUCH IF YOU NEED SOME HELP TO GET STARTED

- Getting started with building a new community can be daunting. Feel free to get in touch with us if you have any questions!
- Contact: info@circl.lu
- <https://www.circl.lu/>
<https://www.misp-project.org/>
- <https://github.com/MISP>
<https://gitter.im/MISP/MISP>
<https://twitter.com/MISPPProject>

MISP AND DECAYING OF INDICATORS

AN INDICATOR SCORING METHOD AND ONGOING IMPL-

TEAM CIRCL

INFO@CIRCL.LU

SEPTEMBER 11, 2024



MISP
Threat Sharing

EXPIRING IOCs: WHY AND HOW?

INDICATORS - PROBLEM STATEMENT

- Sharing information about threats is crucial
- Organisations are sharing more and more

Contribution by unique organisation (Orgc.name) on MISPPriv:

Date	Unique Org
2013	17
2014	43
2015	82
2016	105
2017	118
2018	125
2019-10	135

```
1 {  
2     "distribution": [1, 2, 3]  
3 }
```

INDICATORS - PROBLEM STATEMENT

- Various users and organisations can share data via MISP, multiple parties can be involved
 - ▶ Trust, data quality and time-to-live issues
 - ▶ Each user/organisation has different use-cases and interests
 - Conflicting interests such as operational security, attribution,... (depends on the user)
- Can be partially solved with *Taxonomies*

INDICATORS - PROBLEM STATEMENT

- Various users and organisations can share data via MISP, multiple parties can be involved
 - ▶ Trust, data quality and time-to-live issues
 - ▶ Each user/organisation has different use-cases and interests
 - Conflicting interests such as operational security, attribution,... (depends on the user)
- Can be partially solved with *Taxonomies*
- Attributes can be shared in large quantities (more than 7.3 million on MISPPRIV)
 - ▶ Partial info about their **freshness** (*Sightings*)
 - ▶ Partial info about their **validity** (last update)
- Can be partially solved with our *Decaying model*

REQUIREMENTS TO ENJOY THE DECAYING FEATURE IN MISP

- Starting from **MISP 2.4.116**, the decaying feature is available
- Don't forget to update the decay models and enable the ones you want
- The decaying feature has no impact on the information in MISP, it's just an overlay to be used in the user-interface and API
- Decay strongly relies on *Taxonomies* and *Sightings*, don't forget to review their configuration

SIGHTINGS - REFRESHER

Sightings add temporal context to indicators. A user, script or an IDS can extend the information related to indicators by reporting back to MISP that an indicator has been seen, or that an indicator can be considered as a false-positive

- *Sightings* give more credibility/visibility to indicators
- This information can be used to **prioritise and decay indicators**



ORGANISATIONS OPT-IN - SETTING A LEVEL OF CONFIDENCE

MISP is a peer-to-peer system, information passes through multiple instances.

- Producers can add context (such as tags from *Taxonomies*, *Galaxies*) about their asserted confidence or the reliability of the data
- Consumers can have different levels of trust in the producers and/or analysts themselves
- Users might have other contextual needs

→ Achieved thanks to *Taxonomies*

TAXONOMIES - REFRESHER (1)

Taxonomies

« previous 1 2 next »

Id	Namespace	Description	Version	Enabled	Required	Active Tags	Actions
181	workflow	Workflow support language is a common language to support intelligence analysts to perform their analysis on data and information.	9	Yes	<input type="checkbox"/>	27 / 26 (enable all)	
180	vocabulaire-des-probabilites-estimatives	Ce vocabulaire attribue des valeurs en pourcentage à certains énoncés de probabilité	2	Yes	<input type="checkbox"/>	5 / 5	
179	threats-to-dns	An overview of some of the known attacks related to DNS as described by Torabi, S., Boukhloufa, A., Assi, C., & Debbabi, M. (2018) in Detecting Internet Abuse by Analyzing Passive DNS Traffic: A Survey of Implemented Systems. IEEE Communications Surveys & Tutorials, 1–1, doi:10.1109/comst.2018.2849614	1	No	<input type="checkbox"/>	0 / 18	
178	targeted-threat-index	The Targeted Threat Index is a metric for assigning an overall threat ranking score to emails that deliver malware to a victim's computer. The TTI metric was first introduced at SectOr 2013 by Seth Hardy as part of the talk "RATastrophe: Monitoring a Malware Menagerie" along with Katie Kleemola and Greg Wiseman.	2	Yes	<input type="checkbox"/>	11 / 11	

- Tagging is a simple way to attach a classification to an *Event* or an *Attribute*
- Classification must be globally used to be efficient

TAXONOMIES - REFRESHER (2)

ADMIRALTY-SCALE Taxonomy Library

Id	127
Namespace	admiralty-scale
Description	The Admiralty Scale or Ranking (also called the NATO System) is used to rank the reliability of a source and the credibility of an information. Reference based on FM 2-22.3 (FM 34-52) HUMAN INTELLIGENCE COLLECTOR OPERATIONS and NATO documents.
Version	4
Enabled	Yes (disable)

[= previous](#) [next =](#)

<input type="checkbox"/> Tag	Expanded	Numerical value	Events	Attributes	Tags	Action		
<input type="checkbox"/> admiralty-scale:information-credibility="1"	Information Credibility: Confirmed by other sources	100	6	0	admiralty-scale:information-credibility="1"			-
<input type="checkbox"/> admiralty-scale:information-credibility="2"	Information Credibility: Probably true	75	21	1	admiralty-scale:information-credibility="2"			-
<input type="checkbox"/> admiralty-scale:information-credibility="3"	Information Credibility: Possibly true	50	16	5	admiralty-scale:information-credibility="3"			-
<input type="checkbox"/> admiralty-scale:information-credibility="4"	Information Credibility: Doubtful	25	2	0	admiralty-scale:information-credibility="4"			-
<input type="checkbox"/> admiralty-scale:information-credibility="5"	Information Credibility: Improbable	0	1	0	admiralty-scale:information-credibility="5"			-
<input type="checkbox"/> admiralty-scale:information-credibility="6"	Information Credibility: Truth cannot be judged	50	9	2	admiralty-scale:information-credibility="6"			-
<input type="checkbox"/> admiralty-scale:source-reliability="a"	Source Reliability: Completely reliable	100	1	0	admiralty-scale:source-reliability="a"			-
<input type="checkbox"/> admiralty-scale:source-reliability="b"	Source Reliability: Usually reliable	75	21	76	admiralty-scale:source-reliability="b"			-
<input type="checkbox"/> admiralty-scale:source-reliability="c"	Source Reliability: Fairly reliable	50	9	8	admiralty-scale:source-reliability="c"			-
<input type="checkbox"/> admiralty-scale:source-reliability="d"	Source Reliability: Not usually reliable	25	2	0	admiralty-scale:source-reliability="d"			-
<input type="checkbox"/> admiralty-scale:source-reliability="e"	Source Reliability: Unreliable	0	0	0	admiralty-scale:source-reliability="e"			-
<input type="checkbox"/> admiralty-scale:source-reliability="f"	Source Reliability: Reliability cannot be judged	50	10	7	admiralty-scale:source-reliability="f"			-
<input type="checkbox"/> admiralty-scale:source-reliability="g"	Source Reliability: Deliberately deceptive	0	N/A	N/A				

→ Cherry-pick allowed Tags

TAXONOMIES - REFRESHER (3)

- Some taxonomies have numerical_value
→ Can be used to prioritise Attributes

Description	Value
Completely reliable	100
Usually reliable	75
Fairly reliable	50
Not usually reliable	25
Unreliable	0
Reliability cannot be judged	50 ?
Deliberately deceptive	0 ?

Description	Value
Confirmed by other sources	100
Probably true	75
Possibly true	50
Doubtful	25
Improbable	0
Truth cannot be judged	50 ?

SCORING INDICATORS: OUR SOLUTION

$$\text{score}(\text{Attribute}) = \text{base_score}(\text{Attribute}, \text{Model}) \bullet \text{decay}(\text{Model}, \text{time})$$

Where,

- $\text{score} \in [0, +\infty]$
- $\text{base_score} \in [0, 100]$
- decay is a function defined by model's parameters controlling decay speed
- Attribute Contains *Attribute's values and metadata* (*Taxonomies, Galaxies, ...*)
- Model Contains the *Model's configuration*

CURRENT IMPLEMENTATION IN MISP

IMPLEMENTATION IN MISP: Event/view

The screenshot shows the MISP Event view interface. At the top, there are navigation links: Pivots, Galaxy, Event graph, Correlation graph, ATTACK matrix, Attributes, and Discussion. Below the navigation is a search bar with the placeholder 'x-45: Decay...'. A blue button labeled 'Galaxies' is highlighted. Underneath, there's a section titled 'Galaxies' with a user icon and a plus sign. At the bottom of this section are buttons for '< previous', 'next >', and 'View all'.

The main content area displays a table of events. The columns include: Date, Org, Category, Type, Value, Tags, Galaxies, Comment, Correlate, Related Events, Feed hits, IDS, Distribution, Sightings, Activity, Score, and Actions. The table lists the following events:

Date	Org	Category	Type	Value	Tags	Galaxies	Comment	Correlate	Related Events	Feed hits	IDS	Distribution	Sightings	Activity	Score	Actions
2019-09-12		Network activity	ip-src	5.5.5.5	admiralty-scale:source-reliability:"a" retention:expired						Inherit		(0 0 0)		NIDS Simple Decaying ... 65.26	
2019-08-13		Network activity	ip-src	8.8.8.8	admiralty-scale:source-reliability:"a" retention:expired					1 2 2 2	S1:1	Inherit	(5 0 0)		NIDS Simple Decaying ... 54.6	
2019-08-13		Network activity	ip-src	9.9.9.9	admiralty-scale:source-reliability:"c" misp:confidence-level:"completely-confident" tlp:amber					1 3 19 28	S1:1	Inherit	(4 1 0)	Show 6 more...	NIDS Simple Decaying ... 37.43	
2019-08-13		Network activity	ip-src	7.7.7.7	admiralty-scale:information-credibility:"d" retention:2d					41		Inherit	(0 0 0)		NIDS Simple Decaying ... 37.41	
2019-07-18		Network activity	ip-src	6.6.6.6						41		Inherit	(0 0 0)		NIDS Simple Decaying ... 23.31	

- Decay score toggle button
 - ▶ Shows Score for each *Models* associated to the *Attribute* type

IMPLEMENTATION IN MISP: API RESULT

/attributes/restSearch

```
1 "Attribute": [
2   {
3     "category": "Network activity",
4     "type": "ip-src",
5     "to_ids": true,
6     "timestamp": "1565703507",
7     [...]
8     "value": "8.8.8.8",
9     "decay_score": [
10       {
11         "score": 54.475223849544456,
12         "decayed": false,
13         "DecayingModel": {
14           "id": "85",
15           "name": "NIDS Simple Decaying Model"
16         }
17       },
18     ],
19   [...]
```

IMPLEMENTATION IN MISP: PLAYING WITH MODELS

- **Automatic scoring** based on default values
- **User-friendly UI** to manually set *Model* configuration (lifetime, decay, etc.)
- **Simulation tool**
- Interaction through the **API**
- Opportunity to create your **own** formula or algorithm

DECAYING MODELS IN DEPTH

SCORING INDICATORS: base_score (1)

$$\text{score}(\text{Attribute}) = \text{base_score}(\text{Attribute, Model}) \bullet \text{decay}(\text{Model, time})$$

When scoring indicators¹, multiple parameters² can be taken into account. The **base score** is calculated with the following in mind:

- Data reliability, credibility, analyst skills, custom prioritisation tags (economical-impact), etc.
- Trust in the source

$$\text{base_score} = \omega_{tg} \cdot \text{tags} + \omega_{sc} \cdot \text{source_confidence}$$

Where,

$$\omega_{sc} + \omega_{tg} = 1$$

¹Paper available: <https://arxiv.org/pdf/1803.11052>

²at a variable extent as required

SCORING INDICATORS: base_score (2)

Current implementation ignores source_confidence:

$$\rightarrow \text{base_score} = \text{tags}$$

Tag	Computation			Result	
	Eff.				
		Ratio	numerical_value		
admiralty-scale:source-reliability="Completely reliable"	0.50	*	100.00	50.00	
phishing:psychological-acceptability="high"	0.50	*	75.00	37.50	

→ The base_score can be used to prioritize attribute based on their attached context and source

SCORING INDICATORS: DECAY SPEED (1)

$$\text{score}(\text{Attribute}) = \text{base_score}(\text{Attribute, Model}) \bullet \text{decay}(\text{Model, time})$$

The decay is calculated using:

- The lifetime of the indicator
 - ▶ May vary depending on the indicator type
 - ▶ short for an IP, long for a hash
- The decay rate, or speed at which an attribute loses score over time
- The time elapsed since the latest update or sighting

SCORING INDICATORS: PUTTING IT ALL TOGETHER

→ decay rate is **re-initialized upon sighting** addition, or said differently, the score is reset to its base score as new sightings are applied.

$$\text{score} = \text{base_score} \cdot \left(1 - \left(\frac{t}{\tau} \right)^{\frac{1}{\delta}} \right)$$

- τ = lifetime
- δ = decay speed

IMPLEMENTATION IN MISP: MODELS DEFINITION

$$\rightarrow \text{score} = \text{base_score} \cdot \left(1 - \left(\frac{t}{\tau}\right)^{\frac{1}{\delta}}\right)$$

Models are an instantiation of the formula where elements can be defined:

- Parameters: `lifetime`, `decay_rate`, `threshold`
- `base_score`
- default `base_score`
- `formula`
- associate *Attribute* types
- creator organisation

IMPLEMENTATION IN MISP: MODELS TYPES

Multiple model types are available

- **Default Models:** Models created and shared by the community. Available from `misp-decaying-models` repository³.
 - ▶ → Not editable
- **Organisation Models:** Models created by a user belonging to an organisation
 - ▶ These models can be hidden or shared to other organisation
 - ▶ → Editable

³<https://github.com/MISP/misp-decaying-models.git>

IMPLEMENTATION IN MISP: INDEX

Decaying Models

All Models		My Models		Shared Models		Default Models				
ID	Organization	Usable to everyone	Name	Description	Parameters { } 	Formula	# Assigned Types	Version	Enabled	Actions
29	1	✓	Phishing model	Simple model to rapidly decay phishing website.	{ "lifetime": 3, "decay_speed": 2.3, "threshold": 30, "default_base_score": 80, "base_score_config": { "estimative-language": 0.5, "phishing": 0.5 } }	Polynomial 	9	1	✓	   
85	1	✗	NIDS Simple Decaying Model 	Simple decaying model for Network Intrusion Detection System (NIDS).	{ "lifetime": 120, "decay_speed": 2, "threshold": 30, "default_base_score": 80, "base_score_config": { "estimative-language": 0.25, "priority-level": 0.25, "retention": 0.25, "targeted-threat-index": 0.125, "false-positive": 0.125 } }	Polynomial 	13	1	✓	   

Page 1 of 1, showing 2 records out of 2 total, starting on record 1, ending on 2

[« previous](#) [next »](#)

View, update, add, create, delete, enable, export, import

IMPLEMENTATION IN MISP: FINE TUNING TOOL

Home Event Actions Databases Input Filters Global Actions Sync Actions Administration Audit MISP AI

Import Decoying Model
Add Decoying Model
Decoying Test
List Decoying Models

Decaying Of Indicator Fine Tuning Tool

Show All Types Show MISP Objects Search Attribute Type

Attribute Type	Category	Model ID
abs-r11	Financial fraud	
authenthash	Payload delivery	
bank-account-nr	Financial fraud	
btc	Financial fraud	
bin	Financial fraud	
bro	Network activity	ID 11
btc	Financial fraud	11
cc-number	Financial fraud	
cphash	Payload delivery	
community-id	Network activity	
domain	Network activity	
domainip	Network activity	10-84
email-attachment	Payload delivery	
email-dst	Network activity	11
email-src	Payload delivery	
filename	Payload delivery	
filenameauthenthash	Payload delivery	
filenamefuzzy	Payload delivery	
filenamephash	Payload delivery	
filenamejs	Payload delivery	13
filenamejsphash	Payload delivery	13
filenamesha1	Payload delivery	13

Polynomial

Lifetime: 3 days
Decay speed: 2.3
Cut-off threshold: 30
Adjust base score: Simulate this model:

Phishing model: Simple model to rapidly decay Take

All available models My models Default models

ID	Model Name	Org ID	Description	Formula	Lifetime	Decay speed	Threshold	Default Basesscore	Basesscore config	Settings	# Types	Enabled	Action
29	Phishing model	1	Simple model to rapidly decay	Polynomial	3	2.3	30	80	estimative-language-phishing website.	0.5	9	<input checked="" type="checkbox"/>	<input type="button" value="Load model"/>

Create, modify, visualise, perform mapping

IMPLEMENTATION IN MISP: base_score TOOL

Search Taxonomy x 3 not having numerical value

Default basescore: 80

Taxonomies	Weight
admiralty-scale ▾	
source-reliability ▾	31
information-credibility ▾	30
priority-level ▾	
priority-level ▾	53
retention ▾	
retention ▾	0
estimative-language ▾	
likelihood-probability ▾	0
confidence-in-analytic-judgment ▾	0
misp ▾	
confidence-level ▾	0
threat-level ▾	0
automation-level ▾	0
phishing ▾	
state ▾	0
psychological-acceptability ▾	0
Excluded ▾	

Placeholder for 'Organisation source confidence'

Example

Attribute	Tags	Base score
Tag your attribute		
Attribute 1	admiralty-scale:information-credibility="5"	0.0 ⓘ
Attribute 2	priority-level:baseline-minor admiralty-scale:source-reliability="d" admiralty-scale:information-credibility="2"	38.2 ⓘ
Attribute 3	priority-level:severe admiralty-scale:information-credibility="2"	84.6 ⓘ

Computation steps

Tag	Computation	Result
	Eff. Ratio	Value
priority-level:baseline-minor	0.46 *	25.00 11.62
admiralty-scale:source-reliability="d"	0.27 *	25.00 6.80

IMPLEMENTATION IN MISP: SIMULATION TOOL

NIDS Simple Decaying Model

RestSearch Specific ID

Attribute RestSearch*

```
{"includeDecayScore": 1, "includeFullModel": 0, "score": 30, "excludeDecayed": 0, "decayingModel": [85], "to_ids": 1, "tags": ["estimative-language%", "priority-low%", "interiorotic%", "targeted-threat"], "id": 36759}
```

Search

Sighting: Wed Sep 4 12:18:09 2019 | Current score: 54.60

Base score: Base score configuration not set. But default value sets.

Tag	Computation	Result
misp:confidence-level="usually-confident"	EII, Ratio	0 × 75.00 0
misp:confidence-level="fairly-confident"	EII, Ratio	0 × 50.00 0
adversary-scale-source-reliability="a"	EII, Ratio	0 × 100.00 0
retention_expired	EII, Ratio	0 × Non 0
base_score		80.00

Graph showing the decay of the base score over time:

ID	Event	T	Date	Org	Category	Type	Value	Tags	Event Tags	Galaxies	Comment	IDS	Sightings	Score
36759	45		2019-08-13	ORIONAME	Network activity	ip-src	7.7.7.7	adversary-scale-information-confidence="C" retention_id	misp:confidence-level="usually-confident" misp:confidence-level="fairly-confident"			✓		NIDS Simple Decaying ... 37.41
36757	45		2019-08-13	ORIONAME	Network activity	ip-src	8.8.8.8	adversary-scale-source-reliability="a" retention_expired	misp:confidence-level="usually-confident" misp:confidence-level="fairly-confident"			✓		NIDS Simple Decaying ... 54.6

Page 1 of 1, showing 2 records out of 2 total, starting on record 1, ending on 2

< previous next >

Simulate Attributes with different Models

IMPLEMENTATION IN MISP: API QUERY BODY

/attributes/restSearch

```
1  {
2      "includeDecayScore": 1,
3      "includeFullModel": 0,
4      "excludeDecayed": 0,
5      "decayingModel": [85],
6      "modelOverrides": {
7          "threshold": 30
8      }
9      "score": 30,
10
11 }
```

CREATING A NEW DECAY ALGORITHM (1)

The current architecture allows users to create their **own** formulae.

1. Create a new file `$filename` in
`app/Model/DecayingModelsFormulas/`
2. Extend the Base class as defined in `DecayingModelBase`
3. Implement the two mandatory functions `computeScore` and `isDecayed` using your own formula/algorithm
4. Create a Model and set the formula field to `$filename`

Use cases:

- Add support for **more feature** (expiration taxonomy)
- **Query external services** then influence the score
- Completely **different approach** (i.e streaming algorithm)
- ...

CREATING A NEW DECAY ALGORITHM (2)

```
1 <?php
2 include_once 'Base.php';
3
4 class Polynomial extends DecayingModelBase
{
5     public const DESCRIPTION = 'The description of your new
6     decaying algorithm';
7
8     public function computeScore($model, $attribute, $base_score,
9     $elapsed_time)
10    {
11        // algorithm returning a numerical score
12    }
13
14    public function isDecayed($model, $attribute, $score)
15    {
16        // algorithm returning a boolean stating
17        // if the attribute is expired or not
18    }
19 ?>
```

DECAYING MODELS 2.0

- Improved support of *Sightings*
 - ▶ False positive *Sightings* should somehow reduce the score
 - ▶ Expiration *Sightings* should mark the attribute as decayed
- Potential Model improvements
 - ▶ Instead of resetting the score to `base_score` once a *Sighting* is set, the score should be increased additively (based on a defined coefficient); thus **prioritizing surges** rather than infrequent *Sightings*
 - ▶ Take into account related *Tags* or *Correlations* when computing score
- Increase *Taxonomy* coverage
 - ▶ Users should be able to manually override the `numerical_value` of *Tags*
- For specific type, take into account data from other services
 - ▶ Could fetch data from *BGP ranking*, *Virus Total*, *Passive X* for IP/domain/... and adapt the score

MISP AND DECAYING OF INDICATORS

PRIMER FOR INDICATOR SCORING IN MISP

TEAM CIRCL

INFO@CIRCL.LU

SEPTEMBER 11, 2024



MISP
Threat Sharing

OUTLINE OF THE PRESENTATION

- Present the components used in MISP to expire IOCs
- Present the current state of Indicators life-cycle management in MISP

EXPIRING IOCs: WHY AND HOW?

INDICATORS LIFECYCLE - PROBLEM STATEMENT

- Sharing information about threats is crucial
- Organisations are sharing more and more

Contribution by unique organisation (Orgc.name) on MISPPriv:

Date	Unique Org
2013	17
2014	43
2015	82
2016	105
2017	118
2018	125
2019-10	135

```
1 {  
2     "distribution": [1, 2, 3]  
3 }
```

INDICATORS LIFECYCLE - PROBLEM STATEMENT

- Various users and organisations can share data via MISP, multiple parties can be involved
 - ▶ **Trust, data quality** and **relevance** issues
 - ▶ Each user/organisation have **different use-cases** and interests
 - Conflicting interests: Operational security VS attribution
- Can be partially solved with *Taxonomies*

INDICATORS LIFECYCLE - PROBLEM STATEMENT

- Various users and organisations can share data via MISP, multiple parties can be involved
 - ▶ Trust, data quality and relevance issues
 - ▶ Each user/organisation have different use-cases and interests
 - Conflicting interests: Operational security VS attribution
- Can be partially solved with *Taxonomies*
- Attributes can be shared in large quantities (more than 12M on MISPPRIV - Sept. 2020)
 - ▶ Partial info about their freshness (*Sightings*)
 - ▶ Partial info about their validity (*last_seen*)
- Can be partially solved with our *Data model*

MISP's *Decaying model* combines the two

REQUIREMENTS TO ENJOY THE DECAYING FEATURE IN MISP

- Starting from **MISP 2.4.116**, the decaying feature is available
- **Update** decay models and **enable** some
- MISP Decaying strongly relies on *Taxonomies* and *Sightings*, don't forget to review their configuration

Note: The decaying feature has no impact on the information stored in MISP, it's just an **overlay** to be used in the user-interface and API

SIGHTINGS - REFRESHER (1)

Sightings add a **temporal context** to indicators.

- *Sightings* can be used to represent that you saw the IoC
- **Usecase:** Continuous feedback loop MISP ↔ IDS



SIGHTINGS - REFRESHER (2)

Sightings add a **temporal context** to indicators.

- *Sightings* give more credibility/visibility to indicators
- This information can be used to **prioritise and decay indicators**

TAXONOMIES - REFRESHER (1)

Taxonomies

« previous 1 2 next »

Id	Namespace	Description	Version	Enabled	Required	Active Tags	Actions
181	workflow	Workflow support language is a common language to support intelligence analysts to perform their analysis on data and information.	9	Yes	<input type="checkbox"/>	27 / 26 (enable all)	
180	vocabulaire-des-probabilites-estimatives	Ce vocabulaire attribue des valeurs en pourcentage à certains énoncés de probabilité	2	Yes	<input type="checkbox"/>	5 / 5	
179	threats-to-dns	An overview of some of the known attacks related to DNS as described by Torabi, S., Boukhtouta, A., Assi, C., & Debbabi, M. (2018) in Detecting Internet Abuse by Analyzing Passive DNS Traffic: A Survey of Implemented Systems. IEEE Communications Surveys & Tutorials, 1–1, doi:10.1109/comst.2018.2849614	1	No	<input type="checkbox"/>	0 / 18	
178	targeted-threat-index	The Targeted Threat Index is a metric for assigning an overall threat ranking score to email messages that deliver malware to a victim's computer. The TTI metric was first introduced at SectOr 2013 by Seth Hardy as part of the talk "RATastrophe: Monitoring a Malware Menagerie" along with Katie Kleemola and Greg Wiseman.	2	Yes	<input type="checkbox"/>	11 / 11	

- *Taxonomies are a simple way to attach a classification to an Event or an Attribute*
- *Classification must be globally used to be efficient (or agreed on beforehand)*

TAXONOMIES - REFRESHER (2)

ADMIRALTY-SCALE Taxonomy Library

Id	127
Namespace	admiralty-scale
Description	The Admiralty Scale or Ranking (also called the NATO System) is used to rank the reliability of a source and the credibility of an information. Reference based on FM 2-22.3 (FM 34-52) HUMAN INTELLIGENCE COLLECTOR OPERATIONS and NATO documents.
Version	4
Enabled	Yes (disable)

= previous next =

<input type="checkbox"/> Tag	Expanded	Numerical value	Events	Attributes	Tags	Action
<input type="checkbox"/> admiralty-scale:information-credibility="1"	Information Credibility: Confirmed by other sources	100	6	0	admiralty-scale:information-credibility="1"	 
<input type="checkbox"/> admiralty-scale:information-credibility="2"	Information Credibility: Probably true	75	21	1	admiralty-scale:information-credibility="2"	 
<input type="checkbox"/> admiralty-scale:information-credibility="3"	Information Credibility: Possibly true	50	16	5	admiralty-scale:information-credibility="3"	 
<input type="checkbox"/> admiralty-scale:information-credibility="4"	Information Credibility: Doubtful	25	2	0	admiralty-scale:information-credibility="4"	 
<input type="checkbox"/> admiralty-scale:information-credibility="5"	Information Credibility: Improbable	0	1	0	admiralty-scale:information-credibility="5"	 
<input type="checkbox"/> admiralty-scale:information-credibility="6"	Information Credibility: Truth cannot be judged	50	9	2	admiralty-scale:information-credibility="6"	 
<input type="checkbox"/> admiralty-scale:source-reliability="a"	Source Reliability: Completely reliable	100	1	0	admiralty-scale:source-reliability="a"	 
<input type="checkbox"/> admiralty-scale:source-reliability="b"	Source Reliability: Usually reliable	75	21	76	admiralty-scale:source-reliability="b"	 
<input type="checkbox"/> admiralty-scale:source-reliability="c"	Source Reliability: Fairly reliable	50	9	8	admiralty-scale:source-reliability="c"	 
<input type="checkbox"/> admiralty-scale:source-reliability="d"	Source Reliability: Not usually reliable	25	2	0	admiralty-scale:source-reliability="d"	 
<input type="checkbox"/> admiralty-scale:source-reliability="e"	Source Reliability: Unreliable	0	0	0	admiralty-scale:source-reliability="e"	 
<input type="checkbox"/> admiralty-scale:source-reliability="f"	Source Reliability: Reliability cannot be judged	50	10	7	admiralty-scale:source-reliability="f"	 
<input type="checkbox"/> admiralty-scale:source-reliability="g"	Source Reliability: Deliberately deceptive	0	N/A	N/A		

→ Cherry-pick allowed Tags

TAXONOMIES - REFRESHER (3)

- Some taxonomies have a numerical_value
- Allows concepts to be used in an mathematical expression
 - Can be used to prioritise IoCs

admiralty-scale taxonomy¹

Description	Value
Completely reliable	100
Usually reliable	75
Fairly reliable	50
Not usually reliable	25
Unreliable	0
Reliability cannot be judged	50
Deliberately deceptive	0

Description	Value
Confirmed by other sources	100
Probably true	75
Possibly true	50
Doubtful	25
Improbable	0
Truth cannot be judged	50

¹<https://github.com/MISP/misp-taxonomies/blob/master/admiralty-scale/machinetag.json>

TAXONOMIES - REFRESHER (3)

admiralty-scale taxonomy²

Description	Value
Completely reliable	100
Usually reliable	75
Fairly reliable	50
Not usually reliable	25
Unreliable	0
Reliability cannot be judged	50 ?
Deliberately deceptive	0 ?

Description	Value
Confirmed by other sources	100
Probably true	75
Possibly true	50
Doubtful	25
Improbable	0
Truth cannot be judged	50 ?

→ Users can override tag numerical_value

²<https://github.com/MISP/misp-taxonomies/blob/master/admiralty-scale/machinetag.json>

SCORING INDICATORS: OUR SOLUTION

$$\text{score}(\text{Attribute}) = \text{base_score}(\text{Attribute}, \text{Model}) \bullet \text{decay}(\text{Model}, \text{time})$$

■ $\text{base_score}(\text{Attribute}, \text{Model})$

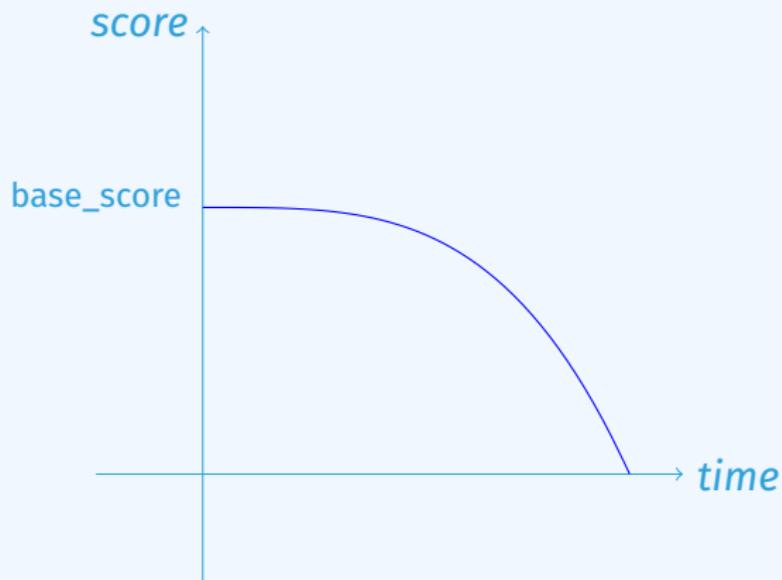
- ▶ Initial score of the *Attribute* only considering the context (*Attribute's type, Tags*)

■ $\text{decay}(\text{Model}, \text{time})$

- ▶ Function composed of the **lifetime** and **decay speed**
- ▶ Decreases the *base_score* over time

SCORING INDICATORS: OUR SOLUTION

$$\text{score}(\text{Attribute}) = \text{base_score}(\text{Attribute, Model}) \bullet \text{decay}(\text{Model, time})$$



CURRENT IMPLEMENTATION IN MISP

IMPLEMENTATION IN MISP: Event/view

The screenshot shows the MISP Event view interface. At the top, there are navigation links: Pivots, Galaxy, Event graph, Correlation graph, ATTACK matrix, Attributes, and Discussion. Below the navigation is a search bar with the placeholder 'x-45: Decay...'. A blue button labeled 'Galaxies' is highlighted. Underneath, there's a section titled 'Galaxies' with a user icon and a plus sign. Below this are buttons for 'previous', 'next >', and 'View all'.

The main area displays a table of events. The columns include: Date, Org, Category, Type, Value, Tags, Galaxies, Comment, Correlate, Related Events, Feed hits, IDS, Distribution, Sightings, Activity, Score, and Actions. The table lists the following events:

Date	Org	Category	Type	Value	Tags	Galaxies	Comment	Correlate	Related Events	Feed hits	IDS	Distribution	Sightings	Activity	Score	Actions	
2019-09-12		Network activity	ip-src	5.5.5.5	admiralty-scale:source-reliability:"a" retention:expired						Inherit	(0 0 0)	NIDS Simple Decaying ...	65.26			
2019-08-13		Network activity	ip-src	8.8.8.8	admiralty-scale:source-reliability:"a" retention:expired				1 2 2 2 Show 11 more...	5 1 1	Inherit	(5 0 0)	NIDS Simple Decaying ...	54.6			
2019-08-13		Network activity	ip-src	9.9.9.9	admiralty-scale:source-reliability:"c" misp:confidence-level:"completely-confident"! tlp:amber				1 3 19 28 Show 6 more...	5 1 1	Inherit	(4 1 0)	NIDS Simple Decaying ...	37.43			
2019-08-13		Network activity	ip-src	7.7.7.7	admiralty-scale:information-credibility:"d" retention:2d				41		Inherit	(0 0 0)	NIDS Simple Decaying ...	37.41			
2019-07-18		Network activity	ip-src	6.6.6.6					41		Inherit	(0 0 0)	NIDS Simple Decaying ...	23.31			

- Decay score toggle button
 - ▶ Shows Score for each *Models* associated to the *Attribute* type

IMPLEMENTATION IN MISP: API RESULT

/attributes/restSearch

```
1 "Attribute": [
2   {
3     "category": "Network activity",
4     "type": "ip-src",
5     "to_ids": true,
6     "timestamp": "1565703507",
7     [...]
8     "value": "8.8.8.8",
9     "decay_score": [
10       {
11         "score": 54.475223849544456,
12         "decayed": false,
13         "DecayingModel": {
14           "id": "85",
15           "name": "NIDS Simple Decaying Model"
16         }
17       },
18     ],
19   [...]
```

IMPLEMENTATION IN MISP: OBJECTIVES

- **Automatic scoring** based on default values
- **User-friendly UI** to manually set *Model* configuration (lifetime, decay, etc.)
- **Simulation tool**
- Interaction through the **API**
- Opportunity to create your **own** formula or algorithm

IMPLEMENTATION IN MISP: MODELS DEFINITION

$$\Rightarrow \text{score} = \text{base_score} \cdot \left(1 - \left(\frac{t}{\tau}\right)^{\frac{1}{\delta}}\right)$$

Models are an instantiation of the formula with configurable parameters:

- Parameters: `lifetime`, `decay_rate`, `threshold`
- `base_score` computation
- default `base_score`
- associate *Attribute* types
- formula
- creator organisation

IMPLEMENTATION IN MISP: MODELS TYPES

Two types of model are available

- **Default Models:** Created and shared by the community.
Coming from `misp-decaying-models` repository³.
 - Not editable

- **Organisation Models:** Created by a user on MISP
 - ▶ Can be hidden or shared to other organisation
 - Editable

³<https://github.com/MISP/misp-decaying-models.git>

IMPLEMENTATION IN MISP: INDEX

Decaying Models

« previous next »

All Models	My Models	Shared Models	Default Models	ID	Organization	Usable to everyone	Name	Description	Parameters { } 	Formula	# Assigned Types	Version	Enabled	Actions
				29	1	✓	Phishing model	Simple model to rapidly decay phishing website.	{ "lifetime": 3, "decay_speed": 2.3, "threshold": 30, "default_base_score": 80, "base_score_config": { "estimative-language": 0.5, "phishing": 0.5 } }	Polynomial 	9	1	✓	   
				85	1	✗	NIDS Simple Decaying Model 	Simple decaying model for Network Intrusion Detection System (NIDS).	{ "lifetime": 120, "decay_speed": 2, "threshold": 30, "default_base_score": 80, "base_score_config": { "estimative-language": 0.25, "priority-level": 0.25, "retention": 0.25, "targeted-threat-index": 0.125, >false-positive": 0.125 } }	Polynomial 	13	1	✓	   

Page 1 of 1, showing 2 records out of 2 total, starting on record 1, ending on 2

« previous next »

Standard CRUD operations: View, update, add, create, delete, enable, export, import

IMPLEMENTATION IN MISP: FINE TUNING TOOL

Home Event Actions Databases Input Filters Global Actions Sync Actions Administration Audit MISP AI

Import Decoying Model
Add Decoying Model
Decoying Tool
List Decoying Models

Decoying Of Indicator Fine Tuning Tool

Show All Types Show MISP Objects Search Attribute Type

Attribute Type	Category	Model ID
file-r11	Financial fraud	
authentihash	Payload delivery	
bank-account-nr	Financial fraud	
btc	Financial fraud	
bin	Financial fraud	
bro	Network activity	ID 11
btc	Financial fraud	11
cc-number	Financial fraud	
cphash	Payload delivery	
community-id	Network activity	
domain	Network activity	
domainip	Network activity	10-84
email-attachment	Payload delivery	
email-dst	Network activity	11
email-src	Payload delivery	
filename	Payload delivery	
filenameauthentihash	Payload delivery	
filenameimpfuzzy	Payload delivery	
filenamejephash	Payload delivery	
filenamejres	Payload delivery	13
filenamejshash	Payload delivery	13
filenamejs1	Payload delivery	13

Polynomial

Lifetime: 3 days
Decay speed: 2.3
Cut-off threshold: 30
Adjust base score: Simulate this model:

Phishing model: Simple model to rapidly decay Take

All available models My models Default models

ID	Model Name	Org ID	Description	Formula	Lifetime	Decay speed	Threshold	Default basesscore	Basescore config	Settings	# Types	Enabled	Action
29	Phishing model	1	Simple model to rapidly decay	polynomial	3	2.3	30	80	estimative-language	0.5	9	<input checked="" type="checkbox"/>	<input type="button" value="Load model"/>
									phishing website.				

Configure models: Create, modify, visualise, perform mapping

IMPLEMENTATION IN MISP: base_score TOOL

Search Taxonomy x 3 not having numerical value

Default basescore: 80

Taxonomies	Weight
admiralty-scale ▾	
source-reliability ▾	31
information-credibility ▾	30
priority-level ▾	
priority-level ▾	53
retention ▾	
retention ▾	0
estimative-language ▾	
likelihood-probability ▾	0
confidence-in-analytic-judgment ▾	0
misp ▾	
confidence-level ▾	0
threat-level ▾	0
automation-level ▾	0
phishing ▾	
state ▾	0
psychological-acceptability ▾	0
Excluded ▾	

Placeholder for 'Organisation source confidence'

admiralty-scale information-credibility (20%) priority-level (68%)

admiralty-scale source-reliability (27%)

Example ⓘ

Attribute	Tags	Base score
Tag your attribute		
Attribute 1	admiralty-scale information-credibility="5"	0.0 ⓘ
Attribute 2	priority-level:baseline-minor admiralty-scale:source-reliability="d" admiralty-scale information-credibility="2"	38.2 ⓘ
Attribute 3	priority-level:severe admiralty-scale:information-credibility="2"	84.6 ⓘ

Computation steps

Tag	Computation		Result
	Eff. Ratio	Value	
priority-level:baseline-minor	0.46	*	25.00 11.62
admiralty-scale:source-reliability="d"	0.27	*	25.00 6.80

IMPLEMENTATION IN MISP: SIMULATION TOOL

NIDS Simple Decaying Model

RestSearch Specific ID

Attribute RestSearch*

```
{"includeDecayScore": 1, "includeFullModel": 0, "score": 30, "excludeDecayed": 0, "decayingModel": [85], "to_ids": 1, "tags": ["estimative-language"], "priority_levels": "intermediate", "targeted_threat": true}
```

Search

Base score: Base score configuration not set. But default value sets.

Tag	Computation	Result
misp:confidence-level="usually-confident"	Eff. Ratio: 0	Value: 75.00
misp:confidence-level="fairly-confident"	Eff. Ratio: 0	Value: 50.00
adversary-scale-source-reliability="a"	Eff. Ratio: 0	Value: 100.00
retention_expired	Eff. Ratio: 0	Value: NaN
base score		80.00

Sighting: Wed Sep 4 12:18:09 2019 | Current score: 54.60

The graph plots the 'base score' over time. It starts at 80.00 in August, drops to approximately 55.00, then fluctuates between 50.00 and 60.00 through early September. A vertical line marks the retention deadline on September 4th. After this point, the score decays steadily to about 37.41 by the end of the month. A red shaded area highlights the period from August 1st to September 4th.

ID	Event	Date	Org	Category	Type	Value	Tags	Event Tags	Galaxies	Comment	IDS	Sightings	Score
36759	45	2019-06-13	ORGNAME	Network activity	ip-src	7.7.7.7	adversary-scale-information-confidence="a" retention:2d	misp:confidence-level="usually-confident" misp:confidence-level="fairly-confident"			✓		NIDS Simple Decaying ... 37.41
36757	45	2019-06-13	ORGNAME	Network activity	ip-src	8.8.8.8	adversary-scale-source-reliability="a" retention:expired	misp:confidence-level="usually-confident" misp:confidence-level="fairly-confident"			✓		NIDS Simple Decaying ... 54.6

Page 1 of 1, showing 2 records out of 2 total, starting on record 1, ending on 2

< previous next >

Simulate decay on *Attributes* with different *Models*

IMPLEMENTATION IN MISP: API QUERY BODY

/attributes/restSearch

```
1  {
2      "includeDecayScore": 1,
3      "includeFullModel": 0,
4      "excludeDecayed": 0,
5      "decayingModel": [85],
6      "modelOverrides": {
7          "threshold": 30
8      }
9      "score": 30,
10 }
11 }
```

CREATING A NEW DECAY ALGORITHM

```
1 <?php
2 include_once 'Base.php';
3
4 class Polynomial extends DecayingModelBase
{
5     public const DESCRIPTION = 'The description of your new
6     decaying algorithm';
7
8     public function computeScore($model, $attribute, $base_score,
9     $elapsed_time)
10    {
11        // algorithm returning a numerical score
12    }
13
14    public function isDecayed($model, $attribute, $score)
15    {
16        // algorithm returning a boolean stating
17        // if the attribute is expired or not
18    }
19 ?>
```

DECAYING MODELS 2.0

- Improved support of *Sightings*
 - ▶ False positive *Sightings* should somehow reduce the score
 - ▶ Expiration *Sightings* should mark the attribute as decayed
- Potential *Model* improvements
 - ▶ Instead of resetting the score to `base_score` once a *Sighting* is set, the score should be increased additively (based on a defined coefficient); thus **prioritizing surges** rather than infrequent *Sightings*
 - ▶ Take into account related *Tags* or *Correlations* when computing score
- Increase *Taxonomy* coverage
 - ▶ Users should be able to manually override the `numerical_value` of *Tags*

FORENSIC SUPPORT IN MISP

TOOLS AND VISUALIZATION TO SUPPORT DIGITAL

TEAM CIRCL

INFO@CIRCL.LU

SEPTEMBER 11, 2024



MISP
Threat Sharing

DFIR AND MISP DIGITAL EVIDENCES

- **Share analyses and reports** of digital forensic evidences.
- **Propose changes** to existing analyses or reports.
- Extending existing events with additional evidences for local or use in limited distribution sharing (sharing can be defined at event level or attribute level).
- **Evaluate correlations**¹ of evidences against external or local attributes.
- **Report sightings** such as false-positive or true-positive (e.g. a partner/analyst has seen a similar indicator).

¹MISP has a flexible correlation engine which can correlate on 1-to-1 value matches, but also on fuzzy hashing (e.g. ssdeep) or CIDR block matching.

BENEFITS OF USING MISP

- LE can leverage the long-standing experience in information sharing and **bridge their use-cases** with MISP's information sharing mechanisms.
- **Accessing existing MISP information sharing communities** by receiving actionable information from CSIRT/CERT networks or security researchers.
- **Bridging LE communities with other communities.** Sharing groups can be created (and managed) cross-sectors to support specific use-cases.
- The **MISP standard** is a flexible format which can be extended by users using the MISP platform. A MISP object template can be created in under 30 minutes, allowing users to rapidly share information using their own data-models with existing communities.

CHALLENGES AND IMPLEMENTATIONS

- Standard sharing mechanism for forensic cases
 - ▶ MISP allows for the efficient **collaborative** analysis of digital evidences
 - ▶ Correlation on certain attributes
- Importing disk images and file system data activity (Mactime)
 - ▶ Development of an adaptable import tool: From Mactime to MISP Mactime object
- Create, modify and visualise the timeline of events
 - ▶ Development of a flexible timeline system at the event level

FORENSIC IMPORT (MISP 2.4.98)

Import analysis file

Analysis file

test.txt

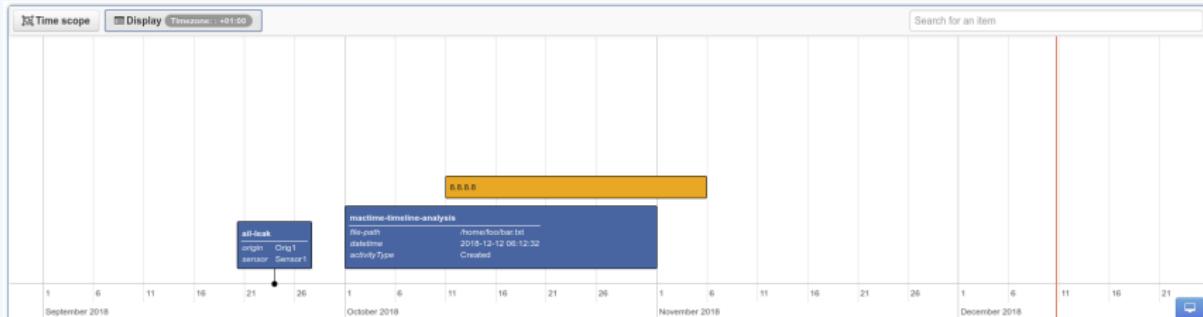
Create Objects

Select text for further analysis

Select	Filepath	File Size	Activity Type	Time Accessed	Permissions
<input type="checkbox"/>	..c.r/rrwxrwxrwx	Xxx			00
<input checked="" type="checkbox"/>	/DCIM/111_06/_MG_0125.JPG(deleted)	3541836	Accessed	Sun Jun 02 2013 00:00:00	r/rrwxrwxrwx
<input checked="" type="checkbox"/>	/DCIM/111_06/_MG_0125.JPG(deleted)	3541836	Created,Modified	Sun Jun 02 2013 15:42:32	r/rrwxrwxrwx
<input checked="" type="checkbox"/>	/DCIM/111_06/IMG_0126.JPG	2255115	Created,Modified	Sun Jun 02 2013 15:42:46	r/rrwxrwxrwx
<input type="checkbox"/>	/DCIM/CANONMSC/M0111.CTG	884	Created,Modified	Sun Jun 02 2013 15:44:08	r/rrwxrwxrwx
<input type="checkbox"/>	/CANON_DC(Volume	0	Modified	Sun Jun 02 2013 16:33:04	r/rrwxrwxrwx
<input checked="" type="checkbox"/>	/DCIM/111_06/IMG_0126.JPG	2255115	Accessed	Sat Feb 06 2016 00:00:00	r/rwxrwxrwx

- Possibility to import **Mactime** files [done]
- Pick only relevant files [done]
- MISPObject will be created [done]

DATA VISUALIZATION (MISP ZOIDBERG BRANCH)



- View: start-date only, spanning and search [dev-branch]
- Manipulate: Edit, Drag and Expand [dev-branch]
- Others: Timezone support [dev-branch]

→ For now [dev-branch], supports up to **micro-seconds** in the database and up to **milliseconds** in the web interface.

MISP RESTSEARCH API

AN EASY WAY TO QUERY, ADD AND UPDATE YOUR THREAT

CIRCL / TEAM MISP PROJECT



13TH ENISA-EC3 WORKSHOP

MISP API REWORKED

- The MISP API has grown gradually with a UI first design in many cases
- Endpoints all solved specific issues with their own rulesets
- Growth was organic - whenever the need to add a new functionality / filter popped up we've added it
- Lead to frankenmonsters such as this:

<http://localhost:5000/events/csv/download/false/false/tag1&&tag2&&tag3/Network%20activity/domain>

GOALS WE'VE SET FOR OURSELVES

- Open up every functionality in MISP available via the UI to the API
- Including ones related to **instance management**
- APIs that expect input objects for data creation should be **self-describing**
- **URL parameters should be discouraged**, but still usable by legacy tools (deprecation)
- APIs should be heavily **tested** (Raphael Vinot's exhaustive test suite in PyMISP)
- Largest focus on Export APIs

EXPORT API'S REIMAGINED

- Scrapped all existing type specific APIs (**deprecated**, documentation moved to legacy, still available)
- **Single entry point** - all export APIs baked into restSearch
- Queries consist of a combination of:
 - ▶ **Scope** (Event, Attribute, Sighting, more coming in the future)
 - ▶ **Filter parameters** - passed via JSON objects, url parameters (key value or ordered list)
 - ▶ **A return format**
- Everything that we could do before the rework we should be able to accomplish after the rework
- Under the hood now also used by the UI search and exports

EXPORT API'S REIMAGINED

- One of our largest issues solved: **pagination**
 - ▶ **Scope specific** pagination (number of events, attributes, etc)
 - ▶ Simply control it via the framework friendly **page / limit** parameters
 - ▶ Alternatively, use the improved **time based controls** (timestamp, publish_timestamp windows)

PERFORMANCE TUNING

- Single execution with subqueries
- Internal pagination **aligned with memory limits**
 - ▶ Probing of available memory for the current process
 - ▶ **Chunking of the query results** to fit in object specific memory envelopes
 - ▶ Constructing export set on disk in chunks has slashed memory usage considerably

DESIGNING TOOLS THAT USE THE APIs CAN BE COMPLEX, BUT THERE'S HELP

- The result of our own frustration
- Built in **ReST client** with templating
- Extensive query builder UI by Sami Mokaddem
- Build queries in a simple interface, automatically set URLs, headers, etc
- Uses the self documentation of APIs
- Export your queries as **cURL or Python scripts**
- Built in testing tools (performance measurements, result parsers)
- Store queries for reuse and download the results directly

WHY IS THE SEARCH API RECEIVING SO MUCH FOCUS?

- The **maturity** of the communities and threat intel sharing at large has improved
- We are sharing more
- Most importantly: we are sharing **more context** along with technical indicators
- This allows us to **manage our data more accurately** before feeding them to our protective tools
- Different contexts (APT targeting me? Persisting techniques?
- lifecycle management)
- Use several queries / boolean operators to select the slice of data most relevant for the task

CLI TOOLS FOR THE CLI GOD, AUTOMATION FOR THE AUTOMATION THRONE

- Open up commonly used system management tasks to the CLI
 - ▶ sync servers/feeds
 - ▶ caching feeds
 - ▶ Password resets
 - ▶ Server settings
 - ▶ Bruteforce protection resets
 - ▶ Enrichment
 - ▶ Worker management
- Goal was also to move away from the often malfunctioning scheduler and have cron friendly CLI scripts

SO WHAT DOES ALL OF THIS LOOK LIKE IN PRACTICE?

Demo time!

PLANS FOR THE FUTURE

- Add export modules to the restSearch API
- Improve the query language to support some missing features (such as AND boolean operators)
- Support for extended events via the restSearch API
 - ▶ We're missing a framing structure in the export module system (how are a list of conversions encapsulated and delimited?)
 - ▶ Proof of concept of the system implemented by Christian Studer already works using the STIX / STIX2 export subsystems
 - ▶ Would open us up to simple customisable search APIs
- Open up search APIs to other scopes (objects, users, organisations, proposals, feeds, galaxies, taxonomies)

BEST PRACTICES IN THREAT INTELLIGENCE

GATHER, DOCUMENT, ANALYSE AND CONTEXTUALISE IN-

CIRCL / TEAM MISP PROJECT

MISP PROJECT

<https://www.misp-project.org/>

13TH ENISA-EC3 WORKSHOP



MISP
Threat Sharing

OBJECTIVES

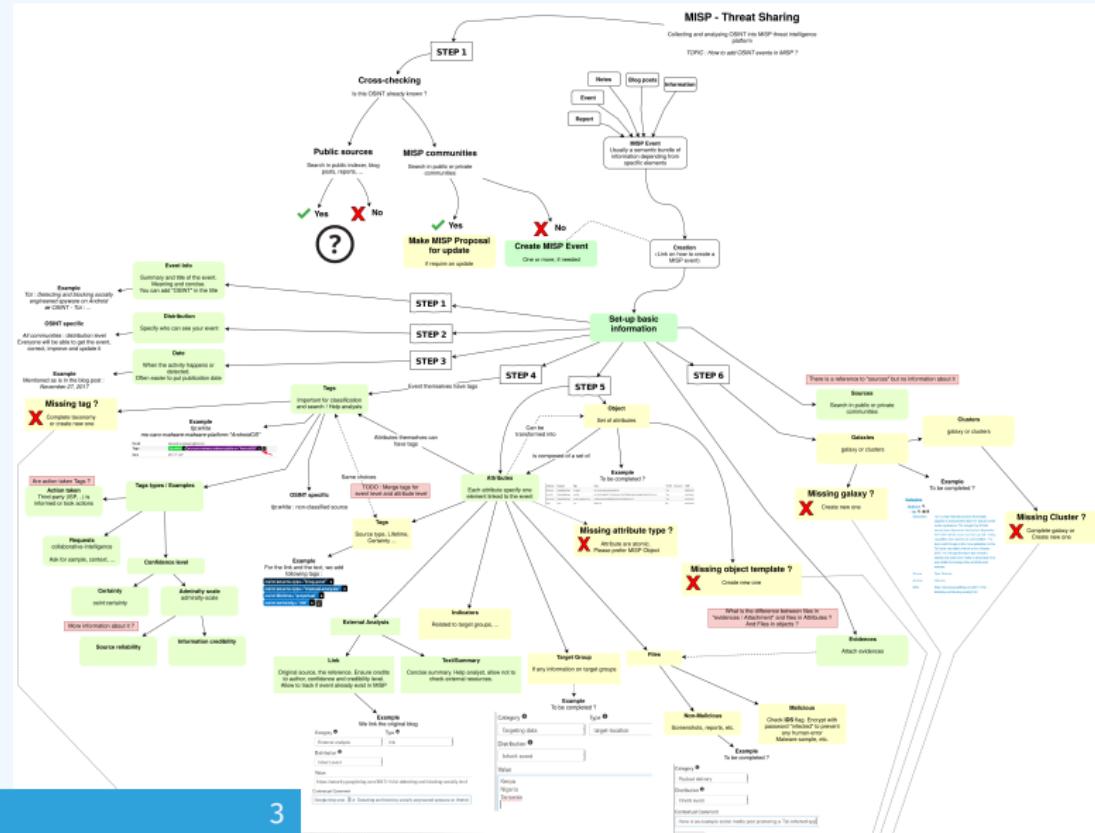
- Learn how to use MISP to support common OSINT gathering use-cases often used by SOC, CSIRTS and CERTs
 - ▶ Use practical exercise examples¹
 - ▶ The exercises are based on **practical recent cases to model and structure intelligence** using the MISP standard
- Improve the data models available in MISP by exchanging live improvements and ideas
- Be able to share the results to the community at the end of this session

¹<https://gist.github.com/adulau/8c1de48060e259799d3397b83b0eec4f>

(THREAT) INTELLIGENCE

- **Cyber threat intelligence (CTI) is a vast concept** which includes different concepts, methods, and workflows
 - ▶ Intelligence is defined differently in the military than in the financial sector than in the intelligence community
- **MISP project doesn't want to lock an organisation or a user into a specific model.** Each model is useful depending on the objectives of an organisation
- A set of pre-defined knowledge base or data-models are available and organisations can select (or create) what they need
- During this session, an overview of the most used taxonomies, galaxies, and objects will be described

OVERALL PROCESS OF COLLECTING AND ANALYSING OSINT



- Quality of indicators/attributes are important but **tagging and classification are also critical to ensure actionable information**
- Organizing intelligence is done in MISP by using tags, which often originate from MISP taxonomy libraries
- The scope can be classification (*tlp, PAP*), type (*osint, type, veris*), state (*workflow*), collaboration (*collaborative-intelligence*), or many other fields
- MISP taxonomy documentation is readily available²
- **Review existing practices of tagging in your sharing community, reuse practices, and improve context**

²<https://www.misp-project.org/taxonomies.html>

- When information cannot be expressed in triple tags format (*namespace:predicate=value*), MISP use Galaxies
- Galaxies contain a huge set of common libraries³ such as threat actors, malicious tools, tactics, target information, mitigations, and more
- When tagging or adding a Galaxy cluster, tagging at the event level is for the whole event (including attributes and objects). Tagging at the attribute level is for a more specific context

³<https://www.misp-project.org/galaxy.html>

ESTIMATIVE PROBABILITY

- Words of Estimative Probability⁴ propose clear wording while estimating probability of occurrence from an event
- A MISP taxonomy called estimative-language⁵ proposes an applied model to tag information in accordance with the concepts of Estimative Probability

⁴<https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/sherman-kent-and-the-board-of-national-estimates-collected-essayswords.html>

⁵<https://www.misp-project.org/taxonomies.html>

RELIABILITY, CREDIBILITY, AND CONFIDENCE

- The **Admiralty Scale**⁶ (also called the **NATO System**) is used to rank the reliability of a source and the credibility of information
- A MISP taxonomy called admiralty-scale⁷ is available
- US DoD **JP 2-0, Joint Intelligence**⁸ includes an appendix to express confidence in analytic judgments
- A MISP predicate in estimative-language called confidence-in-analytic-judgment⁹ is available

⁶<https://www.ijlter.org/index.php/ijlter/article/download/494/234>,
US Army Field Manual 2-22.3, 2006

⁷<https://www.misp-project.org/taxonomies.html>

⁸http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp2_0.pdf,
page 114

⁹<https://www.misp-project.org/taxonomies.html>

ADDING ATTRIBUTES/OBJECTS TO AN EVENT

- If the information is a **single atomic element**, using a single attribute is preferred
 - ▶ Choosing an attribute type is critical as this defines the automation/export rule (e.g. *url* versus *link* or ip-src/ip-dst?)
 - ▶ Enabling the IDS (automation) flag is also important, but *when you are in doubt, don't set the IDS flag*
- If the information is **composite** (ip/port, filename/hash, bank account/BIC), using an object is strongly recommended

HOW TO SELECT THE RIGHT OBJECT?

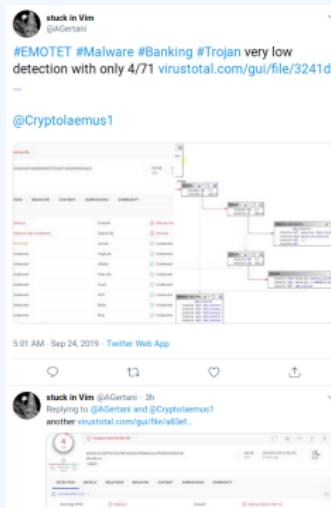
There are more than 150 MISP object¹⁰ templates.
As an example, at CIRCL, we regularly use the following object templates *file*, *microblog*, *domain-ip*, *ip-port*, *coin-address*, *virustotal-report*, *paste*, *person*, *ail-leak*, *pe*, *pe-section*, *registry-key*.

¹⁰<https://www.misp-project.org/objects.html>

MICROBLOG OBJECT

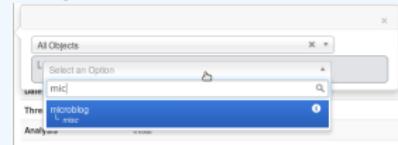
Use case

A series of OSINT tweets from a security researcher. To structure the thread, the information, and keep a history.



Object to use

The microblog object can be used for Tweets or any microblog post (e.g. Facebook). The object can be linked using *followed-by* to describe a series of post.



FILE OBJECT

Use case

- A file sample was received by email or extracted from VirusTotal
- A list of file hashes were included in a report
- A hash value was mentioned in a blog post

Object to use

The file object can be used to describe file. It's usual to have partial meta information such as a single hash and a filename.

Add File Object

Object Template	File v17
Description	File object describing a file with meta-information
Requirements	Required one of: filename, size-in-bytes, authenthash, ssdeep, md5, sha1, sha224, sha256, sha384, sha512, sha512/224, sha512/256, tlsh, pattern-in-file, x509-fingerprint-sha1, malware-sample, attachment, path, fullpath
Meta category	File
Distribution	Inherit event
Comment	

REFERENCES

- Graphical overview of OSINT collection using MISP <https://github.com/adulau/misp-osint-collection>
- MISP objects documentation
<https://www.misp-project.org/objects.html>
- MISP taxonomies documentation
<https://www.misp-project.org/taxonomies.html>
- MISP galaxy documentation
<https://www.misp-project.org/galaxy.html>

MISP CORE DEVELOPMENT HANDS-ON EXERCISE

BUILDING A SMALL NIFTY FEATURE FOR THE MISP CORE

CIRCL / TEAM MISP PROJECT



13TH ENISA-EC3 WORKSHOP



SOME PRACTICAL THINGS FIRST...

- If you'd like to take a peak at the main files already implemented:
<https://github.com/iglocska/misp-dev-training-cheat-sheet>
- Full implementation:
https://github.com/MISP/MISP/tree/dev_session/app

LET'S TRY TO DEVELOP A FEATURE TOGETHER

- Idea: Users should have the option to set alert filters for the publish alert e-mails
- By default receive all alerts as before
- If a filter is set, check if the alert is interesting for us or not

HOW TO ENSURE THAT THE FEATURE IS USEFUL FOR THE COMMUNITY AT LARGE?

- Always try to think in reusable systems instead of fixing a single issue
 - ▶ Much higher chance of getting a PR merged if it doesn't just cover your specific use-case
 - ▶ Try to stay two steps ahead, see how your feature can be reused for other tasks

USER SETTINGS - A LONG OVERDUE FEATURE

- Allow users to set preferences for certain views
- For high level users, all the technical details are sometimes wasted
- Simply not being interested in certain types of data points
- Non-standard MISP deployments (island only MISP instances, etc)
- User pre-sets for certain settings

OBJECTIVES OF THE FEATURE

- User should be able to do the following with filter rules:
 - ▶ set
 - ▶ get
 - ▶ remove
 - ▶ index
- Filter rules should be flexible - we do not want to anticipate all possible settings in advance
- Ensure that the system is easy to extend and reuse

BEFORE WE START WITH ANYTHING...

- Update our MISP instance (git pull origin 2.4)
- Fork github.com/MISP/MISP (via the github interface)
- Add a new remote to our fork:
 - ▶ via username/password auth: git remote add my_fork <https://github.com/iglocska/MISP>
 - ▶ via ssh: git remote add my_fork <gitgithub.com:iglocska/MISP.git>
- Generally a good idea to work on a new branch: git checkout -b dev_exercise
- Enable debug in MISP

- Storage:
 - ▶ Single key/value table for all settings
 - ▶ Each user should be able to set a single instance of a key
 - ▶ Values could possibly become complex, let's use JSON!
 - ▶ Add timestamping for traceability
 - ▶ Consider which fields we might want to look-up frequently for indexing

THE DATABASE CHANGES WE NEED

- The table structure:
 - ▶ id int(11) auto increment //primary key
 - ▶ key varchar(100) //add index!
 - ▶ value text //json
 - ▶ user_id int(11) //add index!
 - ▶ timestamp int(11) //add index!
- Tie it into the upgrade system (app/Model/AppModel.php)
- Test our upgrade process! Check the output in the audit logs

CHECKLIST

■ Outline of the changes needed:

- ▶ New Controller (UserSettingsController.php)
- ▶ New Model (UserSetting.php)
- ▶ New Views (setSetting, index)
- ▶ Add new controller actions to ACL
- ▶ Update the e-mail alert system to use the functionality

CREATE THE NEW MODEL SKELETON

- location: /var/www/MISP/app/Model/UserSetting.php
- Create basic skeleton
- Add model relationships (hasMany/BelongsTo)
- Use the hooking functionality to deal with the JSON field (beforeSave(), beforeFind())
- Add a function that can be used to check if a user should get an alert based on filters (checkPublishFilter())
- Add a function to check if a user can access/modify a setting (checkAccess())

CREATE THE CONTROLLER SKELETON

- location: /var/www/MISP/app/Model/UserSetting.php
- Create basic skeleton
- Set pagination rules
- Define CRUD functions (exceptionally, we diverge here from the norm)
 - ▶ setSetting()
 - ▶ getSetting()
 - ▶ index()
 - ▶ delete()

START WITH AN API ONLY APPROACH AT FIRST

■ setSetting():

- ▶ Accepted methods: ADD / POST
- ▶ Separate handling of API / UI
- ▶ POST should create/update an entry
- ▶ GET should describe the API

■ getSetting():

- ▶ Accepted methods: GET
- ▶ Retrieves a single setting based on either ID or setting key and user_id
- ▶ Encode the data depending on API/UI
- ▶ Accepted methods: GET
- ▶ List all settings
- ▶ Filter user scope on demand
- ▶ Filter available scopes based on role

■ delete():

- ▶ Accepted methods: POST / DELETE
- ▶ Deletes a single entry based on ID or setting key
- ▶ Encode the data depending on API/UI

ADD THE ACL FUNCTIONALITIES

- Tie functions into `checkAccess()`:
 - ▶ Check if user is allowed to execute actions and throw exceptions if not
 - ▶ Add it to: `setSetting()` / `getSetting()` / `delete()`
- Consider that:
 - ▶ Site admins have full reign
 - ▶ Org admins can manage their own users
 - ▶ Everyone else can self-manage

TEST THE FUNCTIONALITIES

- Use the REST client
- Expectations
 - ▶ GET on /setSetting and /delete describing our endpoints
 - ▶ POST /setSetting with "key": "publish_filter", "value": "Event.tags": "%sofacy%" should return newly added or modified filter
 - ▶ GET on /index should list our entries, GET on /getSetting should show an individual entry
 - ▶ DELETE on /delete should delete the entry

START ADDING THE UI COMPONENTS

- We now have a rudimentary CRUD, let's add some simple UI views
 - ▶ setSetting as a simple form
 - ▶ index should use the parametrised generators (IndexTable)
 - ▶ Add both views to the menu systems (side-menu, global menu)
 - ▶ Don't forget about sanitisation and translations!

ADD THE CHECKPUBLISHFILTER() FUNCTION TO THE E-MAILING

- Trace the code path of the e-mail sending to understand the process
- Decide on the best place to inject our check
- Don't break the flow of the process!
- What do we have access to at this point? What format are they in?

TEST IF OUR CODE WORKS CORRECTLY

- Do we see any notices / errors?
- Is our code easily accessible?
- Consider other roles! Can users/org admins do things we don't want them to do?
- Is our code-base breaking the default behaviour?
- Is our update script working as expected?

PUSH OUR CODE TO OUR FORK AND CREATE A PULL REQUEST

- git status to check what changed / got added
- git add /path/to/file to add files we want to commit
- git commit (format: is "new/fix/chg: [topic] My description")
- git push my_fork
- Create pull request from the github interface
- Wait for Travis to run, update the code if needed

MISP RESTSEARCH MODULE DEVELOPMENT

BUILDING A SIMPLE EXPORT MODULE FOR THE CORE

CIRCL / TEAM MISP PROJECT



13TH ENISA-EC3 WORKSHOP



BUILDING A NATIVE RESTSEARCH EXPORT

- Similar in scope to an **export module** of the MISP modules system
- Pros:
 - ▶ Can be used for composited data coming from a **filtered query**
 - ▶ Fast, **native approach**
 - ▶ Can be built to support **several scopes** (events, attributes, sightings)
- Cons...

BUILDING A NATIVE RESTSEARCH EXPORT

- Similar in scope to an **export module** of the MISP modules system
- Pros:
 - ▶ Can be used for composited data coming from a **filtered query**
 - ▶ Fast, **native approach**
 - ▶ Can be built to support **several scopes** (events, attributes, sightings)
- Cons...



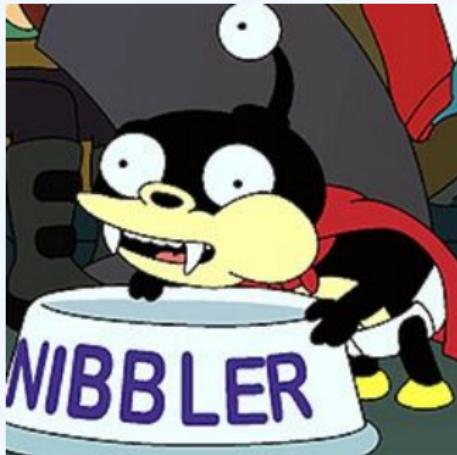
SO HOW DOES RESTSEARCH WORK?

- Standardised way of collecting **parameters**
- Using the parameters, a loop is started to **chunk and gradually build** our export data
- The chunk size depends on memory envelopes
- Each chunk is **converted piece by piece...**
- ... and subsequently are concatenated into a temporary file
- Once no more elements are left, the file is sent in the response

WHERE DOES THE MODULE SYSTEM COME INTO PLAY?

- The export modules handle 5 tasks:
 - ▶ Pass **meta-information** back to restSearch on the export format itself
 - ▶ Add a **start segment** to the exported data
 - ▶ Do the actual **conversion** from MISP's internal format to the desired export format
 - ▶ Provide a **separator** for data chunks
 - ▶ Have a **closing segment** for the returned data, based on the format's conventions

OUR LITTLE TRAINING MODULE: NIBBLER, THE EVER HUNGRY IDS/IPS



- Simplistic tool with its **own proprietary format**
- Meant to mimic a typical **in-house tool**
- Lightweight scope, for simplicity's sake
- **pipe separated values**
- **VALUE | TYPE | DESCRIPTION | REFERENCE | ACTION**

NIBBLER FORMAT - CAVEATS

- Rules can be prepended by comments, each comment line starting with #
- Some characters have to be escaped in some custom, crazy ways
 - ▶ linebreaks: ##LINEBREAK##
 - ▶ commas: ##COMMA##
 - ▶ pipes: ##PIPE##

- **Value:** The actual indicator value
- **Type:** The format of the indicator
- **Description:** A quick description for analysts investigating the alert, why is this relevant
- **Reference:** A backreference that the analyst can use to find out more about the alert
- **Action:** What should Nibbler do if it trips over the value?

SUPPORTED TYPES

- IP
- Domain
- Hostname
- MD5
- SHA1
- SHA256
- Filename

SUPPORTED VALUES

- ALERT - default behaviour, create an alert.
- BLOCK - block the action outright. Only set if the tag nibbler:block is present

MAPPING THE TYPES TO MISP

- Though we have types to map from MISP, in some cases several types map to a Nibbler type
- We've created a rough **mapping** (this is probably the most difficult task) in advance
- Some MISP types map to a Nibbler type directly
- **Composite** MISP types map to **2 Nibbler types** each

MAPPING THE TYPES TO MISP

- ip-dst :: IP
- ip-src :: IP
- domain :: Domain
- domain|ip :: Domain, IP
- hostname :: Hostname
- md5 :: MD5
- sha1 :: SHA1
- sha256 :: SHA256
- filename|md5 :: Filename, MD5
- malware-sample :: Filename, MD5
- filename|sha1 :: Filename, SHA1
- filename|sha256 :: Filename, SHA256

EXPORT MODULE SKELETON

```
<?php
class NibblerExport
{
    public $additional_params = array();
    public function handler(
        $data, $options = array()
    ) {}
    public function header(
        $options = array()
    ) {}
    public function footer() {}
    public function separator() {}
}
```

ADDITIONAL PARAMETERS

```
public $additional_params = array(  
    'flatten' => 1  
);
```

ADDING OUR MAPPING

```
private $__mapping = array(  
    'ip-dst' => 'IP',  
    'ip-src' => 'IP',  
    'domain' => 'Domain',  
    'domain|ip' => ['Domain', 'IP'],  
    'hostname' => 'Hostname',  
    'md5' => 'MD5',  
    'sha1' => 'SHA1',  
    'sha256' => 'SHA256',  
    'filename|md5' => array('Filename', 'MD5'),  
    'malware-sample' => array('Filename', 'MD5'),  
    'filename|sha1' => array('Filename', 'SHA1'),  
    'filename|sha256' => array('Filename', 'SHA256'));
```

WRITING THE START OF THE OUTPUT

```
public function header($options = array())
{
    return sprintf(
        "# Nibbler rules generated by MISP at %s\n",
        date('Y-m-d H:i:s')
    );
}
```

FOOTER FUNCTION - HOW SHOULD THE OUTPUT END?

```
public function footer()
{
    return "\n";
}
```

WHAT SEPARATES THE CHUNKS?

```
public function separator()
{
    return "\n";
}
```

THE ACTUAL LEGWORK, THE HANDLER

```
public function handler($data, $options = array())
{
    if ($options['scope'] === 'Attribute') {
        $data['Attribute']['AttributeTag'] = $data['AttributeTag'];
        return $this->_convertAttribute($data['Attribute'], $data['Event']);
    }
    if ($options['scope'] === 'Event') {
        $result = array();
        foreach ($data['Attribute'] as $attribute) {
            $temp = $this->_convertAttribute($attribute, $data['Event']);
            if ($temp) $result[] = $temp;
        }
        return implode($this->separator(), $result);
    }
    return '';
}
```

BUILDING AN OPTIONAL INTERNAL CONVERTER FUNCTION

```
private function __convertAttribute($attribute, $eve
{
    if (empty($this->__mapping[$attribute['type']])) {
        // mapping not found - invalid type for nibbler
        return '';
    }
    if (is_array($this->__mapping[$attribute['type']]))
        // handle mappings for composites - slide
    } else {
        // handle simple mappings - slide
    }
    // return 1 or 2 lines, separated by separator()
    return implode($this->separator(), $result);
}
```

HANDLING THE SIMPLE CASE

```
$result[] = sprintf(  
    '%s|%s|%s|%s|%s' ,  
    $this->__escapeSpecialChars($attribute['value']) ,  
    $this->__mapping[$attribute['type']] ,  
    $event['uuid'] ,  
    $this->__escapeSpecialChars($event['info']) ,  
    'ALERT'  
);
```

HANDLING THE CASE FOR COMPOSITES

```
$attribute['value'] = explode(
    '|', $attribute['value']
);
foreach (array(0,1) as $part) {
    $result[] = sprintf(
        '%s|%s|%s|%s|%s',
        $this->__escapeSpecialChars(
            $attribute['value'][$part]
        ),
        $this->__mapping[$attribute['type']][$part],
        $event['uuid'],
        $this->__escapeSpecialChars($event['info']),
        'ALERT'
    );
}
```

PUTTING IT TOGETHER

```
private function __convertAttribute($attribute, $event) {
    if (empty($this->__mapping[$attribute['type']])) return '';
    $result = array();
    $attributes = array();
    if (is_array($this->__mapping[$attribute['type']])) {
        $attribute['value'] = explode(' ', $attribute['value']);
        foreach (array(0,1) as $part) {
            $result[] = sprintf(
                '%s|%s|%s|%s',
                $this->__escapeSpecialChars($attribute['value'][$part]),
                $this->__mapping[$attribute['type']][$part],
                '/events/view/ . ' . $event['uuid'],
                $this->__escapeSpecialChars($event['info']),
                $this->__decideOnAction($attribute['AttributeTag'])
            );
        }
    } else {
        $result[] = sprintf(
            '%s|%s|%s|%s',
            $this->__escapeSpecialChars($attribute['value']),
            $this->__mapping[$attribute['type']],
            '/events/view/ . ' . $event['uuid'],
            $this->__escapeSpecialChars($event['info']),
            $this->__decideOnAction($attribute['AttributeTag'])
        );
    }
    return implode($this->separator(), $result);
}
```

ADDING THE FUNCTION THAT DECIDES ON THE ACTION

```
private function __decideOnAction($attributeTags)
{
    foreach($attributeTags as $attributeTag) {
        if (
            $attributeTag['Tag'][ 'name' ] ===
            'nibbler:block'
        ) {
            return 'BLOCK';
        }
    }
    return 'ALERT';
}
```

FINALISING THE EXPORT MODULE... THE ESCAPING FUNCTION

```
private function __escapeSpecialChars($value)
{
    $value = preg_replace(
        "/\r|\n/", "##LINEBREAK##", $value
    );
    $value = preg_replace(
        "/ , /", "##COMMA##", $value
    );
    $value = preg_replace(
        "/ \| /", "##PIPE##", $value
    );
    return $value;
}
```

MODIFYING THE MISP CORE TO KNOW ABOUT THE EXPORT MODULE

- The **models** that we are targeting by scope (Event, Attribute) **need to be updated**
- They are located in **/var/www/MISP/app/Model/**
- The global variable **\$validFormats** houses all mappings
- Simply add a new line such as the following:
- 'nibbler' => array('nibbler', 'NibblerExport', 'nibbler')

LET US TEST THE MODULE!

- Use the **rest client** to test it conveniently
- Both the event and attribute level restSearch function should work
- Simply set the **returnFormat** to nibbler, which should also show up as a valid export format

REST CLIENT

HTTP method to use

POST

Relative path to query

/events/restSearch

Use full path - disclose my apikey Bookmark query
 Show result Skip SSL validation

HTTP headers

```
Authorization: ArSxnHf20foSapnOSyxfrljMdl9oLDnvvmqvHK97q
Accept: application/json
Content-Type: application/json
```

HTTP body

```
{
  "returnFormat": "nibbler",
  "page": 1,
  "limit": 4,
  "type": ["ip-dst", "ip-src", "domain|ip", "hostname", "domain"]
}
```

Run query

MISP - GALAXY 2.0

METHOD FOR SHARING THREAT INTELLIGENCE

TEAM CIRCL

INFO@CIRCL.LU

SEPTEMBER 11, 2024



MISP
Threat Sharing

OUTLINE OF THE PRESENTATION

- Present the features available for Sharing *galaxy clusters*
- Look at the internals of what changed in the datamodel and MISP's behaviors

Galaxy 2.0 introduces various new features for *Galaxies* and their *Clusters* allowing:

- Creation of **custom Clusters**
- **ACL** on *Clusters*
- **Connection** of *Clusters* via *Relations*
- **Synchronization** to connected instances.
- **Visualization** of forks and relationships

DEFAULT GALAXY CLUSTERS

Default Galaxy cluster

- Coming from the misp-galaxy repository¹
- Cannot be edited
 - ▶ Only way to provide modification is to modify the stored JSON or to open a pull request
 - ▶ Are not synchronized
 - ▶ Source of trust
- Restrictions propagate to their children (Galaxy cluster elements, Cluster relationships)

Custom Galaxy cluster

- Can be created via the UI or API
- Belongs to an organisation
 - ▶ Fully editable
 - ▶ Are synchronized

¹<https://github.com/MISP/misp-galaxy>

MISP GALAXY 2.0 - COMPARISON WITH PRIOR VERSION

Clusters and Relations can be edited.

- New *Clusters* fields

- ▶ distribution, sharing_group_id
- ▶ org_id, orgc_id
- ▶ locked, published, deleted
- ▶ default
 - Clusters coming from the misp-galaxies repository are marked as default
 - Not synchronized
 - Same purpose as *Event's* locked field
- ▶ extends_uuid
 - Point to the *Cluster* that has been forked
- ▶ extends_version
 - Keep track of the *Cluster* version that has been forked

MISP GALAXY 2.0 - OTHERS CHANGES

- *Role perm_galaxy_editor*
- Relations also have a distribution and can have *Tags*
- Synchronization servers have 2 new flags
 - ▶ pull_galaxy_clusters
 - ▶ push_galaxy_clusters
- Clusters blocklist

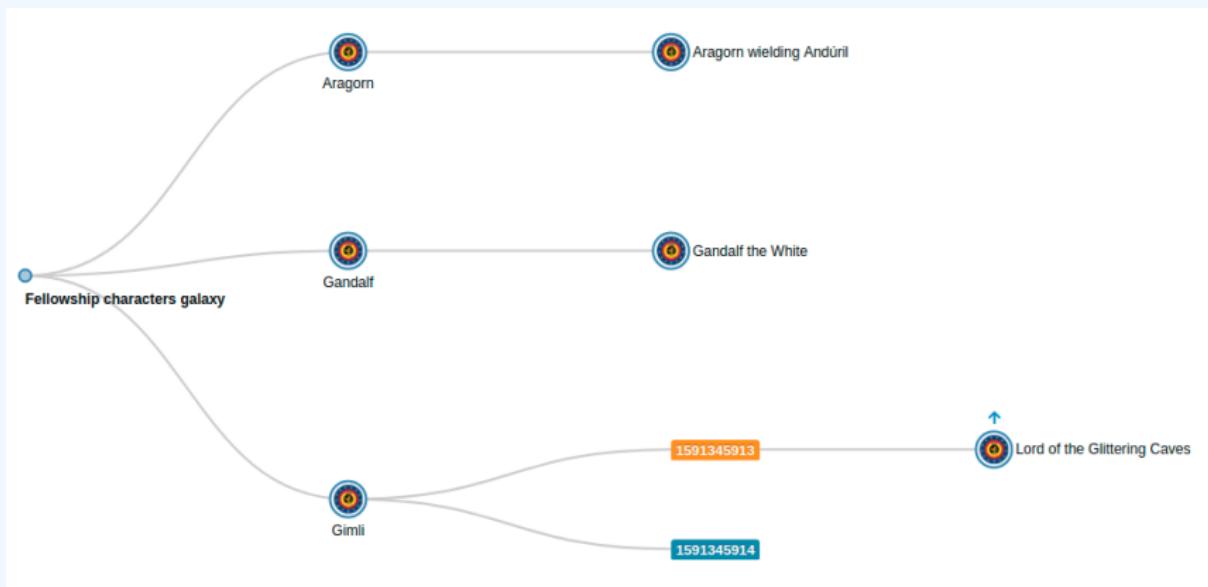
FEATURES IN DEPTH: CRUD

- Standard CRUD
- Soft and Hard deletion
- Publishing
- Update forked cluster to keep it synchronized with its parent
- ACL on the *Cluster* itself, not on its tag
 - ▶ `misp-galaxy:galaxy-type="cluster UUID"`
 - ▶ `misp-galaxy:mitre-attack-pattern="e4932f21-4867-4de6-849a-1b11e48e2682"`

FEATURES IN DEPTH: VISUALIZATION

Tree view of forked Clusters

Advertising
└ Online Advertising
└ Postal Advertising



FEATURES IN DEPTH: VISUALIZATION

Tree and network views for Relations between Clusters

Microsoft Activity Group actor galaxy cluster relationships



FEATURES IN DEPTH: VISUALIZATION

Tree and network views for Relations between Clusters

Source UUID: 8ed81090-f098-4878-b87e-2d801 | Relationship type: dropped | Target UUID: | Distribution: All communities

Tags: Picker | + Add relationship

```
graph LR; R1((Ramnit banker)) --- S1[similar  
estimative-language:likelihood-probability="likely"] --- R2((Ramnit botnet)); R2 --- S2[similar  
estimative-language:likelihood-probability="likely"] --- R3((Ramnit malpedia)); R3 -- "similar  
estimative-language:likelihood-probability="likely"" --> R3
```

GALAXY CLUSTER ELEMENTS

Hasn't been touched: Still a key-value stored. But new feature have been added²

Tabular view

- Allows you to browse **cluster elements** like before

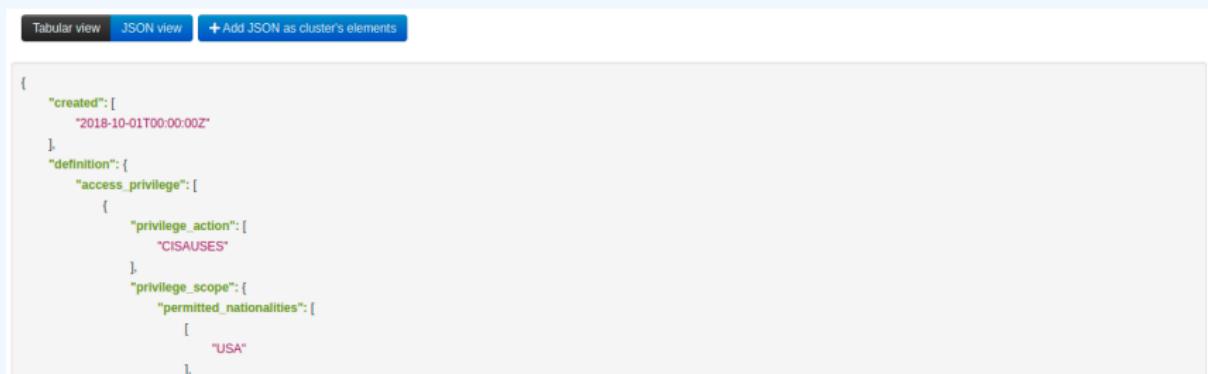
		« previous	1	2	3	next »	last »
		Tabular view	JSON view				
Key ↓		Value			Actions		
created		2018-10-01T00:00:00Z					
definition.access_privilege.0.privilege_action		CISAUSES					
definition.access_privilege.0.privilege_scope.permitted_nationalities.0		USA					
definition.access_privilege.0.privilege_scope.permitted_nationalities.1		AUS					
definition.access_privilege.0.privilege_scope.permitted_nationalities.2		CAN					
definition.access_privilege.0.privilege_scope.permitted_nationalities.3		GBR					
definition.access_privilege.0.privilege_scope.permitted_nationalities.4		NZL					

²Will be included in next release

GALAXY CLUSTER ELEMENTS

JSON view

- Allows you to visualisation **cluster element** in a JSON structure
- Allows you to convert any JSON into **cluster elements** enabling searches and correlations



The screenshot shows a web-based application for managing cluster elements. At the top, there are three tabs: 'Tabular view' (disabled), 'JSON view' (selected, indicated by a blue background), and '+ Add JSON as cluster's elements'. The main content area displays a JSON object representing a cluster element. The JSON structure is as follows:

```
{  
    "created": [  
        "2018-10-01T00:00:00Z"  
    ],  
    "definition": {  
        "access_privilege": [  
            {  
                "privilege_action": [  
                    "CISAUSES"  
                ]  
            },  
            "privilege_scope": {  
                "permitted_nationalities": [  
                    [  
                        "USA"  
                    ]  
                ]  
            }  
        ]  
    }  
}
```

SYNCHRONIZATION IN DEPTH

Has its own synchronization mechanism which can be enabled with the `pull_galaxy_cluster` and `push_galaxy_cluster` flags

- **Pull All:** Pull all remote Clusters (similar to event's pull all)
- **Pull Update:** Update local Clusters (similar to event's pull update)
- **Pull Relevant:** Pull missing Clusters based on local Tags
- **Push:** Triggered whenever a Cluster is published or via standard push

AN INTRODUCTION TO CYBERSECURITY INFORMATION SHARING

MISP - THREAT SHARING

CIRCL / TEAM MISP PROJECT

MISP PROJECT

<https://www.misp-project.org/>

13TH ENISA-EC3 WORKSHOP



MISP
Threat Sharing

CONTENT OF THE PRESENTATION

- Data sharing in MISP
- Data models for the Data layer
- Data models for the Context layer

LAYERS OF DATA MODEL

■ Data layer

- ▶ The raw data itself as well as element to link them together
- ▶ Indicators, Observables and means to contextually link them
- ▶ MISP terminology: Event, Attributes, misp-objects, ...

■ Context layer

- ▶ As important as the data layer, allow triage, false-positive management, risk-assessment and prioritisation
- ▶ Latches on the data layer, usually referencing threat intelligence, concepts, knowledge base and vocabularies
- ▶ Tags, Taxonomies, Galaxies, ...

DATA SHARING IN MISP

SHARING IN MISP: DISTRIBUTION

MISP offers granular distribution settings:

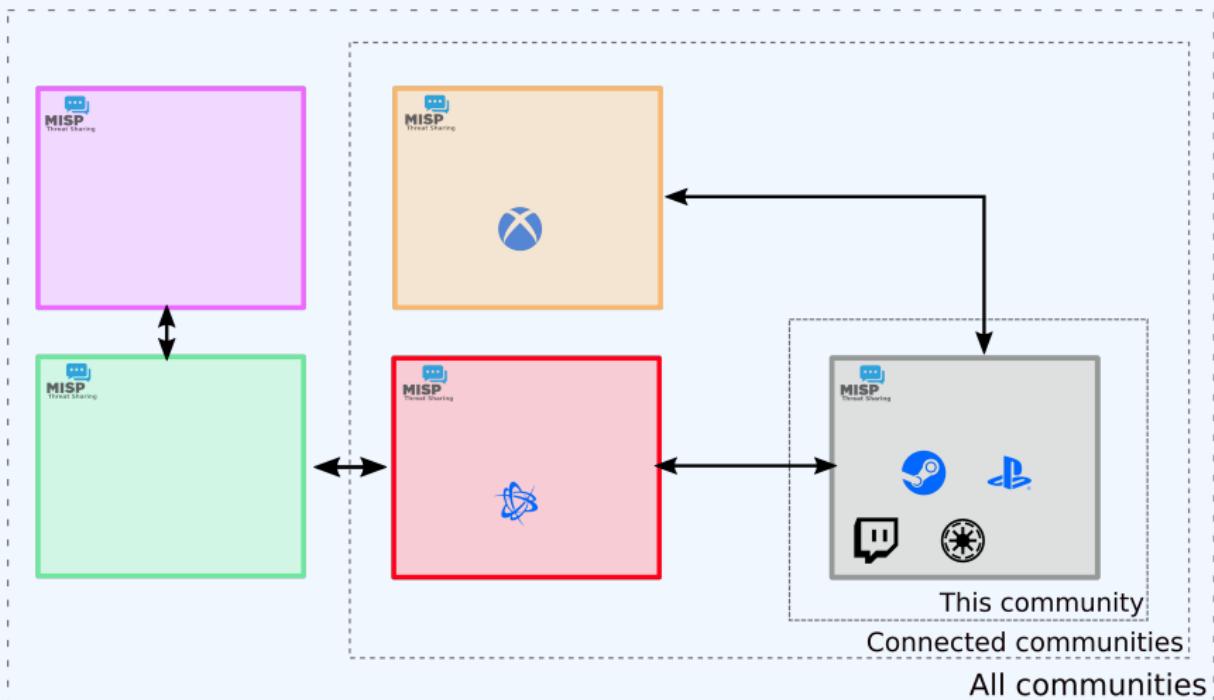
- Organisation only
- This community
- Connected communities
- All communities
- Distribution lists - aka **Sharing groups**

Sharing Group								
Id		11						
Uuid		5a4bf73c-05dc-4586-840f-5848a5e038e14						
Name		Banking sector in Europe						
Releasability		Banks located in Europe						
Description		Everything banking						
Selectable		<input checked="" type="checkbox"/>						
Created by		Training						
Organisations								
Name		Local	Extend	Instances	All orgs			
Training		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<td><td>Local Instance</td><td>https://iglooska.eu</td><td><input checked="" type="checkbox"/></td></td>	<td>Local Instance</td> <td>https://iglooska.eu</td> <td><input checked="" type="checkbox"/></td>	Local Instance	https://iglooska.eu	<input checked="" type="checkbox"/>
A-FUNKY-HUNGARIAN-BANK.hu		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<td><td>https://iglooska.eu</td><td><input checked="" type="checkbox"/></td></td>	<td>https://iglooska.eu</td> <td><input checked="" type="checkbox"/></td>	https://iglooska.eu	<input checked="" type="checkbox"/>	
AFB		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<td></td> <td></td>				
Italian Bank		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<td></td> <td></td>				
NCSC-NL		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<td></td> <td></td>				

At multiple levels: **Events, Attributes, Objects** (and their **Attributes**) and **Galaxy-clusters**

SHARING IN MISP: DISTRIBUTION

Sharing group



DATA LAYER

DATA LAYER: NAMING CONVENTIONS

- Data layer
 - ▶ **Events** are encapsulations for contextually linked information
 - ▶ **Attributes** are individual data points, which can be indicators or supporting data.
 - ▶ **Objects** are custom templated Attribute compositions
 - ▶ **Object references** are the relationships between individual building blocks
 - ▶ **Shadow Attributes/Proposal** are suggestions made by users to modify an existing *attribute*
 - ▶ **Sightings** are a means to convey that a data point has been seen
 - ▶ **Event reports** are supporting materials for analysts to describe *events, processes, etc*

DATA LAYER: EVENTS

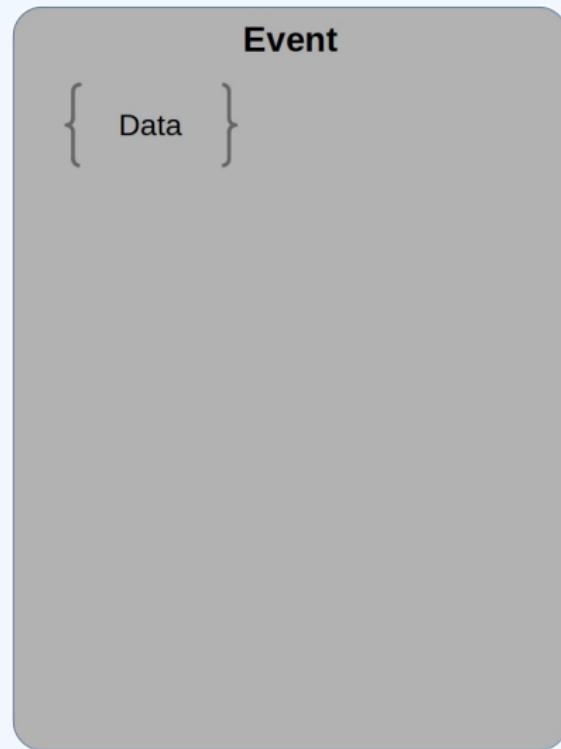
Events are encapsulations for contextually linked information

Purpose: Group datapoints and context together. Acting as an envelop, it allows setting distribution and sharing rules for itself and its children.

Usecase: Encode incidents / events / reports / ...

IoT malware - Gafgyt.Gen28 (active) - 20190220 - 20190222	
Event ID	178
UUID	5c6d21e5-bb60-47b7-b892-42e6950d2111
Creator org	CIRCL
Owner org	Training
Creator user	andras.iklody@circl.lu
Tags	ip:white x osint:source-type="automatic-collection" x circl:incident-classification="malware" x adversary:infrastructure-action="take-down" x + +
Date	2019-02-20
Threat Level	Low
Analysis	Completed
Distribution	All communities + <
Info	IoT malware - Gafgyt.Gen28 (active) - 20190220 - 20190222
Published	Yes (2020-11-28 07:53:39)
#Attributes	2601 (296 Objects)
First recorded change	2019-02-20 09:46:24
Last change	2020-10-10 07:36:28
Modification map	+
Sightings	0 (0) - restricted to own organisation only. ↗

DATA LAYER: EVENT BUILDING BLOCKS - BASE



DATA LAYER: EVENTS

```
1  {
2      "date": "2019-02-20",
3      "info": "IoT malware - Gafgyt.Gen28 (active)",
4      "uuid": "5c6d21e5-bb60-47b7-b892-42e6950d2111",
5      "analysis": "2",
6      "timestamp": "1602315388",
7      "distribution": "3",
8      "sharing_group_id": "0",
9      "threat_level_id": "3",
10     "extends_uuid": "",
11     "Attribute": [...],
12     "Object": [...],
13     "EventReport": [...],
14     "Tag": [...],
15     "Galaxy": [...]
16 }
```

DATA LAYER: ATTRIBUTES

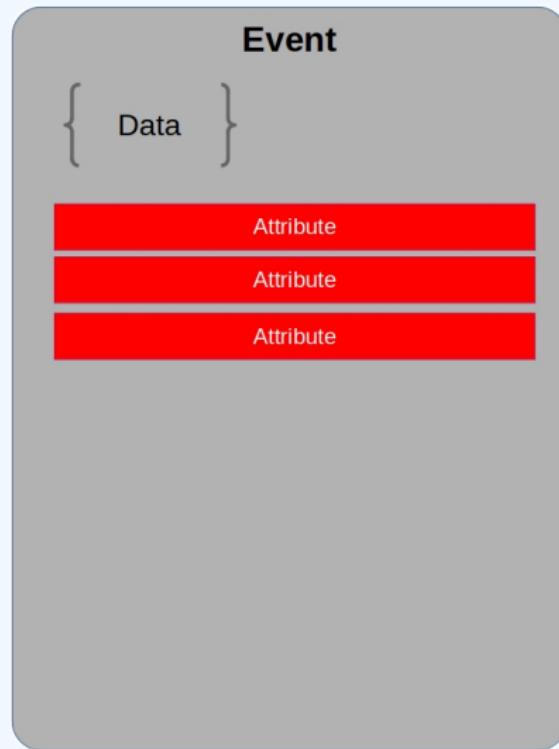
Attributes are individual data points, indicators or supporting data

Purpose: Individual data point. Can be an indicator or supporting data.

Usecase: Domain, IP, link, sha1, attachment, ...

		Filter		Filters: All File Network Financial Proposal Correlation							
Date	Org	Category	Type	Value	Comment	Related Events	ID S	Distribution	Actions		
2016-02-23		Network activity	domain	microsoft.com			No	Inherit	<input checked="" type="checkbox"/> <input type="checkbox"/>		
2016-02-23		Network activity	domain	google.com		25	No	Inherit	<input checked="" type="checkbox"/> <input type="checkbox"/>		
2016-02-23		Network activity	domain	circ.lu			No	Inherit	<input checked="" type="checkbox"/> <input type="checkbox"/>		
2016-02-23		Network activity	ip-src	23.100.122.175	Derived from microsoft.com via the dns enrichment module.		No	Inherit	<input type="checkbox"/> <input checked="" type="checkbox"/>		

DATA LAYER: EVENT BUILDING BLOCKS - RAW DATA



DATA LAYER: ATTRIBUTES

```
1 {  
2     "type": "url",  
3     "category": "Network activity",  
4     "to_ids": true,  
5     "uuid": "5c6d24bd-d094-4dd6-a1b6-4fa3950d2111",  
6     "event_id": "178",  
7     "distribution": "5",  
8     "sharing_group_id": "0",  
9     "timestamp": "1550656701",  
10    "comment": "Delivery point for the malware",  
11    "object_id": "0",  
12    "object_relation": null,  
13    "first_seen": null,  
14    "last_seen": null,  
15    "value": "ftp://185.135.80.163/",  
16    "Tag": [...]  
17    "Galaxy": [...]  
18 }
```

DATA LAYER: MISP OBJECTS

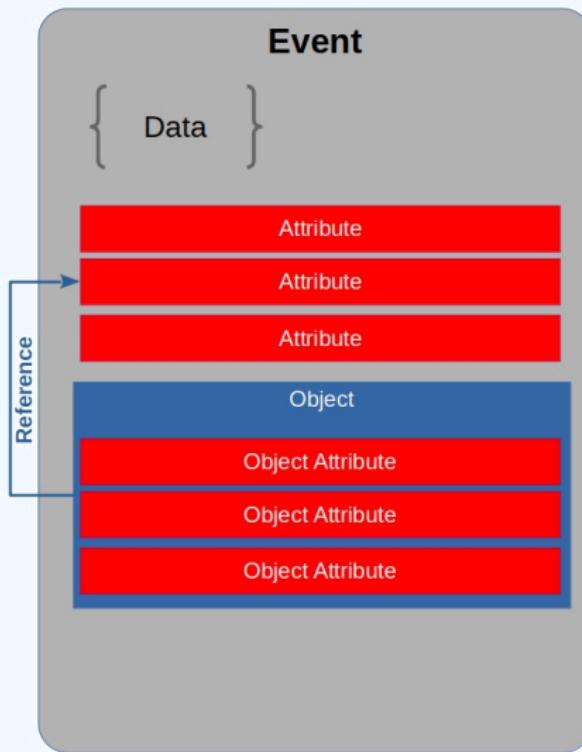
Objects are custom templated Attribute compositions

Purpose: Groups Attributes that are intrinsically linked together

Use case: File, person, credit-card, x509, device, ...

■ 2018-03-27	Name: file ↗		
	References: 1 ↗ +		
■ 2018-03-27	Payload delivery	filename: filename	+ ↗
■ 2018-03-27	Other	size-in-bytes: size-in-bytes	+ ↗
■ 2018-03-27	Other	entropy: float	+ ↗
■ 2018-03-27	Payload delivery	md5: md5	+ ↗
■ 2018-03-27	Payload delivery	sha1: sha1	+ ↗
■ 2018-03-27	Payload delivery	sha256: sha256	+ ↗
■ 2018-03-27	Payload delivery	sha512: sha512	+ ↗
■ 2018-03-27	Payload delivery	malware-sample: putty.exe	+ ↗

DATA LAYER: EVENT BUILDING BLOCKS - DATA COMPOSITION



DATA LAYER: MISP OBJECTS

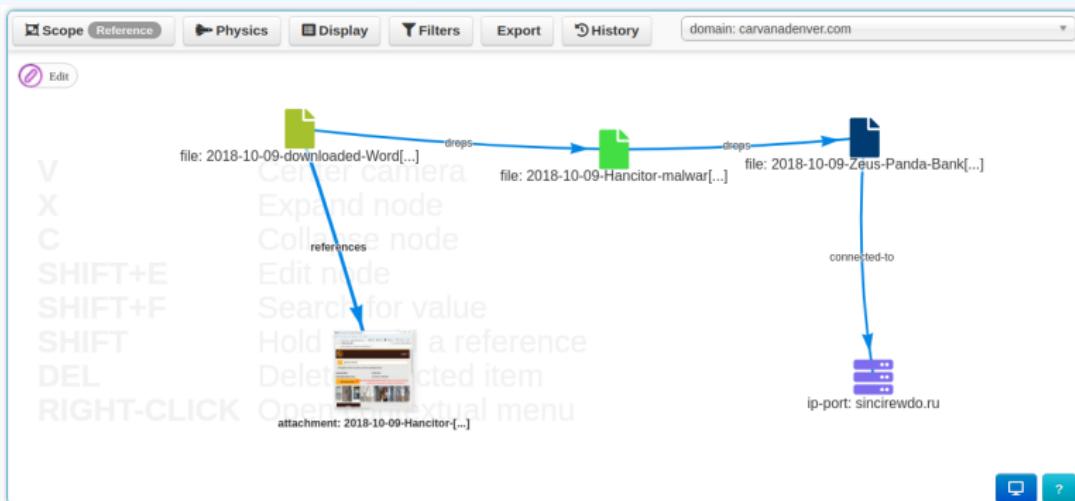
```
1  {
2      "name": "elf-section",
3      "meta-category": "file",
4      "description": "Object describing a sect...",
5      "template_uuid": "ca271f32-1234-4e87-b240-6b6e882de5de",
6      "template_version": "4",
7      "uuid": "ab5foc85-5623-424c-bc03-d79841700d74",
8      "timestamp": "1550655984",
9      "distribution": "5",
10     "sharing_group_id": "0",
11     "comment": "",
12     "first_seen": null,
13     "last_seen": null,
14     "ObjectReference": [],
15     "Attribute": [...]
16 }
```

DATA LAYER: OBJECT REFERENCES

Object references are the relationships between individual building blocks

Purpose: Allows to create relationships between entities, thus creating a graph where they are the edges and entities are the nodes.

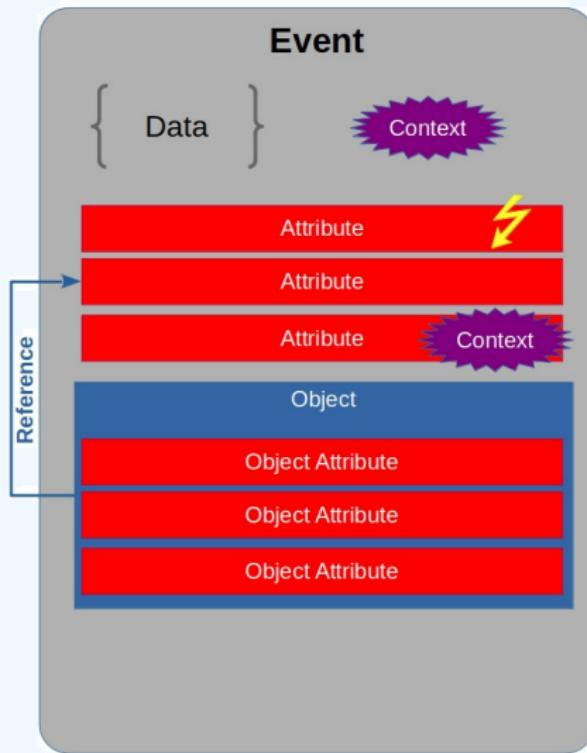
Usecase: Represent behaviours, similarities, affiliation, ...



DATA LAYER: OBJECT REFERENCES

```
1  {
2      "uuid": "5c6d21f9-0384-4bd2-b256-40de950d2111",
3      "timestamp": "1602318569",
4      "object_id": "1024",
5      "source_uuid": "23275e05-c202-460e-aadf-819c417fb326",
6      "referenced_uuid": "ab5foc85-5623-424c-bc03-d79841700d74",
7      "referenced_type": "1",
8      "relationship_type": "included-in",
9      "comment": "Section 0 of ELF"
10 }
```

DATA LAYER: EVENT BUILDING BLOCKS - CONTEXT



DATA LAYER: SIGHTINGS

Sightings are a means to convey that a data point has been seen

Purpose: Allows to add temporality to the data.

Usecase: Record activity or occurrence, perform IoC expiration, ...

The screenshot shows a user interface for managing sightings. At the top, there's a header 'Events' with a dropdown menu. Below it is a table with three rows, each representing a sighting. The first row is highlighted with a red background and has a tooltip 'Sightings CIRCL: 2 (2017-03-19 16:17:59)' pointing to it. The second row has a tooltip '(2/0/0)' and the third row has a tooltip '(0/0/0)'. Each row contains a checkbox, a status indicator ('No'), and an 'Inherit' button. At the bottom of the interface is a horizontal timeline with a red dot indicating a specific point in time.

```
1 {  
2   "org_id": "1",  
3   "date_sighting": "1573722432",  
4   "uuid": "5dcfd1940-5de8-4462-93dd-12a2a5e38e14",  
5   "source": "",  
6   "type": "O",  
7   "attribute_uuid": "5da97b59-9650-4be2-9443-2194a5e38e14"  
8 }
```

DATA LAYER: EVENT REPORTS

Event reports are supporting data for analysis to describe events, processes, etc

Purpose: Supporting data point to describe events or processes

Usecase: Encode reports, provide more information about the Event, ...

The screenshot shows a web-based event report interface. At the top, it says "Event report: Winnti Group targeting universities in Hong Kong". Below that are three buttons: "Markdown", "Raw", and "Edit report". A note below the buttons states: "This report is an excerpt meant for demo purposes. The full report can be found online at [link: https://www.weilivesecurity.com/2...]".

Winnti Group targeting universities in Hong Kong

In November 2019, we discovered a new campaign run by the Winnti Group [A threat actor is listed] against two Hong Kong universities. We found a new variant of the ShadowPad backdoor [malpedia is 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 `hpghostv.dll`, which is the name of a legitimate DLL loaded by `filename: %WINDIR%\temp\hpghostv.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\hpghostv.exe`, was dropped by the attackers, along with their malicious `filename: %WINDIR%\temp\hpghostv.dll`, in `C:\Windows\Temp`.

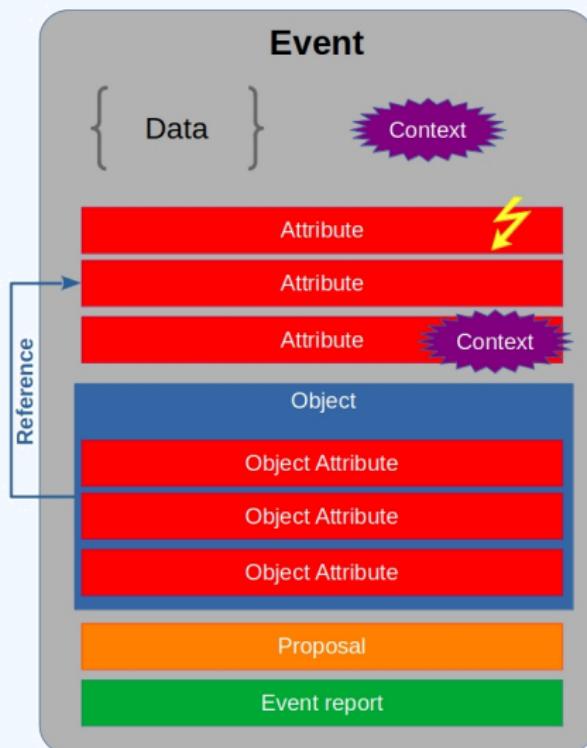
When the malicious DLL is loaded at `hpghostv.exe` stamp, its `DllMain` function is called that will check its parent process for the following sequence of bytes at offset `0x16BA`:

```
85 C0 ; test eax, eax  
8F 64 ; j2
```

In the case where the parent process is `filename: %WINDIR%\temp\hpghostv.exe`, this sequence of bytes is present at this exact location and the malicious DLL will proceed to patch the parent process in memory.

Cancel

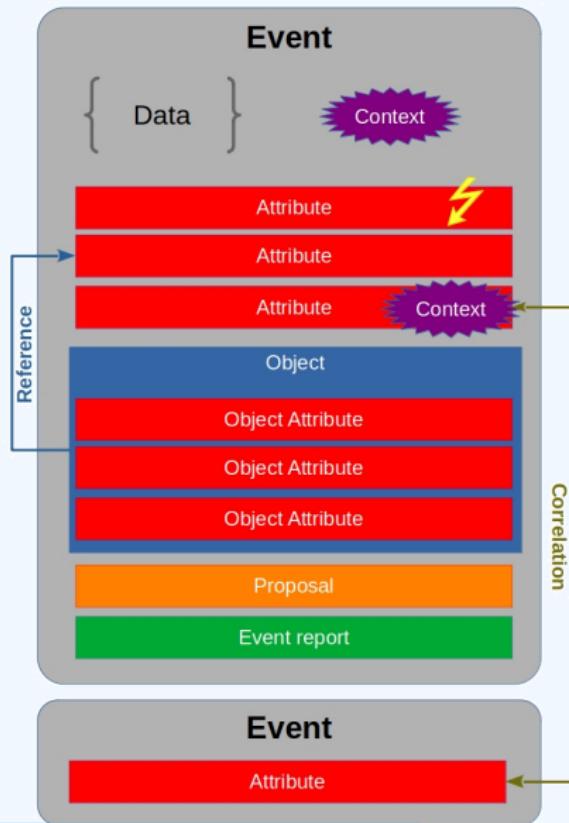
DATA LAYER: EVENT BUILDING BLOCKS - COLLABORATION & INTELLIGENCE



DATA LAYER: EVENT REPORTS

```
1 {
2     "uuid": "076e240b-5a76-4a8b-9eab-cfff551993dd",
3     "event_id": "2127",
4     "name": "Event report (1607362986)",
5     "content": "...",
6     "distribution": "5",
7     "sharing_group_id": "o",
8     "timestamp": "1607362986"
9 }
```

DATA LAYER: EVENT BUILDING BLOCKS - FULL



CONTEXT LAYER

CONTEXT LAYER: NAMING CONVENTIONS

- Context layer
 - ▶ **Tags** are free-text labels attached to events/attributes and can come from **Taxonomies**
 - Android Malware, C2, ...
 - ▶ **Taxonomies** are a set of common classification allowing to express the same vocabulary among a distributed set of users and organisations
 - `tlp:green, false-positive:risk="high", admiralty-scale:information-credibility="2"`

CONTEXT LAYER: NAMING CONVENTIONS

■ Context layer

- ▶ **Galaxies** are container composed of **Galaxy-clusters** that belongs to the same family
 - Similar to what **Events** are to **Attributes**
 - Country, Threat actors, Botnet, ...
- ▶ **Galaxy-clusters** are knowledge base items coming from **Galaxies**.
 - Basically a taxonomy with additional meta-information
 - misp-galaxy:threat-actor="APT 29",
misp-galaxy:country="luxembourg"

CONTEXT LAYER: TAGS

Simple free-text labels

TLP AMBER

TLP:AMBER

Threat tlp:Amber

tlp-amber

tlp::amber

tlp:amber

```
1 {  
2   "name": "Android malware",  
3   "colour": "#22681C",  
4   "exportable": true,  
5   "numerical_value": null,  
6 }
```

CONTEXT LAYER: TAXONOMIES

Simple label standardised on common set of vocabularies

Purpose: Enable efficient classification globally understood, easing consumption and automation.

Use case: Provide classification such as: TLP, Confidence, Source, Workflows, Event type, ...

Tag	Events	Attributes	Tags
<input type="checkbox"/> workflow:state="complete"	11	0	workflow:state="complete" 
<input type="checkbox"/> workflow:state="draft"	0	0	workflow:state="draft" 
<input type="checkbox"/> workflow:state="Incomplete"	55	10	workflow:state="Incomplete" 
<input type="checkbox"/> workflow:state="ongoing"	0	0	workflow:state="ongoing" 

CONTEXT LAYER: TAXONOMIES

```
1 {  
2   "Taxonomy": {  
3     "namespace": "admiralty-scale",  
4     "description": "The Admiralty Scale or Ranking (also called  
5       the NATO System) ...",  
6     "version": "6",  
7     "exclusive": false,  
8   },  
9   "entries": [  
10     {  
11       "tag": "admiralty-scale:information-credibility=\"1\"",  
12       "expanded": "Information Credibility: Confirmed by other  
13         sources",  
14       "numerical_value": 100,  
15       "exclusive_predicate": true,  
16     },  
17     ...  
18   ]  
19 }
```

CONTEXT LAYER: GALAXIES

Collections of galaxy clusters

Threat Actor galaxy

Galaxy ID	8
Name	Threat Actor
Namespace	misp
UUID	698774c7-8022-42c4-9171-8d6e4f06ada3
Description	Threat actors are characteristics of malicious actors (or adversaries) representing a cyber attack threat including presumed intent and historically observed behaviour.

= previous next =

All	Default	Custom	0	My Clusters	Deleted	View Fork Tree	View Galaxy Relationships	apt29	Filter			
ID	Published	Value	Synonyms	Owner Org	Creator Org	Default	Activity	#Events	#Relations	Description	Distribution	Actions
7059	N/A	APT 29	Dukes, Group 100, Cozy Duke, CozyDuke, EuroAPT, CozyBear, CozyCar, Cozer, Onion Mandaroon	MISP	MISP	✓	—	0	0 0 0	A 2015 report by F-Secure describe APT29 as: 'The Dukes are a well-resourced, highly dedicated and organized cyberspies group that we believe has been working for the Russian Federation since at least 2008 to collect intelligence in support of foreign and security policy decision-making. The Dukes show unusual confidence in their ability to conduct a successful communication tactic	All communities	

CONTEXT LAYER: GALAXY CLUSTERS

Kownledge base items including a description, links, synonyms, meta-information and relationships

Purpose: Enable description of complex high-level information for classification

UseCase: Extensively describe elements such as threat actors, countries, technique used, ...

Threat Actor :: APT 29

Cluster ID	2805
Name	APT 29
Parent Galaxy	Threat Actor
Description	A 2015 report by F-Secure describe APT29 as: "The Dukes are a well-resourced, highly dedicated and organized cyberespionage group that we believe has been working for the Russian Federation..."
Published	No
Default	Yes
Version	190
UUID	b2056ff0-00b9-482e-b11c-c771daa5f28a
Collection UUID	7cdff317-a673-4474-84ec-4f1754947823
Source	MISP Project
Authors	Alexandre Dulaunoy, Florian Roth, Thomas Schreck, Timo Steffens, Various
Distribution	All communities
Owner Organisation	 MISP
Creator Organisation	 MISP
Connector tag	misp-galaxy:threat-actor="APT 29"
Events	0
Forked From	
Forked By	

CONTEXT LAYER: GALAXY CLUSTERS

Galaxy cluster elements: Tabular view

Key ↓	Value	Actions
attribution-confidence	50	
cfr-suspected-state-sponsor	Russian Federation	
cfr-suspected-victims	United States	
cfr-suspected-victims	China	
cfr-suspected-victims	New Zealand	

Galaxy cluster elements: JSON view

CONTEXT LAYER: GALAXY CLUSTERS

```
1 {  
2     "uuid": "5edaoa53-1d98-4d01-ae06-40da0a00020f",  
3     "type": "fellowship-characters",  
4     "value": "Aragorn wielding Anduril",  
5     "tag_name": "misp-galaxy:fellowship-characters=\"c3fe907a-6a36  
6         -4cd1-9456-dcdf35c3f907\"",  
7     "description": "The Aragorn character wielding Anduril",  
8     "source": "Middle-earth universe by J. R. R. Tolkien",  
9     "authors": null,  
10    "version": "1591347795",  
11    "distribution": "0",  
12    "sharing_group_id": null,  
13    "default": false,  
14    "extends_uuid": "5edao117-1e14-4boa-9e26-34aff331dc3b",  
15    "extends_version": "1591345431",  
16    "GalaxyElement": [...],  
17    "GalaxyClusterRelation": [...]  
18 }
```

CONTEXT LAYER: GALAXIES & GALAXY CLUSTERS

- MISP integrates MITRE's Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) and similar Galaxy Matrix
- MISP terminology of these matrixes: Galaxy Matrix

Pre Attack - Attack Pattern	Enterprise Attack - Attack Pattern	Mobile Attack - Attack Pattern									
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	Securidty 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 Doppelganging	Password Filter DLL	System Information Discovery	Windows Remote Management	Clipboard Data	Exfiltration Over Other Network Medium	Multilayer 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	Seuid 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	

GALAXY JSON MATRIX-LIKE

```
1  {
2      "description": "Universal Development and Security Guidelines as
3          Applicable to Election Technology.",
4      "icon": "map",
5      "kill_chain_order": {           \\\bTab in the matrix
6          "example-of-threats": [     \\\bColumn in the matrix
7              "setup | party/candidate-registration",
8              "setup | electoral-rolls",
9              "campaign | campaign-IT",
10             "all-phases | governement-IT",
11             "voting | election-technology",
12             "campaign/public-communication | media/press"
13         ]
14     },
15     "name": "Election guidelines",
16     "namespace": "misp",
17     "type": "guidelines",
18     "uuid": "c1dc03b2-89b3-42a5-9d41-782ef726435a",
19     "version": 1
}
```

CLUSTER JSON MATRIX-LIKE

```
1  {
2      "description": "DoS or overload of party/campaign
3          registration , causing them to miss the deadline",
4      "meta": {
5          "date": "March 2018.",
6          "kill_chain": [ \Define in which column the cluster should be placed
7              "example-of-threats:setup | party/candidate-registration"
8          ],
9          "refs": [
10             "https://www.ria.ee/sites/default/files/content-editors/
11                 kuberturve/cyber_security_of_election_technology.pdf
12             "
13         ]
14     },
15     "uuid": "154c6186-a007-4460-a029-ea23163448fe",
16     "value": "DoS or overload of party/campaign registration ,
17             causing them to miss the deadline"
18 }
```

EXPRESSING RELATION BETWEEN CLUSTERS

- Cluster can be related to one or more clusters using default relationships from MISP objects and a list of tags to classify the relation.

```
1   "related": [
2     {
3       "dest-uuid": "5ce5392a-3a6c-4e07-9df3-9b6a9159ac45",
4       "tags": [
5         "estimative-language:likelihood-probability=\\\"likely\\\"",
6         ],
7         "type": "similar"
8       }
9     ],
10    "uuid": "oca45163-e223-4167-b1af-fo88ed14a93d",
11    "value": "Putter Panda"
```

ACKNOWLEDGEMENTS

- Supported by the grant 2018-LU-IA-0148



Co-financed by the European Union
Connecting Europe Facility

VISUALISE ALL THE THINGS

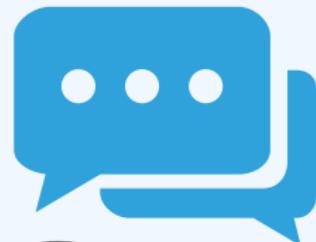
BUILDING DASHBOARD WIDGETS FOR MISP

CIRCL / TEAM MISP PROJECT

[HTTP://WWW.MISP-PROJECT.ORG/](http://www.misp-project.org/)

TWITTER: @MISPPROJECT

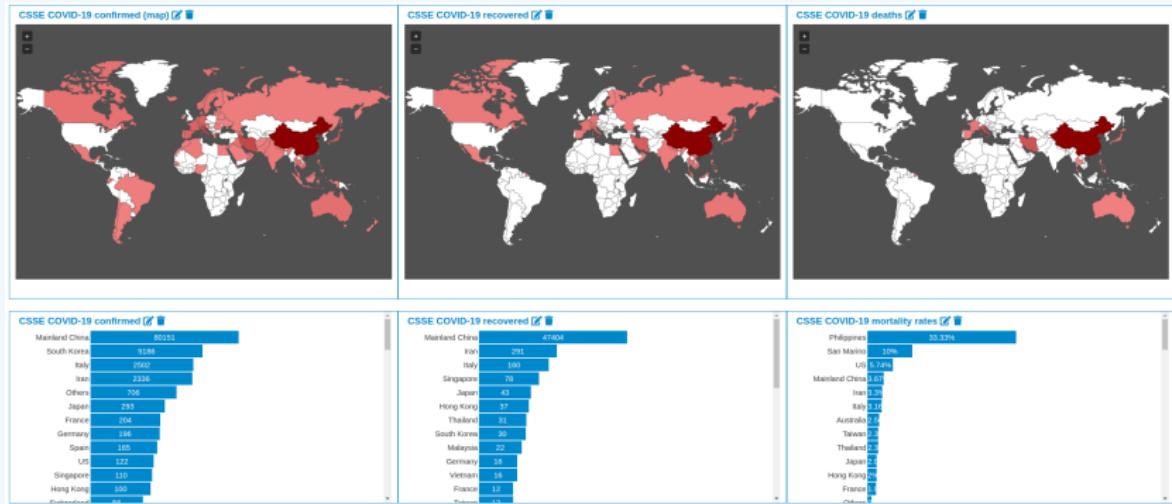
13TH ENISA-EC3 WORKSHOP



MISP
Threat Sharing

DASHBOARD IN MISP

- User configurable simple dashboard interface
- Visualise, aggregate and track data important to you
- Brand new feature, still undergoing reworks



THE INTERNALS OF AWIDGET

- Backend for the widget, full access to all MISP internals
- Load, convert, format to be represented via view widgets
- Widget metadata - size, name, description, behaviours
- Only main function required to be implemented: **handler()**
- Optional: **checkPermissions()** for ACL
- Accepts user configuration for which a template can be provided
- Located in /var/www/MISP/app/Lib/Dashboard/
- Custom widgets can be placed in
/var/www/MISP/app/Lib/Dashboard/Custom/

THE VIEW LAYER OF A WIDGET

- View files are included by default and reusable
- Currently we have a small but growing list of views
 - ▶ BarChart
 - ▶ SimpleList
 - ▶ WorldMap
- Converts the data passed by the Widget logic to HTML
- Located in
`/var/www/MISP/view/Elements/dashboard/Widgets/`

- Widgets can additionally be tied to certain **behaviours**:
 - ▶ Caching
 - Executions of the widget logic are cached
 - **Separate caches for each organisation in addition to site admins**
 - Cache duration is controlled by the widget logic
 - ▶ Refresh
 - Widgets can be set to refresh after x seconds
 - ▶ Both of these should be used with special care in regards to the use of **system resources**

EXERCISE MODULE: SIMPLE WHOAMI

- Let's start with a skeleton
- Create /var/www/MISP/app/Lib/Dashboard/Cus-
tom/WhoamiWidget.php
- MISP will parse anything ending with Widget.php in this
directory

EXERCISE MODULE: SIMPLE WHOAMI

```
1 <?php
2 class MispWhoamiWidget
3 {
4     public $title = 'Whoami';
5     public $render = 'SimpleList';
6     public $width = 2;
7     public $height = 2;
8     public $params = array();
9     public $description = 'Shows information about the
10        currently logged in user.';
11     public $cacheLifetime = false;
12     public $autoRefreshDelay = 3;
13
14     public function handler($user, $options = array())
15     {
16         $data = array();
17         return $data;
18     }
}
```

META INFORMATION

- **\$title:** The name of the widget
- **\$description:** A description of the widget
- **\$render:** The view element to use in rendering the widget
- **\$width & \$height:** Default relative dimensions
- **\$params:** Configuration array with explanations for each key
- **\$cacheLifetime:** The lifetime of the caches in seconds (false disables it)
- **\$autoRefreshDelay:** The time in seconds between each refresh (false disables it)

THE HANDLER

```
1 public function handler($user, $options = array())
2 {
3     $this->Log = ClassRegistry::init('Log');
4     $entries = $this->Log->find('all', array(
5         'recursive' => -1,
6         'conditions' => array(
7             'action' => 'login', 'user_id' => $user['id']
8         ),
9         'order' => 'id desc',
10        'limit' => 5,
11        'fields' => array('created', 'ip')
12    ));
13    foreach ($entries as &$entry) {
14        $entry = $entry['Log']['created'] . ' --- ' .
15        (
16            empty($entry['Log']['ip']) ?
17                'IP not logged' :
18                $entry['Log']['ip']
19        );
20    }
21    return array(
22        array('title' => 'Email', 'value' => $user['email']),
23        array(
24            'title' => 'Role', 'value' => $user['Role']['name']
25        ),
26        array(
27            'title' => 'Organisation',
28            'value' => $user['Organisation']['name']
29        ),
30        array(
31            'title' => 'IP', 'value' => $_SERVER['REMOTE_ADDR']
32        ),
33        array('title' => 'Last logins', 'value' => $entries)
34    );
35 }
```

RESULT

Whoami  

Email: admin@admin.test

Role: admin

Organisation: ORGNAME

IP: ::1

Last logins:

2020-03-05 06:50:46 --- ::1

2020-03-04 21:35:15 --- IP not logged

2020-03-04 09:34:44 --- IP not logged

2020-03-03 16:58:35 --- IP not logged

2020-03-03 06:49:10 --- IP not logged

TURNING DATA INTO ACTIONABLE INTELLIGENCE

ADVANCED FEATURES IN MISP SUPPORTING YOUR ANALYSES AND TOOLS

CIRCL / TEAM MISP PROJECT



13TH ENISA-EC3 WORKSHOP



ABOUT CIRCL



- The Computer Incident Response Center Luxembourg (CIRCL) is a government-driven initiative designed to provide a systematic response facility to computer security threats and incidents. CIRCL is the CERT for the private sector, communes and non-governmental entities in Luxembourg and is operated by securitymadein.lu g.i.e.

- CIRCL is mandated by the Ministry of Economy and acting as the Luxembourg National CERT for private sector.
- CIRCL leads the development of the Open Source MISP threat intelligence platform which is used by many military or intelligence communities, private companies, financial sector, National CERTs and LEAs globally.
- **CIRCL runs multiple large MISP communities performing active daily threat-intelligence sharing.**

THE AIM OF THIS PRESENTATION

- To give some insight into what sort of an evolution of our various communities' have gone through as observed over the past 8 years
- Show the importance of **strong contextualisation...**
- ...and how that can be leveraged when trying to make our data **actionable**

DEVELOPMENT BASED ON PRACTICAL USER FEEDBACK

- There are many different types of users of an information sharing platform like MISP:
 - ▶ **Malware reversers** willing to share indicators of analysis with respective colleagues.
 - ▶ **Security analysts** searching, validating and using indicators in operational security.
 - ▶ **Intelligence analysts** gathering information about specific adversary groups.
 - ▶ **Law-enforcement** relying on indicators to support or bootstrap their DFIR cases.
 - ▶ **Risk analysis teams** willing to know about the new threats, likelihood and occurrences.
 - ▶ **Fraud analysts** willing to share financial indicators to detect financial frauds.

THE INITIAL SCOPE OF MISP

- Extract information during the analysis process
- Store and correlate these datapoints
- Share the data with partners
- Focus on technical indicators: IP, domain, hostname, hashes, filename, pattern in file/memory/traffic
- Generate protective signatures out of the data: snort, suricata, OpenIOC

INITIAL WORKFLOW



WHY WAS IT SO SIMPLISTIC?

- This was both a reflection of our maturity as a community
 - ▶ Capabilities for **extracting** information
 - ▶ Capabilities for **utilising** the information
 - ▶ Lack of **willingness** to share context
 - ▶ Lack of **co-operation** between teams doing technical analysis/monitoring and threat-intel
- The more growth we saw in maturity, the more we tried to match it with our data-model, often against pushback

THE GROWING NEED TO CONTEXTUALISE DATA

- There were separate factors that made our data-sets less and less useful for detection/defense in general
 - ▶ **Growth of our communities**
 - ▶ Distinguish between information of interest and raw data
 - ▶ **False-positive** management
 - ▶ TTPs and aggregate information may be prevalent compared to raw data (risk assessment)
 - ▶ **Increased data volumes** leads to be able to prioritise

OUR INITIAL SOLUTION

- Allow users to **tag any information** created in MISP
- We wanted to be **lax with what we accept** in terms of data, but be **strict on what we fed to our tools**, with strong filter options
- We had some ideas on how to potentially move forward...

OUR INITIAL FAILURES

- Try to capture different aspects of contextualisation into **normalised values** (threat level, source reliability, etc)
 - ▶ Didn't scale with needs other than our own
 - ▶ Incorporating new types of contextualisation would mean **the modification of the software**
 - ▶ Getting communities with **established naming conventions** to use anything but their go-to vocabularies was a pipe-dream
 - ▶ Heated arguments over numeric conversions

HUMAN CREATIVITY

- We tried an alternate approach instead: Free tagging
 - ▶ Result was spectacularly painful, at least 7 different ways to spell tlp:amber
 - ▶ No canonisation for common terms lead to tagging ultimately becoming a highly flawed tool for filtering within a sharing community

TLP AMBER

TLP:AMBER

Threat tlp:Amber

tlp-amber

tlp::amber

tlp:amber

HOW WE ENDED UP TACKLING THE ISSUE MORE SUCCESSFULLY

- We ended up with a mixed approach, currently implemented by the MISP-taxonomy system
 - ▶ Taxonomies are **vocabularies** of known tags
 - ▶ Tags would be in a **triple tag format**
namespace:predicate="value"
 - ▶ Create your own taxonomies, recipients should be able to use data you tag with them without knowing it at the first place
 - ▶ Avoid any coding, stick to **JSON**
- Massive success, approaching 100 taxonomies
- Organisations can solve their own issues without having to rely on us

Tag	Events	Attributes	Tags
<input type="checkbox"/> workflow.state="complete"	11	0	workflow.state="complete" ↗
<input type="checkbox"/> workflow.state="draft"	0	0	workflow.state="draft" ↗
<input type="checkbox"/> workflow.state="Incomplete"	55	10	workflow.state="Incomplete" ↗
<input type="checkbox"/> workflow.state="ongoing"	0	0	workflow.state="ongoing" ↗

WE WERE STILL MISSING SOMETHING...

- Taxonomy tags often **non self-explanatory**
- Example: universal understanding of tlp:green vs APT 28
- For the latter, a single string was ill-suited
- So we needed something new in addition to taxonomies - **Galaxies**
 - ▶ Community driven **knowledge-base libraries used as tags**
 - ▶ Including descriptions, links, synonyms, meta information, etc.
 - ▶ Goal was to keep it **simple and make it reusable**
 - ▶ Internally it works the exact same way as taxonomies (stick to **JSON**)

B Ransomware galaxy	
Galaxy ID	373
Name	Ransomware
Namespace	misp
Uuid	3f44af2e-1480-4b6b-9aa8-9bb21341078
Description	Ransomware galaxy based on...
Version	4
Value ↓	Synonyms
.CryptoHasYou.	
777	Sevleg
7ev3n	7ev3n-HONE\$T

BROADENING THE SCOPE OF WHAT SORT OF CONTEXT WE ARE INTERESTED IN

- Who can receive our data? What can they do with it?
- Data accuracy, source reliability
- Why is this data relevant to us?
- Who do we think is behind it, what tools were used?
- What sort of motivations are we dealing with? Who are the targets?
- How can we block/detect/remediate the attack?
- What sort of impact are we dealing with?

PARALLEL TO THE CONTEXTUALISATION EFFORTS: FALSE POSITIVE HANDLING

- Low quality / false positive prone information being shared
- Lead to **alert-fatigue**
- Exclude organisation xy out of the community?
- False positives are often obvious - **can be encoded**
- **Warninglist system¹** aims to do that
- Lists of well-known indicators which are often false-positives like RFC1918 networks, ...

LIST OF KNOWN IPV4 PUBLIC DNS RESOLVERS

Id	89
Name	List of known IPv4 public DNS resolvers
Description	Event contains one or more public IPv4 DNS resolvers as attribute with an IDS flag set
Version	20181114
Type	string
Accepted attribute types	ip-src, ip-dst, domain ip
Enabled	Yes (disable)
Values	
1.0.0.1	
1.1.1.1	
1.11.71.4	

Warning: Potential false positives

List of known IPv4 public DNS resolvers

Top 1000 website from Alexa

List of known google domains

¹<https://github.com/MISP/misp-warninglists>

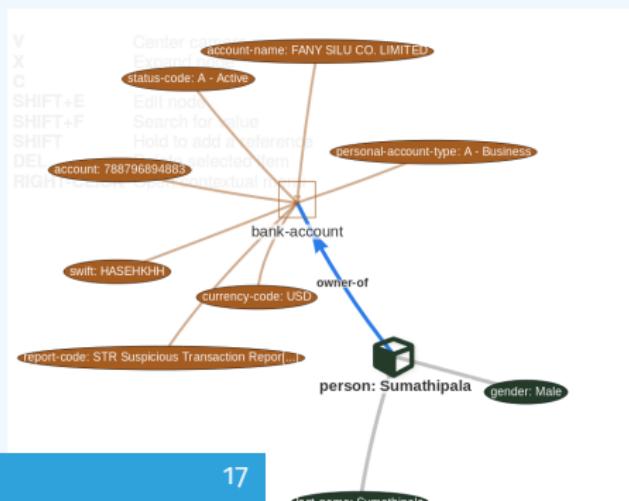
MORE COMPLEX DATA-STRUCTURES FOR A MODERN AGE

- Atomic attributes were a great starting point, but lacking in many aspects
- **MISP objects**² system
 - ▶ Simple **templating** approach
 - ▶ Use templating to build more complex structures
 - ▶ Decouple it from the core, allow users to **define their own** structures
 - ▶ MISP should understand the data without knowing the templates
 - ▶ Massive caveat: **Building blocks have to be MISP attribute types**
 - ▶ Allow **relationships** to be built between objects

²<https://github.com/MISP/misp-objects>

SUPPORTING SPECIFIC DATAMODEL

Date	Org	Category	Type	Value	Tags	Galleries	Comment	Correlate	Related Events
2018-09-28			Name: bank-account	*					
			References:	1					
2018-09-28	Other		status-code:	A - Active	<input type="button" value="x"/>	<input type="button" value="Add"/>		<input type="checkbox"/>	
2018-09-28	Other		report-code:	STR Suspicious Transaction Report	<input type="button" value="x"/>	<input type="button" value="Add"/>		<input type="checkbox"/>	
2018-09-28	Other		personal-account-type:	A - Business	<input type="button" value="x"/>	<input type="button" value="Add"/>		<input type="checkbox"/>	
2018-09-28	Financial fraud		swift:	HASEHKHH	<input type="button" value="x"/>	<input type="button" value="Add"/>		<input checked="" type="checkbox"/>	3849 11320 11584
2018-09-28	Financial fraud		account:	788796894883	<input type="button" value="x"/>	<input type="button" value="Add"/>		<input checked="" type="checkbox"/>	
2018-09-28	Other		account-name:	FANY SILU CO. LIMITED	<input type="button" value="x"/>	<input type="button" value="Add"/>		<input checked="" type="checkbox"/>	
2018-09-28	Other		currency-code:	USD	<input type="button" value="x"/>	<input type="button" value="Add"/>		<input type="checkbox"/>	



CONTINUOUS FEEDBACK LOOP

- Data ingested by MISP was in a sense frozen in time
- We had a creation date, but lacked a way to use the output of our detection
- Lead to the introduction of the **Sighting system**
- The community could sight indicators and convey the time of sighting
- Potentially powerful tool for IoC lifecycle management, clumsy query implementation default

SUPPORTING SPECIFIC DATAMODEL

Events	
<input checked="" type="checkbox"/>	No
<input checked="" type="checkbox"/>	No
<input checked="" type="checkbox"/>	No Inherit

Sightings

CIRCL: 2 (2017-03-19 16:17:59)



(2/0/0)

Tags [+](#)

Date 2016-02-24

Threat Level High

Analysis Initial

Distribution Connected communities
freetext test

Sighting Details

No

MISP: 2 CIRCL: 2

- Discussion

MAKING USE OF ALL THIS CONTEXT

- Most obvious goal: Improve the way we query data
 - ▶ Unified all export APIs
 - ▶ Incorporate all contextualisation options into **API filters**
 - ▶ Allow for an **on-demand** way of **excluding potential false positives**
 - ▶ Allow users to easily **build their own** export modules feed their various tools

EXAMPLE QUERY

```
/attributes/restSearch
{
    "returnFormat": "netfilter",
    "enforceWarninglist": 1,
    "tags": {
        "NOT": [
            "tlp:white",
            "type:OSINT"
        ],
        "OR": [
            "misp-galaxy:threat-actor=\"Sofacy\"",
            "misp-galaxy:sector=\"Chemical\""
        ],
    }
}
```

SYNCHRONISATION FILTERS

- Make decisions on whom to share data with based on context
 - ▶ MISP by default decides based on the information creator's decision who data gets shared with
 - ▶ Community hosts should be able to **act as a safety net** for sharing
 - **Push filters** - what can I push?
 - **Pull filters** - what am I interested in?
 - **Local tags** allow for information flow control

THE EMERGENCE OF ATT&CK AND SIMILAR GALAXIES

- Standardising on high-level **TTPs** was a solution to a long list of issues
- Adoption was rapid, tools producing ATT&CK data, familiar interface for users
- A much better take on kill-chain phases in general
- Feeds into our **filtering** and **situational awareness** needs extremely well
- Gave rise to other, ATT&CK-like systems tackling other concerns
 - ▶ **attck4fraud**³ by Francesco Bigarella from ING
 - ▶ **Election guidelines**⁴ by NIS Cooperation Group

³https://www.misp-project.org/galaxy.html#_attck4fraud

⁴https://www.misp-project.org/galaxy.html#_election_guidelines

EXAMPLE QUERY TO GENERATE ATT&CK HEATMAPS

```
/events/restSearch
{
    "returnFormat": "attack",
    "tags": [
        "misp-galaxy:sector=\"Chemical\""
    ],
    "timestamp": "365d"
}
```

A SAMPLE RESULT FOR THE ABOVE QUERY

Pre Attack - Attack Pattern	Enterprise Attack - Attack Pattern	Mobile Attack - Attack Pattern									
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	Securityd 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	Regexec/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 Doppelganging	Password Filter DLL	System Information Discovery	Windows Remote Management	Clipboard Data	Exfiltration Over Other Network Medium	Multilayer Encryption	
Supply Chain Compromise	CMSIPT	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	

MONITOR TRENDS OUTSIDE OF MISP (EXAMPLE: DASHBOARD)



DECAYING OF INDICATORS

- We were still missing a way to use all of these systems in combination to decay indicators
- Move the decision making **from complex filter options to complex decay models**
- Decay models would take into account various **taxonomies, sightings, the type** of each indicator **Sightings** and **Creation date**
- The first iteration of what we have in MISP now took:
 - ▶ 2 years of research
 - ▶ 3 published research papers
 - ▶ A lot of prototyping

SCORING INDICATORS: OUR SOLUTION

$$\text{score}(\text{Attribute}) = \text{base_score}(\text{Attribute, Model}) \bullet \text{decay}(\text{Model, time})$$

Where,

- $\text{score} \in [0, 100]$
- $\text{base_score} \in [0, 100]$
- decay is a function defined by model's parameters controlling decay speed
- Attribute Contains *Attribute's values and metadata* (*Taxonomies, Galaxies, ...*)
- Model Contains the *Model's configuration*

IMPLEMENTATION IN MISP: Event/view

The screenshot shows the MISP Event view interface. At the top, there are navigation links: Pivots, Galaxy, Event graph, Correlation graph, ATTACK matrix, Attributes, and Discussion. Below the navigation is a search bar with the placeholder 'Galaxies' and a user icon. Underneath the search bar are buttons for 'previous', 'next', and 'view all'. The main area displays a table of events. The columns include Date, Org, Category, Type, Value, Tags, Galaxies, Comment, Correlate, Related Events, Feed hits, IDS, Distribution, Sightings, Activity, Score, and Actions. The table lists several network activity events from different dates, each with associated tags like 'admiralty-scale.source-reliability', 'misp.confidence-level', and 'tp:amber'. The 'Score' column shows values like 65.26, 59.88, 54.6, 37.43, 37.41, and 23.31, with a note that Model 5 has a score of 0. The 'Actions' column contains icons for edit, delete, and other operations.

Date	Org	Category	Type	Value	Tags	Galaxies	Comment	Correlate	Related Events	Feed hits	IDS	Distribution	Sightings	Activity	Score	Actions
2019-09-12		Network activity	ip-src	5.5.5.5				<input checked="" type="checkbox"/>		<input type="checkbox"/> Inherit	(0/0)	(0/0)	(0/0)	(0/0)	NIDS Simple Decaying ... 65.26	
2019-08-13		Network activity	ip-src	8.8.8.8	admiralty-scale.source-reliability:"a" retention:expired			<input checked="" type="checkbox"/>	1 2 2 2 Show 11 more...	S1:1 <input checked="" type="checkbox"/> Inherit	(0/0)	(0/0)	(0/0)	(0/0)	NIDS Simple Decaying ... 59.88	
2019-08-13		Network activity	ip-src	9.9.9.9	admiralty-scale.source-reliability:"c" misp.confidence-level:"completely-confident" tp:amber			<input checked="" type="checkbox"/>	1 3 19 28 Show 6 more...	S1:1 <input checked="" type="checkbox"/> Inherit	(4/10)	(4/10)	(4/10)	(4/10)	NIDS Simple Decaying ... 54.6	
2019-08-13		Network activity	ip-src	7.7.7.7	admiralty-scale.information-credibility:"e" retention:2d			<input checked="" type="checkbox"/>	41	<input checked="" type="checkbox"/> Inherit	(0/0)	(0/0)	(0/0)	(0/0)	NIDS Simple Decaying ... 37.43	
2019-07-18		Network activity	ip-src	6.6.6.6				<input checked="" type="checkbox"/>	41	<input checked="" type="checkbox"/> Inherit	(0/0)	(0/0)	(0/0)	(0/0)	NIDS Simple Decaying ... 37.41	
															Model 5 0	
															NIDS Simple Decaying ... 23.31	
															Model 5 0	

- Decay score toggle button
 - ▶ Shows Score for each *Models* associated to the *Attribute* type

IMPLEMENTATION IN MISP: API RESULT

```
/attributes/restSearch
"Attribute": [
  {
    "category": "Network activity",
    "type": "ip-src",
    "to_ids": true,
    "timestamp": "1565703507",
    [...]
    "value": "8.8.8.8",
    "decay_score": [
      {
        "score": 54.475223849544456,
        "decayed": false,
        "DecayingModel": {
          "id": "85",
          "name": "NIDS Simple Decaying Model"
        }
      }
    ]
  }
]
```

IMPLEMENTATION IN MISP: INDEX

Decaying Models

All Models		My Models		Shared Models		Default Models				
ID	Organization	Usable to everyone	Name	Description	Parameters { } 	Formula	# Assigned Types	Version	Enabled	Actions
29	1	✓	Phishing model	Simple model to rapidly decay phishing website.	{ "lifetime": 3, "decay_speed": 2.3, "threshold": 30, "default_base_score": 80, "base_score_config": { "estimative-language": 0.5, "phishing": 0.5 } }	Polynomial 	9	1	✓	     
85	1	✗	NIDS Simple Decaying Model 	Simple decaying model for Network Intrusion Detection System (NIDS).	{ "lifetime": 120, "decay_speed": 2, "threshold": 30, "default_base_score": 80, "base_score_config": { "estimative-language": 0.25, "priority-level": 0.25, "retention": 0.25, "targeted-threat-index": 0.125, "false-positive": 0.125 } }	Polynomial 	13	1	✓	     

Page 1 of 1, showing 2 records out of 2 total, starting on record 1, ending on 2

[« previous](#) [next »](#)

View, update, add, create, delete, enable, export, import

IMPLEMENTATION IN MISP: FINE TUNING TOOL

Home Event Actions Databases Input Filters Global Actions Sync Actions Administration Audit MISP AI

Import Decoying Model
Add Decoying Model
Decoying Tool
List Decoying Models

Decoying Of Indicator Fine Tuning Tool

Show All Types Show MISP Objects Search Attribute Type

Attribute Type	Category	Model ID
abs-r11	Financial fraud	
authentihash	Payload delivery	
bank-account-nr	Financial fraud	
btc	Financial fraud	
bin	Financial fraud	
bro	Network activity	ID 11
btc	Financial fraud	11
cc-number	Financial fraud	
cphash	Payload delivery	
community-id	Network activity	
domain	Network activity	
domainip	Network activity	ID 84
email-attachment	Payload delivery	
email-dst	Network activity	11
email-src	Payload delivery	
filename	Payload delivery	
Renameauthentihash	Payload delivery	
Renameimpfuzzy	Payload delivery	
Renamejepfuzzy	Payload delivery	
Renamejephash	Payload delivery	
Renamejns	Payload delivery	13
Renamejphash	Payload delivery	13
Renamejs1	Payload delivery	13

Polynomial

Lifetime: 3 days
Decay speed: 2.3
Cut-off threshold: 30
Adjust base score: Simulate this model:

Phishing model: Simple model to rapidly decay Take

All available models My models Default models

ID	Model Name	Org ID	Description	Formula	Lifetime	Decay speed	Threshold	Default basesscore	Basescore config	Settings	# Types	Enabled	Action
29	Phishing model	1	Simple model to rapidly decay	polynomial	3	2.3	30	80	estimative-language-phishing website.	0.5	9	<input checked="" type="checkbox"/>	<input type="button" value="Load model"/>

Create, modify, visualise, perform mapping

IMPLEMENTATION IN MISP: base_score TOOL

Search Taxonomy x 3 not having numerical value

Default basescore: 80

Taxonomies Weight

Taxonomy	Weight
admiralty-scale ▾	
source-reliability ▾	31
information-credibility ▾	30
priority-level ▾	
priority-level ▾	53
retention ▾	
retention ▾	0
estimative-language ▾	
likelihood-probability ▾	0
confidence-in-analytic-judgment ▾	0
misp ▾	
confidence-level ▾	0
threat-level ▾	0
automation-level ▾	0
phishing ▾	
state ▾	0
psychological-acceptability ▾	0
Excluded ▾	

Placeholder for 'Organisation source confidence'

admiralty-scale information-credibility (20%) priority-level (68%)

admiralty-scale source-reliability (27%)

Example ⓘ

Attribute	Tags	Base score
Tag your attribute		
Attribute 1	admiralty-scale information-credibility="5"	0.0 ⓘ
Attribute 2	priority-level:baseline-minor admiralty-scale:source-reliability="d" admiralty-scale information-credibility="2"	38.2 ⓘ
Attribute 3	priority-level:severe admiralty-scale:information-credibility="2"	84.6 ⓘ

Computation steps

Tag	Computation		Result
	Eff. Ratio	Value	
priority-level:baseline-minor	0.46 *	25.00	11.62
admiralty-scale:source-reliability="d"	0.27 *	25.00	6.80

IMPLEMENTATION IN MISP: SIMULATION TOOL

NIDS Simple Decaying Model

RestSearch Specific ID

Attribute RestSearch*

```
{"includeDecayScore": 1, "includeFullModel": 0, "score": 30, "excludeDecayed": 0, "decayingModel": [85], "to_ids": 1, "tags": ["estimative-language%", "priority-level%", "intermediate%", "targeted-threat"], "id": 36759}
```

Search

Base score: Base score configuration not set. But default value sets.

Tag	Computation	Result
misp:confidence-level="usually-confident"	EHI, Ratio	0 × 75.00 0
misp:confidence-level="fairly-confident"	EHI, Ratio	0 × 50.00 0
adversary-scale-source-reliability="a"	EHI, Ratio	0 × 100.00 0
retention_expired	EHI, Ratio	0 × N/A 0
base_score		80.00

Sighting: Wed Sep 4 12:18:09 2019 | Current score: 54.60

Base score: Base score configuration not set. But default value sets.

Score

August September October November December 2020

ID: 36759 | Sighting: Wed Sep 4 12:18:09 2019 | Score: 54.60

ID	Event	T	Date	Org	Category	Type	Value	Tags	Event Tags	Galaxies	Comment	ID#	Sightings	Score
36759	45		2019-08-13	ORIONAME	Network activity	ip-src	7.7.7.7	adversary-scale-information-confidence="C" retention_id=36759	misp:confidence-level="usually-confident" misp:confidence-level="fairly-confident"			✓		37.41
36757	45		2019-08-13	ORIONAME	Network activity	ip-src	8.8.8.8	adversary-scale-source-reliability="a" retention_expired	misp:confidence-level="usually-confident" misp:confidence-level="fairly-confident"			✓		54.6

Page 1 of 1, showing 2 records out of 2 total, starting on record 1, ending on 2

< previous next >

Simulate Attributes with different Models

IMPLEMENTATION IN MISP: API QUERY BODY

```
/attributes/restSearch
{
    "includeDecayScore": 1,
    "includeFullModel": 0,
    "excludeDecayed": 0,
    "decayingModel": [85],
    "modelOverrides": {
        "threshold": 30
    }
    "score": 30,
}
```

TO SUM IT ALL UP...

- Massive rise in **user capabilities**
- Growing need for truly **actionable threat intel**
- Lessons learned:
 - ▶ **Context is king** - Enables better decision making
 - ▶ **Intelligence and situational awareness** are natural by-products of context
 - ▶ Don't lock users into your **workflows**, build tools that enable theirs

GET IN TOUCH IF YOU HAVE ANY QUESTIONS

■ Contact us

- ▶ https://twitter.com/mokaddem_sami
- ▶ <https://twitter.com/iglocska>

■ Contact CIRCL

- ▶ info@circl.lu
- ▶ https://twitter.com/circl_lu
- ▶ <https://www.circl.lu/>

■ Contact MISPPProject

- ▶ <https://github.com/MISP>
- ▶ <https://gitter.im/MISP/MISP>
- ▶ <https://twitter.com/MISPPProject>

TURNING DATA INTO ACTIONABLE INTELLIGENCE

ADVANCED FEATURES IN MISP SUPPORTING YOUR ANALYTICS AND TOOLS

CIRCL / TEAM MISP PROJECT



13TH ENISA-EC3 WORKSHOP



THE AIM OF THIS PRESENTATION

- Why is **contextualisation** important?
- What options do we have in MISP?
- How can we **leverage** this in the end?

THE GROWING NEED TO CONTEXTUALISE DATA

- Contextualisation became more and more important as we as a community matured
 - ▶ **Growth and diversification** of our communities
 - ▶ Distinguish between information of interest and raw data
 - ▶ **False-positive** management
 - ▶ TTPs and aggregate information may be prevalent compared to raw data (risk assessment)
 - ▶ **Increased data volumes** leads to a need to be able to prioritise
- These help with filtering your TI based on your **requirements...**
- ...as highlighted by Pasquale Stirparo *Your Requirements Are Not My Requirements*

OBJECTIVES

- Some main objectives we want to achieve when producing data
 - ▶ Ensure that the information is **consumable** by everybody
 - ▶ That it is **useful** to the entire target audience
 - ▶ The data is **contextualised** for it to be understood by everyone
- What we ideally want from our data
 - ▶ We want to be able to **filter** data for different use-cases
 - ▶ We want to be able to get as much knowledge out of the data as possible
 - ▶ We want to know where the data is from, how it got there, why we should care

DIFFERENT LAYERS OF CONTEXT

- Context added by analysts / tools
- Data that tells a story
- Encoding analyst knowledge to automatically leverage the above

CONTEXT ADDED BY ANALYSTS / TOOLS

EXPRESSING WHY DATA-POINTS MATTER

- An IP address by itself is barely ever interesting
- We need to tell the recipient / machine why this is relevant
- All data in MISP has a bare minimum required context
- We differentiate between indicators and supporting data

BROADENING THE SCOPE OF WHAT SORT OF CONTEXT WE ARE INTERESTED IN

- Who can receive our data? What can they do with it?
- Data accuracy, source reliability
- Why is this data relevant to us?
- Who do we think is behind it, what tools were used?
- What sort of motivations are we dealing with? Who are the targets?
- How can we block/detect/remediate the attack?
- What sort of impact are we dealing with?

TAGGING AND TAXONOMIES

- Simple labels
- Standardising on vocabularies
- Different organisational/community cultures require different nomenclatures
- Triple tag system - taxonomies
- JSON libraries that can easily be defined without our intervention

Tag	Events	Attributes	Tags
<input type="checkbox"/> workflow:state="complete"	11	0	workflow:state="complete" 
<input type="checkbox"/> workflow:state="draft"	0	0	workflow:state="draft" 
<input type="checkbox"/> workflow:state="Incomplete"	55	10	workflow:state="Incomplete" 
<input type="checkbox"/> workflow:state="ongoing"	0	0	workflow:state="ongoing" 

- Taxonomy tags often **non self-explanatory**
 - ▶ Example: universal understanding of tlp:green vs APT 28
- For the latter, a single string was ill-suited
- So we needed something new in addition to taxonomies - **Galaxies**
 - ▶ Community driven **knowledge-base libraries used as tags**
 - ▶ Including descriptions, links, synonyms, meta information, etc.
 - ▶ Goal was to keep it **simple and make it reusable**
 - ▶ Internally it works the exact same way as taxonomies (stick to **JSON**)

B Ransomware galaxy		
Galaxy ID	373	
Name	Ransomware	
Namespace	misp	
Uuid	3f44af2e-1480-4b6b-9aa8-f9bb21341078	
Description	Ransomware galaxy based on...	
Version	4	
Value ↓		Synonyms
.CryptoHasYou.		
777		Sevleg
7ev3n		7ev3n-HONE\$T

THE EMERGENCE OF ATT&CK AND SIMILAR GALAXIES

- Standardising on high-level **TTPs** was a solution to a long list of issues
- Adoption was rapid, tools producing ATT&CK data, familiar interface for users
- A much better take on kill-chain phases in general
- Feeds into our **filtering** and **situational awareness** needs extremely well
- Gave rise to other, ATT&CK-like systems tackling other concerns
 - ▶ **attck4fraud**¹ by Francesco Bigarella from ING
 - ▶ **Election guidelines**² by NIS Cooperation Group

¹https://www.misp-project.org/galaxy.html#_attck4fraud

²https://www.misp-project.org/galaxy.html#_election_guidelines

DATA THAT TELLS A STORY

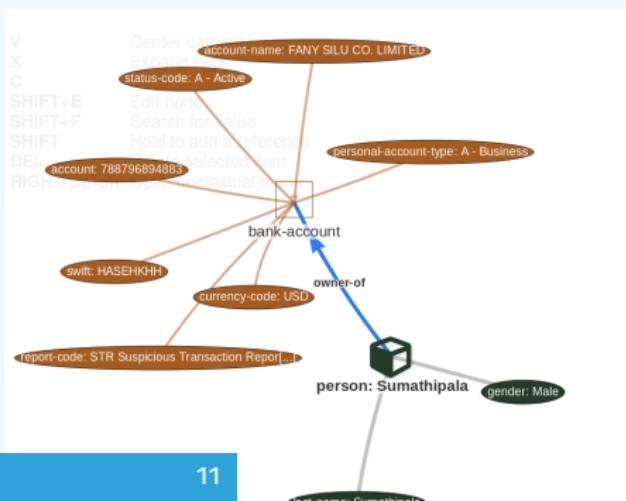
MORE COMPLEX DATA-STRUCTURES FOR A MODERN AGE

- Atomic attributes were a great starting point, but lacking in many aspects
- **MISP objects³** system
 - ▶ Simple **templating** approach
 - ▶ Use templating to build more complex structures
 - ▶ Decouple it from the core, allow users to **define their own** structures
 - ▶ MISP should understand the data without knowing the templates
 - ▶ Massive caveat: **Building blocks have to be MISP attribute types**
 - ▶ Allow **relationships** to be built between objects

³<https://github.com/MISP/misp-objects>

SUPPORTING SPECIFIC DATAMODELS

Date	Org	Category	Type	Value	Tags	Galaxies	Comment	Correlate	Related Events
2018-09-28			Name: bank-account	*					
			References:	0					
2018-09-28		Other	status-code: text	A - Active	+ Add				
2018-09-28		Other	report-code: text	STR Suspicious Transaction Report	+ Add				
2018-09-28		Other	personal-account-type: text	A - Business	+ Add				
2018-09-28		Financial fraud	swift: bic	HASEHKHH	+ Add			<input checked="" type="checkbox"/>	3849 11320 11584
2018-09-28		Financial fraud	account: bank-account-nr	788799994883	- Add			<input checked="" type="checkbox"/>	
2018-09-28		Other	account-name: text	FANY SILU CO. LIMITED	+ Add			<input checked="" type="checkbox"/>	
2018-09-28		Other	currency-code: text	USD	+ Add				



CONTINUOUS FEEDBACK LOOP

- Data shared was **frozen in time**
- All we had was a creation/modification timestamp
- Improved tooling and willingness allowed us to create a **feedback loop**
- Lead to the introduction of the **Sighting system**
- Signal the fact of an indicator sighting...
- ...as well as **when** and **where** it was sighted
- Vital component for IoC **lifecycle management**

CONTINUOUS FEEDBACK LOOP (2)

Events

<input checked="" type="checkbox"/>	No	Sightings
<input checked="" type="checkbox"/>	No	(2/0/0)
<input checked="" type="checkbox"/>	No	Inherit (0/0/0)

Sightings

CIRCL: 2 (2017-03-19 16:17:59)

(2/0/0)

Tags +

Date 2016-02-24

Threat Level High

Analysis Initial

Distribution Connected communities
freetext test

Sighting Details

No

MISP: 2

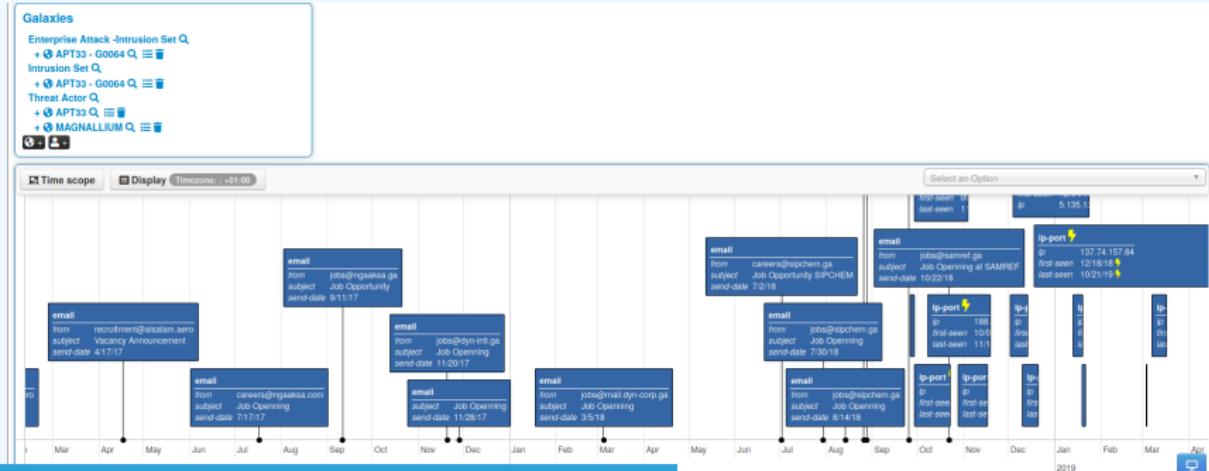
CIRCL: 2

4 (2) - restricted to own organisation only.

- Discussion

A BRIEF HISTORY OF TIME - ADDING TEMPORALITY TO OUR DATA

- As Andreas said - no time based aspect was painful
- Recently introduced **first_seen** and **last_seen** data points
- Along with a complete integration with the **UI**
- Enables the **visualisation** and **adjustment** of indicators timeframes



THE VARIOUS WAYS OF ENCODING ANALYST KNOWLEDGE TO AUTOMATI- CALLY LEVERAGE OUR TI

FALSE POSITIVE HANDLING

- Low quality / false positive prone information being shared
- Lead to **alert-fatigue**
- Exclude organisation xy out of the community?
- FPs are often obvious - **can be encoded**
- **Warninglist system⁴** aims to do that
- Lists of well-known indicators which are often false-positives like RFC1918 networks, ...

LIST OF KNOWN IPV4 PUBLIC DNS RESOLVERS

Id	89
Name	List of known IPv4 public DNS resolvers
Description	Event contains one or more public IPv4 DNS resolvers as attribute with an IDS flag set
Version	20181114
Type	string
Accepted attribute types	ip-src, ip-dst, domain ip
Enabled	Yes (disabled)
Values	
1.0.0.1	
1.1.1.1	
1.11.71.4	

Warning: Potential false positives

List of known IPv4 public DNS resolvers

Top 1000 website from Alexa

List of known google domains

⁴<https://github.com/MISP/misp-warninglists>

MAKING USE OF ALL THIS CONTEXT

- Providing advanced ways of querying data
 - ▶ Unified export APIs
 - ▶ Incorporating all contextualisation options into **API filters**
 - ▶ Allowing for an **on-demand** way of **excluding potential false positives**
 - ▶ Allowing users to easily **build their own** export modules feed their various tools

EXAMPLE QUERY

```
/attributes/restSearch
{
    "returnFormat": "netfilter",
    "enforceWarninglist": 1,
    "tags": {
        "NOT": [
            "tlp:white",
            "type:OSINT"
        ],
        "OR": [
            "misp-galaxy:threat-actor=\"Sofacy\"",
            "misp-galaxy:sector=\"Chemical\""
        ],
    }
}
```

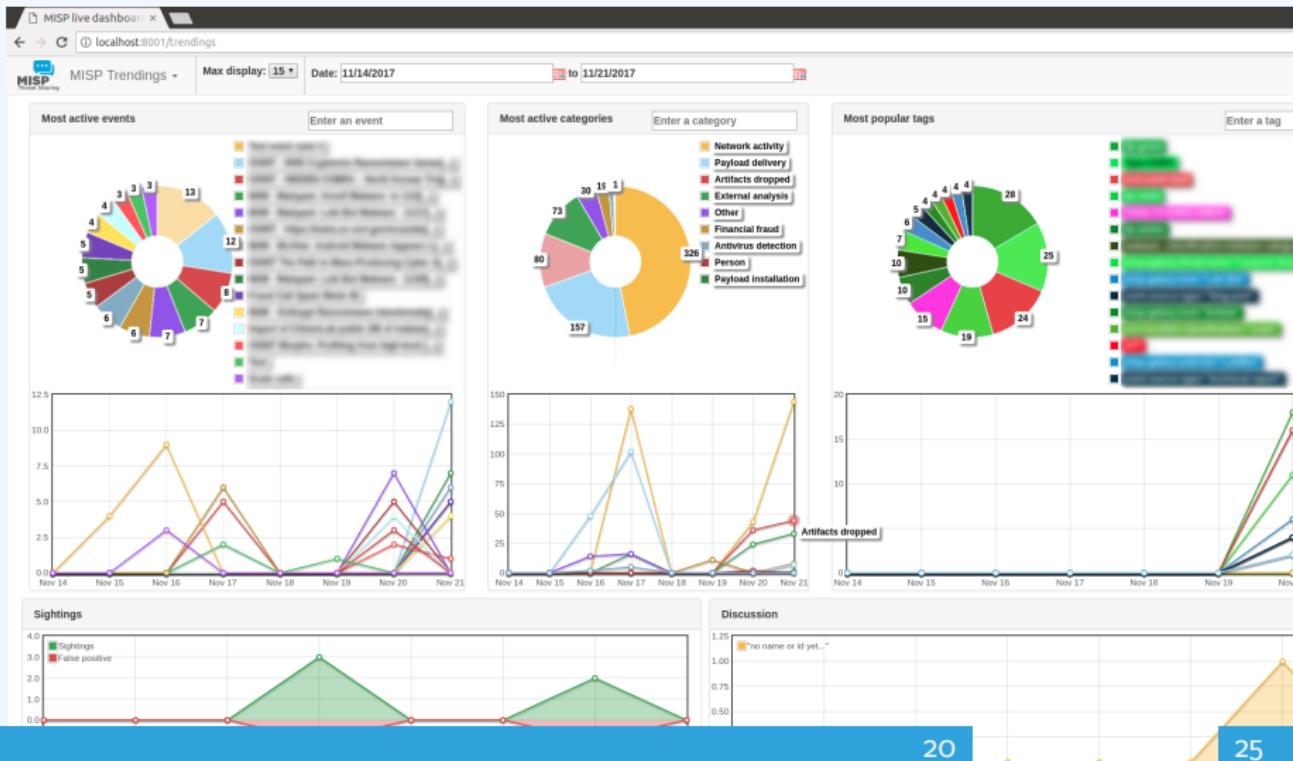
EXAMPLE QUERY TO GENERATE ATT&CK HEATMAPS

```
/events/restSearch
{
    "returnFormat": "attack",
    "tags": [
        "misp-galaxy:sector=\"Chemical\""
    ],
    "timestamp": "365d"
}
```

A SAMPLE RESULT FOR THE ABOVE QUERY

Pre Attack - Attack Pattern	Enterprise Attack - Attack Pattern	Mobile Attack - Attack Pattern								
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	Securityd 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	Regexec/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 Doppelganging	Password Filter DLL	System Information Discovery	Windows Remote Management	Clipboard Data	Exfiltration Over Other Network Medium	Multilayer Encryption
Supply Chain Compromise	CMSIPT	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

MONITOR TRENDS OUTSIDE OF MISP (EXAMPLE: DASHBOARD)



DECAYING OF INDICATORS

- We were still missing a way to use all of these systems in combination to decay indicators
- Move the decision making **from complex filter options to complex decay models**
- Decay models would take into account various available **context**
 - ▶ Taxonomies
 - ▶ Sightings
 - ▶ type of each indicator
 - ▶ Creation date
 - ▶ ...

IMPLEMENTATION IN MISP: Event/view

Pivots Galaxy Event graph Correlation graph ATT&CK matrix Attributes Discussion

x 45 Decays

Galaxies

+ + +

< previous next > view all

Scope toggle Deleted Decay score Context Related Tags Filtering tool (1)

Date	Org	Category	Type	Value	Tags	Galaxies	Comment	Correlate	Related	Feed	IDS	Distribution	Sightings	Activity	Score	Actions	
										Events	hits						
2019-09-12			Network activity	ip-src	5.5.5.5			<input checked="" type="checkbox"/>	<input type="checkbox"/>	Inherit	(WORK)		NIDS Simple Decaying ...	65.26			
2019-08-13			Network activity	ip-src	8.8.8.8	 4 4 x		<input checked="" type="checkbox"/>	1 2 2 2 S1:1	Inherit	(S0/0)		NIDS Simple Decaying ...	54.6			
2019-08-13			Network activity	ip-src	9.9.9.9	 4 4 "completely-confident" "completely-confident" x		<input checked="" type="checkbox"/>	1 3 19 S1:1 28 Show 6	Inherit	(4/10)		NIDS Simple Decaying ...	37.43			
2019-08-13			Network activity	ip-src	7.7.7.7	 4 4 x		<input checked="" type="checkbox"/>	41	<input checked="" type="checkbox"/>	Inherit	(2/0)		NIDS Simple Decaying ...	37.41		
2019-07-18			Network activity	ip-src	6.6.6.6			<input checked="" type="checkbox"/>	41	<input checked="" type="checkbox"/>	Inherit	(0/0)		NIDS Simple Decaying ...	23.31		

- Decay score toggle button
 - ▶ Shows Score for each *Models* associated to the *Attribute* type

IMPLEMENTATION IN MISP: API RESULT

```
/attributes/restSearch
"Attribute": [
  {
    "category": "Network activity",
    "type": "ip-src",
    "to_ids": true,
    "timestamp": "1565703507",
    [...]
    "value": "8.8.8.8",
    "decay_score": [
      {
        "score": 54.475223849544456,
        "decayed": false,
        "DecayingModel": {
          "id": "85",
          "name": "NIDS Simple Decaying Model"
        }
      }
    ]
  }
]
```

TO SUM IT ALL UP...

- Massive rise in **user capabilities**
- Growing need for truly **actionable threat intel**
- Lessons learned:
 - ▶ **Context is king** - Enables better decision making
 - ▶ **Intelligence and situational awareness** are natural by-products of context
 - ▶ Don't lock users into your **workflows**, build tools that enable theirs

GET IN TOUCH IF YOU HAVE ANY QUESTIONS

■ Contact us

- ▶ https://twitter.com/mokaddem_sami
- ▶ <https://twitter.com/iglocska>

■ Contact CIRCL

- ▶ info@circl.lu
- ▶ https://twitter.com/circl_lu
- ▶ <https://www.circl.lu/>

■ Contact MISPPProject

- ▶ <https://github.com/MISP>
- ▶ <https://gitter.im/MISP/MISP>
- ▶ <https://twitter.com/MISPPProject>

MISP STANDARD

THE COLLABORATIVE INTELLIGENCE STANDARD POW-

CIRCL / TEAM MISP PROJECT

[HTTP://WWW.MISP-STANDARD.ORG/](http://www.misp-standard.org/)

TWITTER: @MISPPROJECT

13TH ENISA-EC3 WORKSHOP



MISP
Threat Sharing

MISP STANDARD

- Following the growth of organisations relying on MISP, the **JSON format used by MISP are standardised under the misp-standard.org umbrella**
- The goal is to provide a flexible set of standards to support information exchange and data modeling in the following field:
 - ▶ Cybersecurity intelligence
 - ▶ Threat intelligence
 - ▶ Financial fraud
 - ▶ Vulnerability information
 - ▶ Border control information
 - ▶ Digital Forensic and Incident Response
 - ▶ and intelligence at large

STANDARD - MISP CORE FORMAT

This standard describes the **MISP core format** used to exchange indicators and threat information between MISP instances. The **JSON format includes the overall structure along with the semantics associated for each respective key**. The format is described to support other implementations, aiming to reuse the format and ensuring the interoperability with the existing MISP software and other Threat Intelligence Platforms.

MISP OBJECT TEMPLATE FORMAT

This standard describes the **MISP object** template format which describes a simple JSON format to represent the various templates used to construct MISP objects. A **public directory of common MISP object templates and relationships** is available and relies on the MISP object reference format.

MISP GALAXY FORMAT

This standard describes the **MISP galaxy format which describes a simple JSON format to represent galaxies and clusters** that can be attached to MISP events or attributes. A public directory of MISP galaxies is available and relies on the MISP galaxy format. MISP galaxies are used to attach additional information structures such as MISP events or attributes. **MISP galaxy is a public repository of known malware, threats actors and various other collections of data that can be used to mark, classify or label data in threat information sharing.**

SIGHTINGDB FORMAT

This standard describes the format used by SightingDB to give automated context to a given Attribute by **counting occurrences and tracking times of observability**. SightingDB was designed to provide to MISP and other tools an interoperable, scalable and fast way to store and retrieve attributes sightings.

INTERNET-DRAFT - IETF FOR MISP FORMATS AND MISP STANDARD

- If you want to contribute to our IETF Internet-Draft for the MISP standard, `misp-rfc1` is the repository where to contribute.
- **Update only the markdown file**, the XML and ASCII for the IETF I-D are automatically generated.
- If a major release or updates happen in the format, we will publish the I-D to the IETF².
- The process is always MISP implementation → IETF I-D updates.
- Then published standards in `misp-standard.org`.

¹<https://github.com/MISP/misp-rfc>

²<https://datatracker.ietf.org/doc/search/?name=misp&active=drafts=on&rfcbs=on>

MISP CLI

AUTOMATE ALL THE THINGS

CIRCL / TEAM MISP PROJECT



13TH ENISA-EC3 WORKSHOP

MISP CLI FUNCTIONALITIES

- The MISP API is great for remotely executing administrative tasks
- But sometimes we want to simplify the process / avoid having to deal with authentication
- MISP also has an extensive CLI sub-system for this reason

TYPES OF OBJECTIVES FOR THE SCRIPTS

- Automating recurring tasks
- Recovery from loss of access
- Updates / initialisation
- Background worker management

CLI DOCUMENTATION

■ <https://path.to.your.misp/events/automation>

Administering the background workers via the API.

You can start/stop and view the background workers via the API.

Add worker: `http://localhost:5001/servers/startWorker/[queue_name]`

Stop worker: `http://localhost:5001/servers/stopWorker/[worker_pid]`

Get worker info: `http://localhost:5001/servers/getWorkers`

Administering MISP via the CLI

Certain administrative tasks are exposed to the API, these help with maintaining and configuring MISP in an automated way / via external tools.:

Get Setting: `MISP/app/Console/cake Admin getSetting [setting]`

Set Setting: `MISP/app/Console/cake Admin setSetting [setting] [value]`

Get Authkey: `MISP/app/Console/cake Admin getAuthkey [email]`

Set Baseurl: `MISP/app/Console/cake Baseurl [baseurl]`

Change Password: `MISP/app/Console/cake Password [email] [new_password] [--override_password_change]`

Clear BruteForce Entries: `MISP/app/Console/cake Admin clearBruteforce [user_email]`

Run Database Update: `MISP/app/Console/cake Admin updateDatabase`

Update All JSON Structures: `MISP/app/Console/cake Admin updateJSON`

Update Galaxy Definitions: `MISP/app/Console/cake Admin updateGalaxies`

Update Taxonomy Definitions: `MISP/app/Console/cake Admin updateTaxonomies`

Update Object Templates: `MISP/app/Console/cake Admin updateObjectTemplates`

Update Warninglists: `MISP/app/Console/cake Admin updateWarningLists`

USAGE

```
/var/www/MISP/app\Console/cake [Shell] [Command]  
[parameters]
```

- Example:
 - ▶ /var/www/MISP/app\Console/cake Password
"andras.iklody@gmail.com" "Nutella"
 - ▶ Change password to "Nutella" for my user
 - ▶ Some shells are single use and don't need a command parameter
- Also used by the background processing
- Automation is meant to be used via cron jobs

AUTOMATION VIA CRONTAB

- Edit crontab of www-data user
- `crontab -u www-data -e`
- `0 3,9,15,21 * * *`
`/var/www/MISP/app/Console/cake Server pull 1`
`30 full`
- Pull server ID #30 as user #1 every 6 hours
- `@hourly /var/www/MISP/app/Console/cake Server`
`cacheFeed 1 csv full`
- Cache all csv feeds as user #1 every hour

MISP DEPLOYMENT

SOME BASIC GUIDELINES

CIRCL / TEAM MISP PROJECT



13TH ENISA-EC3 WORKSHOP

MISP DEPLOYMENT CONSIDERATIONS

- Deployment types
- Distro choice
- Hardware specs
- Authentication
- Other considerations - **settings, gotchas**

DEPLOYMENT TYPES

- Native install
 - ▶ Manual
 - ▶ One liner script - INSTALL.sh
<https://github.com/MISP/MISP/tree/2.4/INSTALL>
- MISP VM
<https://www.circl.lu/misp-images/latest/>
- Docker
- RPM maintained by SWITCH
<https://github.com/amuehlem/MISP-RPM>
- Cloud provider images
<https://github.com/MISP/misp-cloud>

DOCKER OPTIONS

- Ostefano's Docker instance (x86-64 (AMD64) and ARM64 (M1)) <https://github.com/ostefano/docker-misp>
 - ▶ <https://blogs.vmware.com/security/2023/01/how-to-deploy-a-threat-intelligence-platform-in-your-docker-environment.html>
- National Cyber and Information Security Agency of the Czech Republic <https://github.com/NUKIB/misp>
- CoolAcid's MISP images
<https://github.com/coolacid/docker-misp>
- MISP-docker by XME
<https://github.com/MISP/misp-docker>
- docker-misp by Harvard security
<https://github.com/MISP/docker-misp>

DISTRO OPTIONS

- Ubuntu 22.04 (20.04 will also work)
 - ▶ Our target platform
 - ▶ Our CI target
 - ▶ Use this unless you are absolutely forced not to
 - ▶ This is the platform we can support you with!
- CentOS 7
 - ▶ Annoying to operate
 - ▶ Less tested, though used by many
 - ▶ CentOS is dead. Consider other options
- RHEL 7
 - ▶ Same annoyance as CentOS in general
 - ▶ We test against CentOS in general, some assembly may be required

HARDWARE SPECS

- No firm recommendations, it's highly usage dependent
- It's better to go a bit over what you need than under
- **SSDs** are massively beneficial
- Let's look at what affects specs and some sample configurations

HARDWARE CONSIDERATIONS

- What are the factors that can impact my performance?
 - ▶ Clustering of the data (how many datapoints / event?) (RAM, disk speed)
 - ▶ Correlation (RAM, disk speed, disk space)
 - Consider blocking overtly correlating values from doing so
 - Feed ingestion strategy is crucial
 - ▶ Over-contextualisation (RAM, disk speed)
 - Tag/attach galaxies to the event instead of each attribute when possible

HARDWARE CONSIDERATIONS - CONTINUES

- What are the factors that can impact my performance?
 - ▶ Number of users that are active at any given time (RAM, CPU, disk speed)
 - ▶ Logging strategy (Disk space)
 - ▶ API users especially with heavy searches (substring searches for example) (RAM, CPU, Disk speed)

HARDWARE CONSIDERATIONS - CONTINUES

- What are the factors that generally do **NOT** impact my performance as much as expected?
 - ▶ Warninglist usage
 - ▶ Number of raw attributes on the instance
 - ▶ Number of sync connections / recurring syncs (with measure)
 - ▶ Tools feeding off the automation channels (ZMQ, kafka, syslog)

AUTHENTICATION OPTIONS

- Username/password is the default
- Some built in modules by 3rd parties (LDAP, Shibboleth, x509, OpenID, Azure Active Directory)
- CustomAuth system for more flexibility
- Additionally, consider Email OTP

OTHER CONSIDERATIONS - TUNING

- PHP tuning
 - ▶ Maximum memory usage (per process)
 - ▶ Timeout settings
 - ▶ Consider setting it per role!
 - ▶ Background processes are exempt
- MySQL: key buffer size is important
- Generally, tune for few heavy requests rather than many light ones

OTHER CONSIDERATIONS - HIGH AVAILABILITY

- Clustering
 - ▶ Load balanced apache servers with MISP
 - ▶ Replicating / mirrored database backends
- Careful about session pinning
- Attachment storage can be abstracted / network attached
- An example implementation for AWS
<https://github.com/oxtf/HAMISPA>

AN INTRODUCTION TO WORKFLOWS IN MISP

MISP - THREAT SHARING

CIRCL / TEAM MISP PROJECT

MISP PROJECT

<https://www.misp-project.org/>

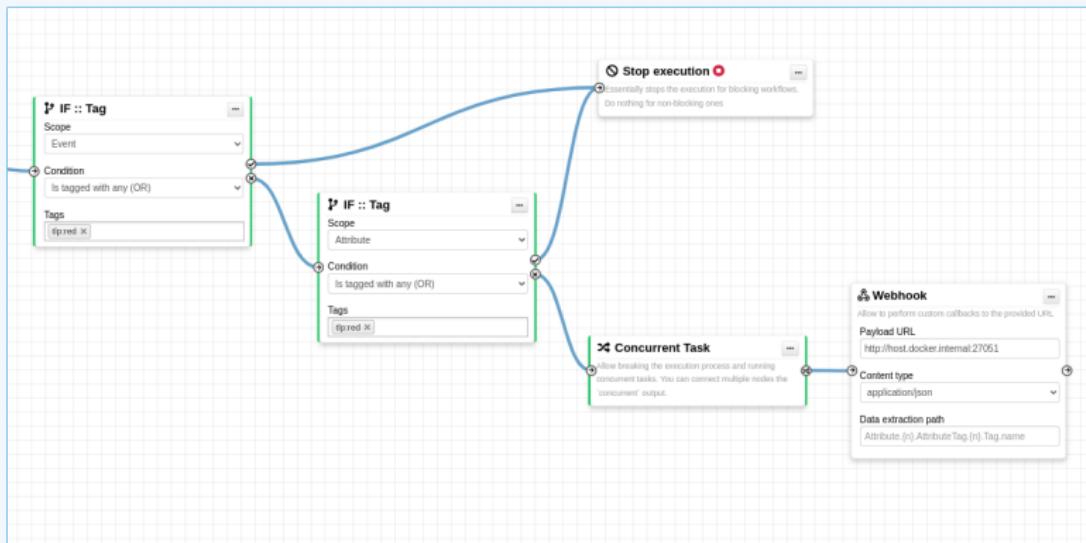
13TH ENISA-EC3 WORKSHOP



MISP
Threat Sharing

CONTENT OF THE PRESENTATION

- MISP Workflows fundamentals
- Getting started
- Design of the system & how it can be extended



WHAT PROBLEMS ARE WE TRYING TO TACKLE

- Initial idea came during GeekWeek^{7.5}¹



- Needs:

- ▶ Prevent default MISP behaviors
 - ▶ Hook specific actions to run callbacks

- Use-cases:

- ▶ Prevent publication of events not meeting some criterias
 - ▶ Prevent querying third-party services (e.g. virustotal) with sensitive information
 - ▶ Send notifications in a chat rooms
 - ▶ And much much more..

¹Workshop organized by the Canadian Cyber Center

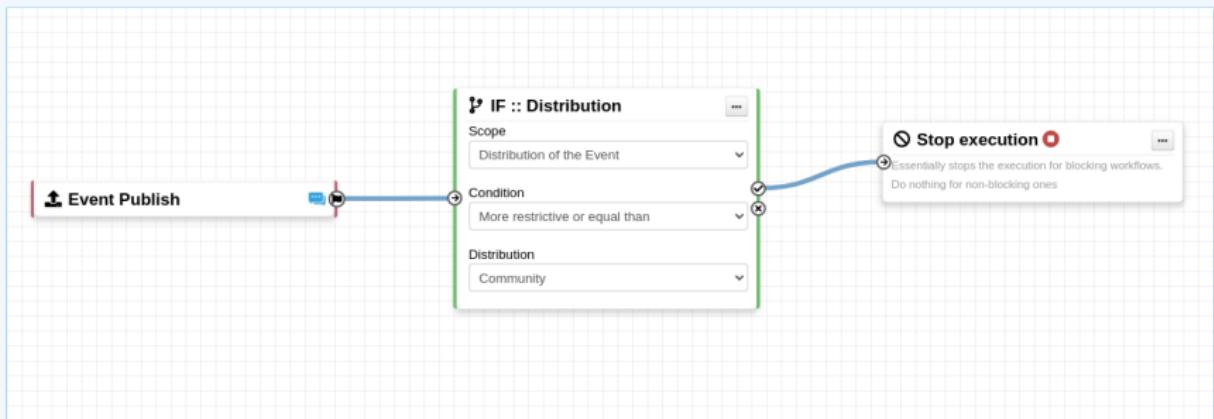
WORKFLOW - FUNDAMENTALS

SIMPLISTIC OVERVIEW OF A WORKFLOW IN ACTION

1. An **action** happens in MISP
2. If there is an **enabled** Workflow for that **action**, run it
3. If all went fine, MISP **continue** to perform the action
 - ▶ The operation can potentially be cancelled by blocking modules

TERMINOLOGY

- **workflow:** Sequence of all operations (nodes) to be executed. Basically the whole graph.
- **execution path:** A path composed of nodes
- **trigger:** Starting point of a workflow. Triggers are called when specific actions happen in MISP
 - ▶ A trigger can only have one workflow and vice-versa



WORKFLOW EXECUTION PROCESS

Typical execution process:

1. An action happens in MISP
2. The workflow associated to the trigger is ran
3. Execution result?
 - ▶ **success**: Continue the action
 - ▶ **failure** | **blocked**: Cancel the action

Example for Event publish:

1. An Event is about to be published
2. MISP executes the workflow listening to the event-publish trigger
 - ▶ **success**: Continue the publishing action
 - ▶ **failure** | **blocked**: Stop publishing and log the reason

BLOCKING AND NON-BLOCKING WORKFLOWS

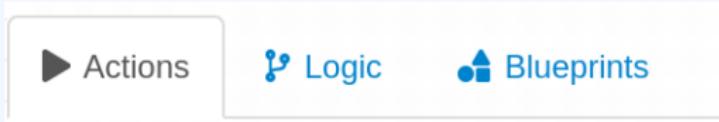
Currently 2 types of workflows:

- **Blocking:** Completion of the action can be prevented
 - ▶ If a **blocking module** blocks the action
 - ▶ If a **blocking module** raises an exception
- **Non-blocking:** Workflow execution outcome has no impact
 - ▶ **Blocking modules** can still stop the execution

EXECUTION CONTEXT

- Workflows can be triggered by **any users**
- Workflows can be triggered by actions done via the **UI or API**
- However, the user for which the workflow executes has:
 - ▶ The site-admin permission
 - ▶ Is from the MISP.host_org_id
- Ensures data is processed regardless of ownership and access: **no ACL**

CLASSES OF WORKFLOW MODULES



3 classes of modules

- **action:** Allow to execute functions, callbacks or scripts
 - ▶ Can stop execution
 - ▶ e.g. Webhook, block the execution, perform enrichments, ...
- **logic:** Allow to redirect the execution flow.
 - ▶ IF condition, fork the blocking execution into a non-blocking one, ...
- **blueprint:** Allow to reuse composition of modules
 - ▶ Can save subworkflows and its module's configuration

SOURCES OF WORKFLOW MODULES

3 sources of action modules

- Built-in **default** modules

- ▶ Part of the MISP codebase
- ▶ `app/Model/WorkflowModules/action/[module_name].php`

- User-defined **custom** modules

- ▶ Written in PHP
- ▶ Can extend existing default modules
- ▶ Can use MISP's built-in functionalities (restsearch, enrichment, push to zmq, ...)
- ▶ Faster and easier to implement new complex behaviors
- ▶ `app/Lib/WorkflowModules/action/[module_name].php`

SOURCES OF WORKFLOW MODULES

3 sources of action modules

- Modules from the **enrichment service**

- ▶ **Default** and **custom** modules
- ▶ From the *misp-module* 
- ▶ Written in Python
- ▶ Can use any python libraries
- ▶ New *misp-module* module type: action

→ Both the PHP and Python systems are **plug-and-play**

TRIGGERS CURRENTLY AVAILABLE

Currently 8 triggers can be hooked. 3 being blocking.

Trigger name	Scope	Trigger overhead	Description	Run counter	Blocking Workflow	MISP Core format	Workflow ID	Last Update	Enabled	Actions
(Attribute After Save)	attribute	high ⓘ	This trigger is called after an Attribute has been saved in the database	58	✗	✓	160	2022-07-29 06:58:11	✓	▶ ⏪ ⏴ ⏵ ⏹
(*) Enrichment Before Query	others	low	This trigger is called just before a query against the enrichment service is done	841	✓	✓	162	2022-07-29 08:32:32	✓	▶ ⏪ ⏴ ⏵ ⏹
(Event After Save)	event	medium ⓘ	This trigger is called after an Event has been saved in the database	11	✗	✓	175	2022-07-29 08:37:23	✓	▶ ⏪ ⏴ ⏵ ⏹
(Event Publish)	event	low	This trigger is called just before a MISP Event starts the publishing process	1	✓	✓	180	2022-07-29 12:14:10	✓	▶ ⏪ ⏴ ⏵ ⏹
(Object After Save)	object	high ⓘ	This trigger is called after an Object has been saved in the database	35	✗	✓	161	2022-07-28 13:59:37	✗	▶ ⏪ ⏴ ⏵ ⏹
(Post After Save)	post	low	This trigger is called after a Post has been saved in the database	36	✗	✗	176	2022-07-28 13:59:51	✓	▶ ⏪ ⏴ ⏵ ⏹
(User After Save)	user	low	This trigger is called after a user has been saved in the database	55	✗	✗	159	2022-07-28 14:00:03	✓	▶ ⏪ ⏴ ⏵ ⏹
(User Before Save)	user	low	This trigger is called just before a user is save in the database	42	✓	✗	158	2022-07-28 14:00:32	✓	▶ ⏪ ⏴ ⏵ ⏹

WORKFLOW - GETTING STARTED

GETTING STARTED WITH WORKFLOWS (1)

Review MISP settings:

1. Make sure `MISP.background_jobs` is turned on
2. Make sure workers are up-and-running and healthy
3. Turn the setting `Plugin.Workflow_enable` on

Overview MISP settings (20) Encryption settings (7) Proxy settings (5) Security settings (6) Plugin settings (465) SimpleBackgroundJobs settings (11) Diagn			
Enrichment			
Import			
Export			
Action			
Critical	Plugin.Action_services_enable	true	Enabled/disable the action services
Recommended	Plugin.Action_services_url	http://host.docker.internal	The url used to access the action services. By default, it is accessible at http://127.0.0.1:6666
Recommended	Plugin.Action_services_port	6677	The port used to access the action services. By default, it is accessible at 127.0.0.1:6666
Recommended	Plugin.Action_timeout	10	Set a timeout for the action services
			Value not set.

4. [optional:misp-module] Turn the setting `Plugin.Action_services_enable` on

Overview MISP settings (20) Encryption settings (7) Proxy settings (5) Security settings (6) Plugin settings (465) SimpleBackgroundJobs settings (11) Diagn			
Enrichment			
Import			
Export			
Action			
Cortex			
Sightings			
Workflow			
Recommended	Plugin.Workflow_enable	true	Enable/disable workflow feature

GETTING STARTED WITH WORKFLOWS (2)

If you wish to use action modules from misp-module, make sure to have:

- The latest update of misp-module
 - ▶ There should be an `action_mod` module type in `misp-modules/misp_modules/modules`
- Restarted your misp-module application

```
1 # This command should show all 'action' modules
2 $ curl -s http://127.0.0.1:6666/modules | \
3 jq '.[] | select(.meta.module-type == "action") | \
4 {name: .name, version: .meta.version}'
```

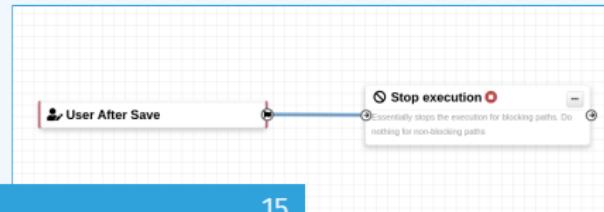
GETTING STARTED WITH WORKFLOWS (3)

1. Go to the list of modules
 - ▶ Administration > Workflows > List Modules
 - ▶ or /workflows/moduleIndex
2. Make sure **default** modules are loaded
3. [optional:misp-module] Make sure **misp-module** modules are loaded

CREATING A WORKFLOW WITH THE EDITOR

1. Go to the list of triggers Administration > Workflows
2. Enable and edit a trigger from the list
3. Drag an action module from the side panel to the canvas
4. From the trigger output, drag an arrow into the action's input (left side)
5. Execute the action that would run the trigger and observe the effect!

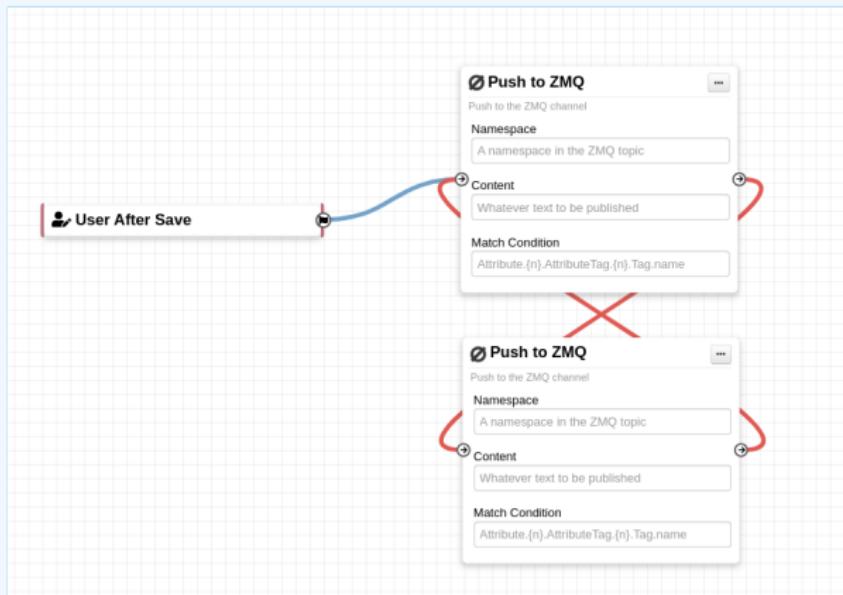
Trigger name	Scope	Trigger overhead	Description	Run counter	Blocking Workflow	MISP Core format	Workflow ID	Last Update	Enabled	Actions
Attribute After Save	attribute	high	This trigger is called after an Attribute has been saved in the database	58	x	✓	160	2022-07-29 06:58:11	✓	■ ⓘ ⓘ
Enrichment Before Query	others	low	This trigger is called just before a query against the enrichment service is done	841	✓	✓	162	2022-07-29 08:32:32	✓	■ ⓘ ⓘ
Event After Save	event	medium	This trigger is called after an Event has been saved in the database	11	x	✓	175	2022-07-29 08:37:23	✓	■ ⓘ ⓘ
Event Publish	event	low	This trigger is called just before a MISP Event starts the publishing process	1	✓	✓	180	2022-07-29 12:14:10	✓	■ ⓘ ⓘ
Object After Save	object	high	This trigger is called after an Object has been saved in the database	35	x	✓	161	2022-07-28 13:59:37	x	▶ ⓘ ⓘ
Post After Save	post	low	This trigger is called after a Post has been saved in the database	36	x	x	176	2022-07-28 13:59:31	✓	■ ⓘ ⓘ
User After Save	user	low	This trigger is called after a user has been saved in the database	55	x	x	159	2022-07-28 14:00:03	✓	■ ⓘ ⓘ
User Before Save	user	low	This trigger is called just before a user is save in the database	42	✓	x	158	2022-07-28 14:00:32	✓	■ ⓘ ⓘ



WORKING WITH THE EDITOR

Operations not allowed:

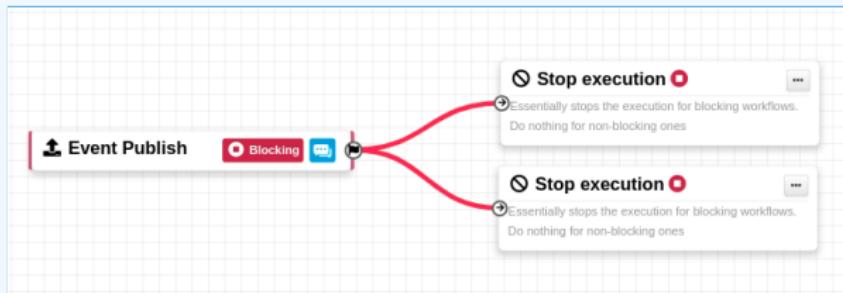
- Execution loop are not authorized
 - ▶ Current caveat: If an action re-run the workflow in any way



WORKING WITH THE EDITOR

Operations not allowed:

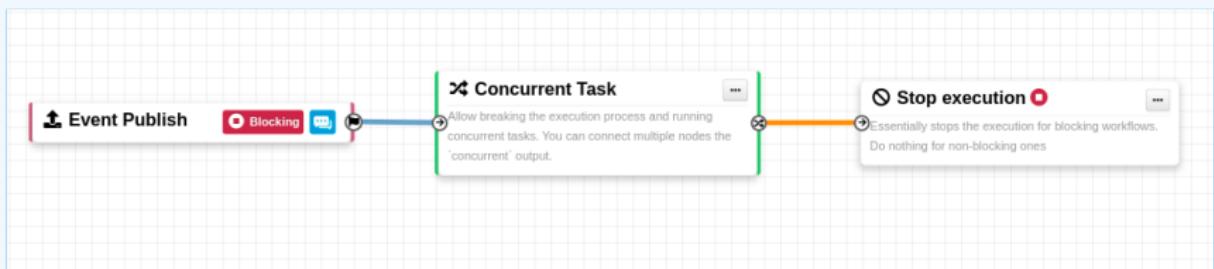
- Multiple connections from the same output
 - ▶ Execution order not guaranteed and confusing for users



WORKING WITH THE EDITOR

Operations showing a warning:

- Blocking modules after a **concurrent tasks** module
- Blocking modules in a **non-blocking** workflow



WORKFLOW BLUEPRINTS

1. Blueprints allow to **re-use parts** of a workflow in another one
2. Blueprints can be saved, exported and **shared**

Debugging webhook v1656059209

9ff210dd-ee7e-49c8-a5af-10cd42cdadb6

Default: **X**

Blueprint Content: **1 node**

 1

Webhook module pre-configured for debugging purposes

Blueprints origins:

1. From the "official" `misp-workflow-blueprints` repository
2. Created or imported by users

WORKFLOW BLUEPRINTS: CREATE

Select one or more modules to be saved as blueprint then click on the save blueprint button

The screenshot shows the 'Workflow: publish' interface with the 'Blueprints' tab selected. On the left, there are several workflow parts listed:

- Workflow part 1**: Blueprint Content: 3 nodes. Contains nodes 1, 2, and 3.
- Workflow part 2 with a super long text**: Blueprint Content: 3 nodes. Contains nodes 1, 2, and 3.
- Workflow part 2 with a super long text**: Blueprint Content: 7 nodes. Contains nodes 1 through 7.
- Debugging webhook**: Blueprint Content: 1 node. Contains node 1.
- part3**: Blueprint Content: 2 nodes. Contains nodes 1 and 2.
- Mattemost module configuration**: Blueprint Content: 1 node. Contains node 1.

A central modal window titled 'Add Workflow Blueprint' is open, prompting for a 'Name' (Name of the workflow blueprint) and a 'Description' (Concise description of the workflow blueprint). Below the modal, a 'Workflow Blueprint Content' section lists the available node types:

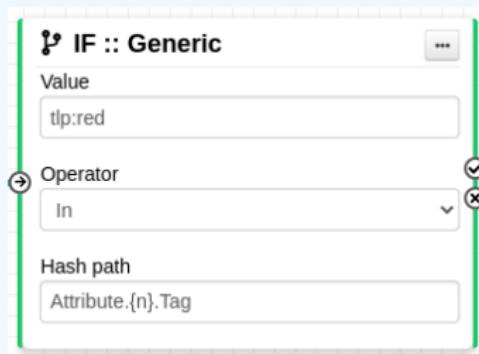
- Parallel Task
 - Has filter
- Push to ZMQ
 - Has filter
 - Has parameters
- Push to ZMQ
 - Has filter
 - Has parameters
- Push to ZMQ
 - Has filter
 - Has parameters
- Stop execution
 - Has filter
- Push to ZMQ
 - Has filter
 - Has parameters
- Webhook

At the bottom of the modal are 'Submit' and 'Cancel' buttons.

HASH PATH FILTERING

- Some modules have the possibility to filter or check conditions using CakePHP's path expression.

```
1 $path_expression = '{n}[name=fred].id';
2 $users = [
3     {'id': 123, 'name': 'fred', 'surname': 'bloggs'},
4     {'id': 245, 'name': 'fred', 'surname': 'smith'},
5     {'id': 356, 'name': 'joe', 'surname': 'smith'},
6 ];
7 $ids = Hash::extract($users, $path_expression);
8 // => $ids will be [123, 245]
```



MODULE FILTERING

- Some action modules accept **filtering** conditions
- E.g. the enrich-event module will only perform the enrichment on Attributes having a tlp:white Tag

Module Filtering

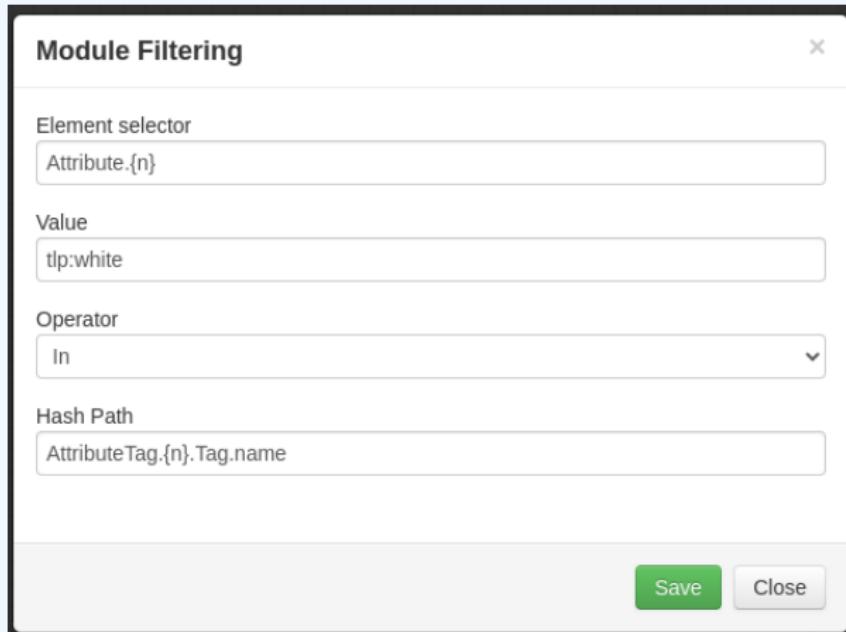
Element selector
Attribute.{n}

Value
tlp:white

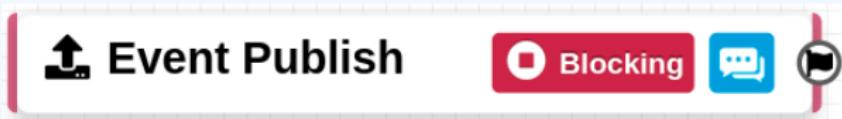
Operator
In

Hash Path
AttributeTag.{n}.Tag.name

Save **Close**



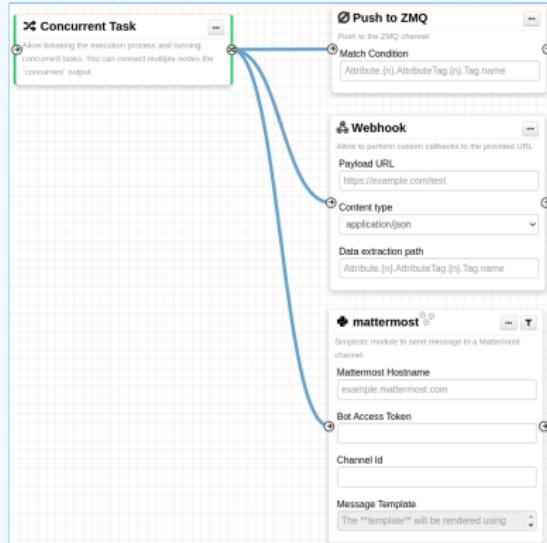
DATA FORMAT IN WORKFLOWS



- All triggers will inject data in a workflow
- In some cases, there is no format (e.g. User after-save)
- In others, the format is **compliant with the MISP Core format**
- In addition to the RFC, the passed data has **additional properties**
 - ▶ Attributes are **always encapsulated** in the Event or Object
 - ▶ Additional key **_AttributeFlattened**
 - ▶ Additional key **_allTags**
 - ▶ Additional key **inherited** for Tags

LOGIC MODULE: CONCURRENT TASK

- Special type of **logic** module allowing multiple connections
- Allows **breaking the execution** flow into a concurrent tasks to be executed later on by a background worker
- As a side effect, blocking modules **cannot cancel** ongoing operations



DEBUGGING WORKFLOWS: LOG ENTRIES

- Workflow execution is logged in the application logs:
 - ▶ `/admin/logs/index`
- Or stored on disk in the following file:
 - ▶ `/app/tmp/logs/workflow-execution.log`
- Use the `webhook-listener.py` tool
 - ▶ `/app/tools/misp-workflows/webhook-listener.py`

Logs

The screenshot shows a table of log entries. At the top, there are navigation buttons: '« previous' and 'next »'. Below that is a header row with tabs: 'Emails', 'Authentication issues', 'MISP Update results', 'Setting changes', and 'Warnings and errors'. The 'Emails' tab is currently selected and highlighted in black. The table has a header row with columns: 'Id ↑', 'Email', 'Org', 'Created', 'Model', 'Model ID', 'Action', and 'Title'. There are two data rows:

Id ↑	Email	Org	Created	Model	Model ID	Action	Title
49146	SYSTEM	SYSTEM	2022-08-01 07:34:40	Workflow	162	execute_workflow	Finished executing workflow for trigger 'enrichment-before-query' (162). Outcome: success
49144	SYSTEM	SYSTEM	2022-08-01 07:34:39	Workflow	162	execute_workflow	Started executing workflow for trigger 'enrichment-before-query' (162)

DEBUGGING WORKFLOWS: DEBUG MODE

- The  Debug Mode: On can be turned on for each workflows
- Each nodes will send data to the provided URL
 - ▶ Configure the setting: `Plugin.Workflow_debug_url`
- Result can be visualized in
 - ▶ **offline:** `tools/misp-workflows/webhook-listener.py`
 - ▶ **online:** `requestbin.com` or similar websites

Today		
2:25:10 pm	POST	<code>/end?outcome=blocked</code>
2:25:09 pm	POST	<code>/exec/stop-execution?result=success</code>
2:25:09 pm	POST	<code>/exec/tag-if?result=success</code>
2:25:08 pm	POST	<code>/init?type=blocking</code>

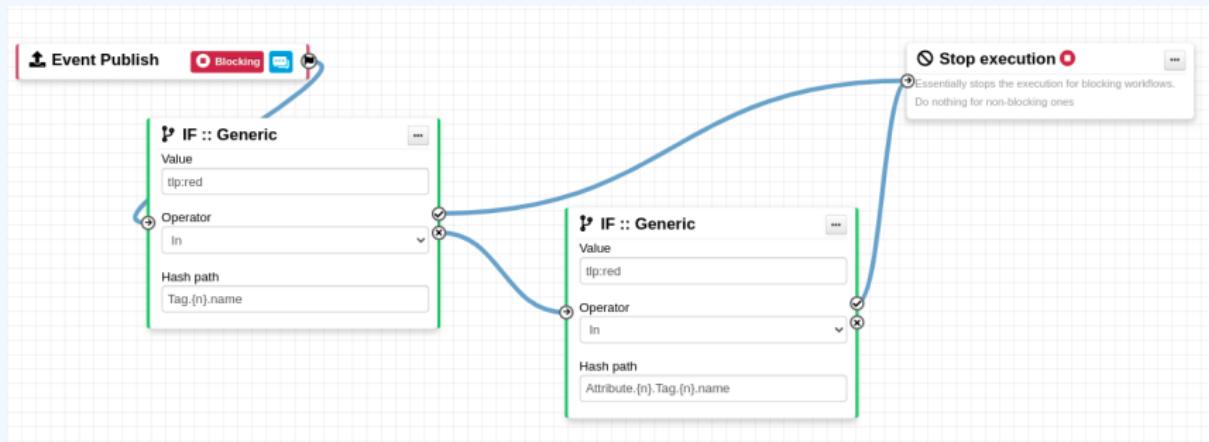
LEARNING BY EXAMPLES

WORKFLOW EXAMPLE 1



1. The Event-Publish trigger uses the MISP core format
2. The IF::Tag module checks if at least one of the Attribute has the tlp:white tag
3. If it does, the Push-to-ZMQ module will be executed

WORKFLOW EXAMPLE 2



- If an event has the tlp:red tag or any of the attribute has it, the publish process will be cancelled

EXTENDING THE SYSTEM

CREATING A NEW MODULE IN PHP

```
app > Lib > WorkflowModules > action > Module_blueprint_action_module.php > ...
1  <?php
2  include_once APP . 'Model/WorkflowModules/WorkflowBaseModule.php';
3
4  class Module_blueprint_action_module extends WorkflowBaseModule
5  {
6      public $is_blocking = false;
7      public $disabled = true;
8      public $id = 'blueprint-action-module';
9      public $name = 'Blueprint action module';
10     public $description = 'Lorem ipsum dolor, sit amet consectetur adipisicing elit.';
11     public $icon = 'shapes';
12     public $inputs = 1;
13     public $outputs = 1;
14     public $params = [];
15
16     public function exec(array $node, WorkflowRoamingData $roamingData, array &$errors = [])
17     : bool
18     {
19         parent::exec($node, $roamingData, $errors);
20         // If $this->is_blocking == true, returning 'false' will stop the execution.
21         $errors[] = __('Execution stopped');
22         return false;
23     }
}
```

- **app/Lib/WorkflowModules/action/[module_name].php**
- Module configuration are defined as public variables
- The exec function has to be implemented.
 - ▶ If it returns **true**, execution will proceed
 - ▶ If it returns **false**
 - And the module is blocking, the execution will stop and the operation will be blocked

CREATING A NEW MODULE IN PYTHON

```
home > sami > git > misp-modules > misp_modules > modules > action_mod > testaction.py > ...
1 > import json
2
3
4 misperrors = {'error': 'Error'}
5
6 # config fields that your code expects from the site admin
7 moduleconfig = {
8     'foo': {
9         'type': 'string',
10        'description': 'blablabla',
11        'value': 'xyz'
12    },
13    'bar': {
14        'type': 'string',
15        'value': 'meh'
16    }
17};
18
19 # blocking modules break the execution of the chain of actions (such as publishing)
20 blocking = False
21
22 # returns either "boolean" or "data"
23 # Boolean is used to simply signal that the execution has finished.
24 # For blocking modules the actual boolean value determines whether we break execution
25 returns = 'boolean'
26
27 moduleinfo = {'version': '0.1', 'author': 'Andras Iklody',
28               'description': 'This module is merely a test, always returning true. Triggers on event publishing.',
29               'module-type': ['action']}
30
31
32 def handler(q=False):
33     if q is False:
34         return False
35     result = json.loads(q) # noqa
36     output = result # Insert your magic here!
37     r = {'data': output}
38     return r
39
40
41 > def introspection():
42
```

- Module configuration are defined in the `moduleinfo` and `moduleconfig` variables
- The `handler` function has to be implemented.
- Blocking logic is the same as other modules

AUTOMATION WITH WORKFLOWS IN MISP

SHORT VERSION

SAMI MOKADDEM

MISP PROJECT

<https://www.misp-project.org/>



1. Automation in MISP

2. MISP Workflows

- ▶ Fundamentals
- ▶ Demo with examples
- ▶ Using the system
- ▶ How it can be extended

AUTOMATION IN MISP: WHAT ALREADY EXISTS?



MISP API / PyMISP

- Needs CRON Jobs in place
- Potentially heavy for the server
- Not realtime



PubSub channels

- After the actions happen: No feedback to MISP
- Tougher to put in place & to share
- Full integration amounts to develop a new tool

- No way to **prevent** behavior
- Difficult to setup **hooks** to execute callbacks

SIMPLE AUTOMATION IN MISP MADE EASY



- **Visual** dataflow programming
- **Drag & Drop** editor
- Flexible **Plug & Play** system
- Share workflows, **debug** and **replay**

EXAMPLE OF USE-CASES

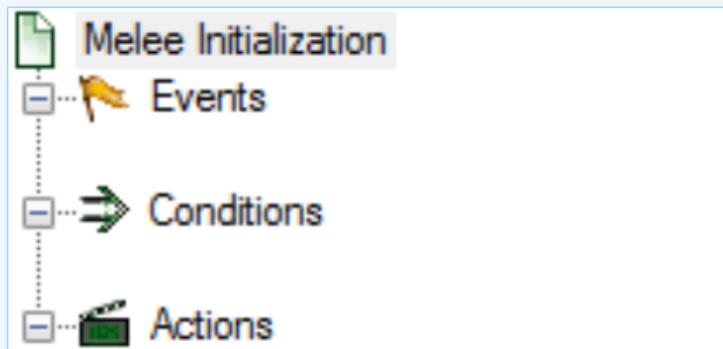
- **Notification** on specific actions
 - ▶ New events matching criteria
 - ▶ New users
 - ▶ Automated alerts for high-priority IOCs
- **Extend** existing MISP behavior
 - ▶ Push data to another system
 - ▶ Automatic enrichment
 - ▶ Sanity check to block publishing / sharing
 - ▶ Curation pipelines
- **Hook** capabilities
 - ▶ Assign tasks and notify incident response team members
- ...

WORKFLOW - FUNDAMENTALS

Objective: Start with the foundation to understand the basics



HOW DOES IT WORK



1. An **event** happens in MISP
2. (*optional*) Check if all **conditions** are satisfied
3. Execute all **actions**
 - ▶ May prevent MISP to complete its original event

WHAT KIND OF EVENTS?

Events

- New MISP Event
- Attribute has been saved
- New discussion post
- New user created
- Query against third-party services
- ...

- ② Supported events in MISP are called **Triggers**
- ② A **Trigger** is associated with **1-and-only-1 Workflow**

TRIGGERS CURRENTLY AVAILABLE

Currently 11 triggers can be hooked. 3 being Blocking.

Flags Triggers

List the available triggers that can be listened to by workflows.

Missing a trigger? Feel free to open a Github issue!

Documentation and concepts

« previous | next »

All	attribute	event	log	object	others	post	user	Blocking	Enabled	Disabled	
Trigger name	Scope	Trigger overhead	Run counter	Blocking	Workflow	MISP Core format	Workflow ID	Last Update	Debug enabled	Enabled	Actions
Attribute After Save	attribute	high	110				160	2023-09-14 06:54:37	<input type="checkbox"/>		
* Enrichment Before Query	others	low	2226				162	2023-10-09 07:56:42	<input type="checkbox"/>		
Event After Save	event	high	191				175	2023-10-02 14:55:19	<input type="checkbox"/>		
Event After Save New	event	low	7				182	2023-03-16 14:05:07	<input type="checkbox"/>		
Event After Save New From Pull	event	low	6				183	2023-10-09 07:57:02	<input type="checkbox"/>		
Event Publish	event	low	2				188	2023-10-09 07:56:25	<input type="checkbox"/>		
Log After Save	log	high	0				185	2023-06-05 13:26:50	<input type="checkbox"/>		
Object After Save	object	high	35				161	2023-06-05 13:27:00	<input type="checkbox"/>		
Post After Save	post	low	36				176	2022-07-28 13:59:51	<input type="checkbox"/>		
User After Save	user	low	0				181	2022-08-05 07:19:46	<input type="checkbox"/>		
User Before Save	user	low	42				158	2023-06-05 13:27:25	<input type="checkbox"/>		

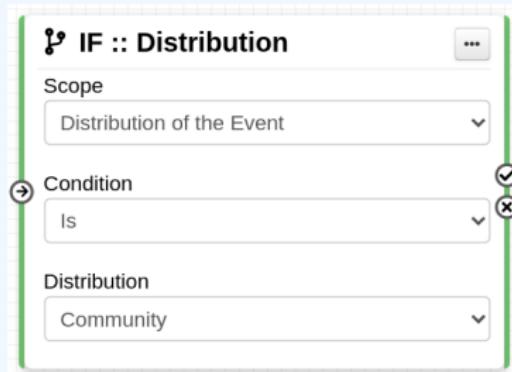
Page 1 of 1, showing 1 records out of 11 total, starting on record 1, ending on 11

WHAT KIND OF CONDITIONS?

→ Conditions

- A MISP Event is tagged with tlp:red
- The distribution of an Attribute is a sharing group
- The creator organisation is circl.lu
- Or any other **generic** conditions

❓ These are also called **Logic modules**



WORKFLOW - LOGIC MODULES

- ➔ logic modules: Allow to redirect the execution flow.
 - ▶ IF conditions
 - ▶ Delay execution

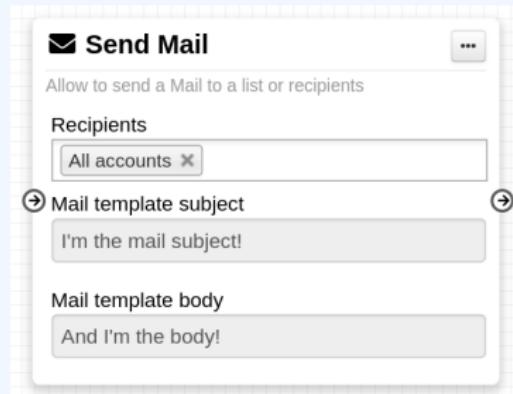
All	Action	Logic	misp-module	Custom	Blocking	Enabled	Disabled	Enter value to search	Filter	X	
					Type	Blocking	MISP Core format	misp-module	Custom	Enabled	Actions
<input type="checkbox"/>	Module name										
<input type="checkbox"/>	(Blueprint logic module)				logic	✗	✗	✗	✓	✗	▶ ⚡
<input type="checkbox"/>	.concurrent Task				logic	✗	✗	✗	✗	✓	■ ⚡
<input type="checkbox"/>	IF :: Distribution				logic	✗	✓	✗	✗	✓	■ ⚡
<input type="checkbox"/>	Filter :: Generic				logic	✗	✗	✗	✗	✗	▶ ⚡
<input type="checkbox"/>	Filter :: Remove filter				logic	✗	✗	✗	✗	✗	▶ ⚡
<input type="checkbox"/>	IF :: Generic				logic	✗	✗	✗	✗	✓	■ ⚡
<input type="checkbox"/>	IF :: Organisation				logic	✗	✓	✗	✗	✓	■ ⚡
<input type="checkbox"/>	IF :: Published				logic	✗	✓	✗	✗	✓	■ ⚡
<input type="checkbox"/>	IF :: Tag				logic	✗	✓	✗	✗	✓	■ ⚡
<input type="checkbox"/>	IF :: Threat Level				logic	✗	✗	✗	✗	✗	▶ ⚡

WHAT KIND OF ACTIONS?

Actions

- Send an email notification
- Perform enrichments
- Send a chat message on MS Teams
- Attach a local tag
- ...

 These are also called **Action modules**



WORKFLOW - ACTION MODULES

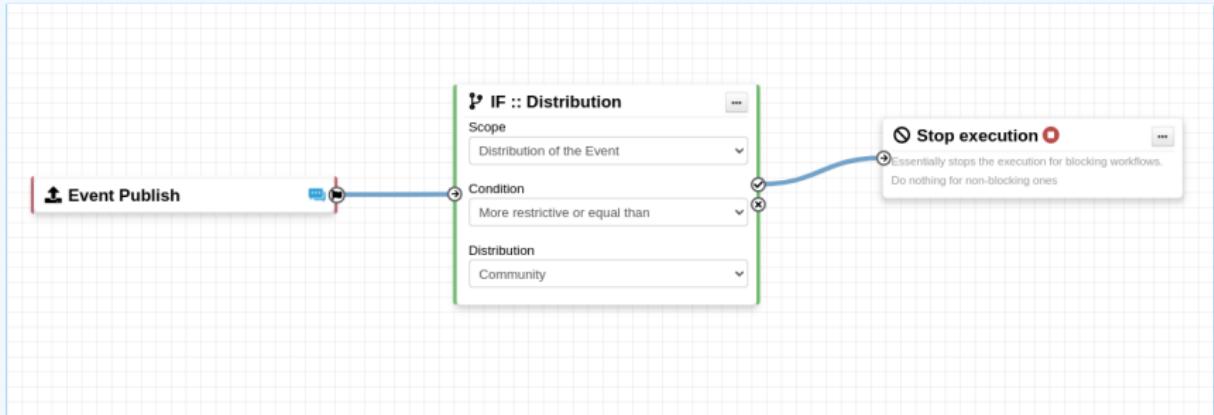
■ action modules: Allow to execute operations

- ▶ Tag operations
- ▶ Send notifications
- ▶ Webhooks & Custom scripts

All	Action	Logic	misp-module	Custom	Blocking	Enabled	Disabled	Enter value to search	Filter	X
Module name		Type	Blocking	MISP Core format	misp-module	Custom	Enabled	Actions		
<input type="checkbox"/>	* Attach enrichment	action	x	✓	x	x	✓			
<input type="checkbox"/>	 Attribute edition operation	action	x	✓	x	x	✓			
<input type="checkbox"/>	 Attribute IDS Flag operation	action	x	✓	x	x	✓			
<input type="checkbox"/>	 Blueprint action module	action	x	x	x	✓	✓			
<input type="checkbox"/>	* Enrich Event	action	x	✓	x	x	✓			
<input type="checkbox"/>	 mattermost	action	x	x	✓	x	✓			
<input type="checkbox"/>	 MS Teams Webhook	action	x	x	x	x	✓			
<input type="checkbox"/>	 Push to ZMQ	action	x	x	x	x	✓			
<input type="checkbox"/>	 Send Log Mail	action	x	x	x	x	x			
<input type="checkbox"/>	 Send Mail	action	x	x	x	x	✓			
<input type="checkbox"/>	> Splunk HEC export	action	x	✓	x	x	x			
<input type="checkbox"/>	 Stop execution	action	✓	x	x	x	✓			
<input type="checkbox"/>	 Tag operation	action	x	✓	x	x	✓			
<input type="checkbox"/>	 testaction	action	x	x	✓	x	✓			
<input type="checkbox"/>	 Webhook	action	x	x	x	x	✓			

WHAT IS A MISP WORKFLOW?

- Sequence of all nodes to be executed in a specific order
- Workflows can be enabled / disabled
- A Workflow is associated to **1-and-only-1 trigger**



SOURCES OF WORKFLOW MODULES (o)

Currently 36 built-in modules.

- **Trigger** module (11): built-in **only**
 - ▶ Get in touch if you want more
- **Logic** module (10): built-in & **custom**
- **Action** module (20): built-in & **custom**

SOURCES OF WORKFLOW MODULES (1)

■ Built-in **default** modules

- ▶ Part of the MISP codebase
- ▶ Get in touch if you want us to increase the selection (or merge PR!)



SOURCES OF WORKFLOW MODULES (2)

User-defined **custom** modules

- Written in PHP
- Extend existing modules
- MISP code reuse



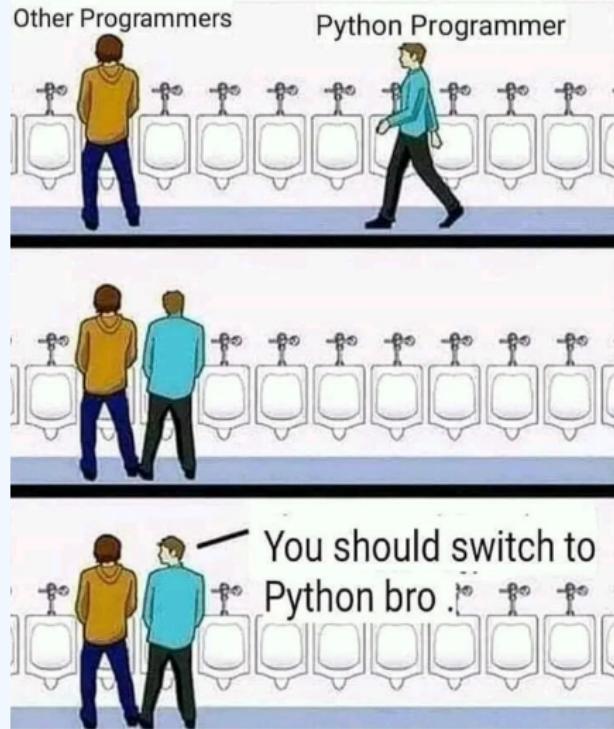
SOURCES OF WORKFLOW MODULES (3)

Modules from the

misp-module^{⊗⊗}

enrichment service

- Written in Python
- Can use any python libraries
- Plug & Play

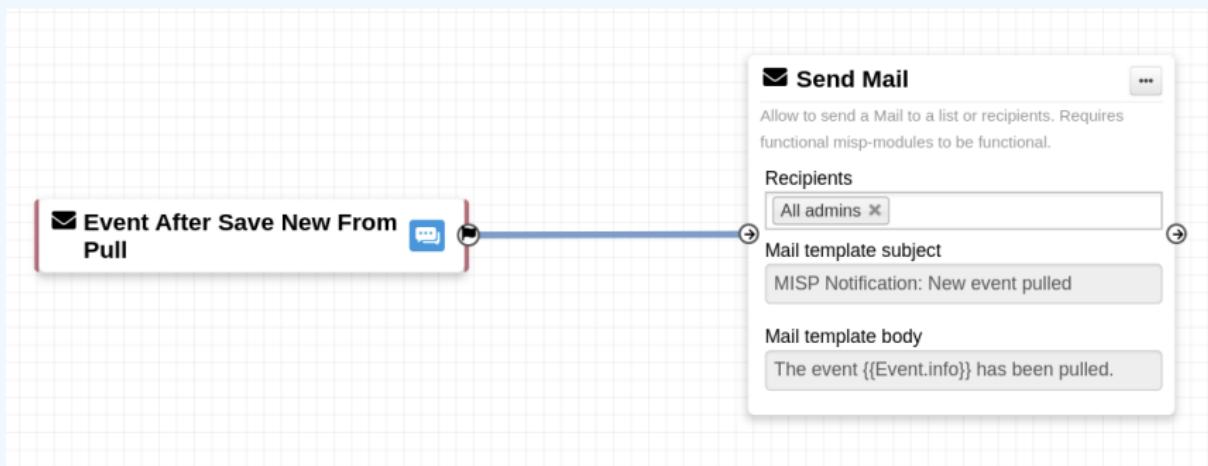


DEMO BY EXAMPLES

- WF-1. Send an email to **all admins** when a new event has been pulled

- WF-2. Block queries on 3rd party services when **tlp:red** or **PAP:red**
 - ▶ **tlp:red**: For the eyes and ears of individual recipients only
 - ▶ **PAP:RED**: Only passive actions that are not detectable from the outside

DEMO WF-1: SEND AN EMAIL TO **ALL ADMINS** WHEN A NEW EVENT HAS BEEN PULLED



DEMO WF-2: BLOCK QUERIES ON 3RD PARTY SERVICES WHEN TLP:RED OR PAP:RED

- **tlp:red:** For the eyes and ears of individual recipients only
- **PAP:RED:** Only passive actions that are not detectable from the outside



GETTING STARTED WITH WORKFLOWS

Everything is ready?

Let's see how to build a workflow!



CREATING A WORKFLOW WITH THE EDITOR

1. Prevent event publication if tlp:red tag
 - ▶ Send a mail to admin@admin.test about potential data leak
2. else, send a notification on Mattermost

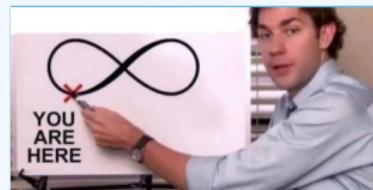
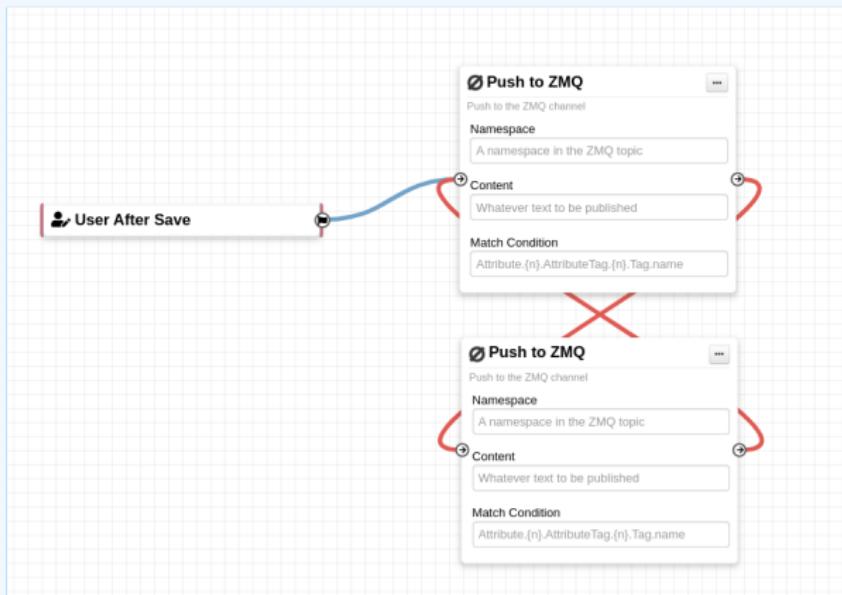
CONSIDERATIONS WHEN WORKING WITH WORKFLOWS

Objective: Overview of some common pitfalls

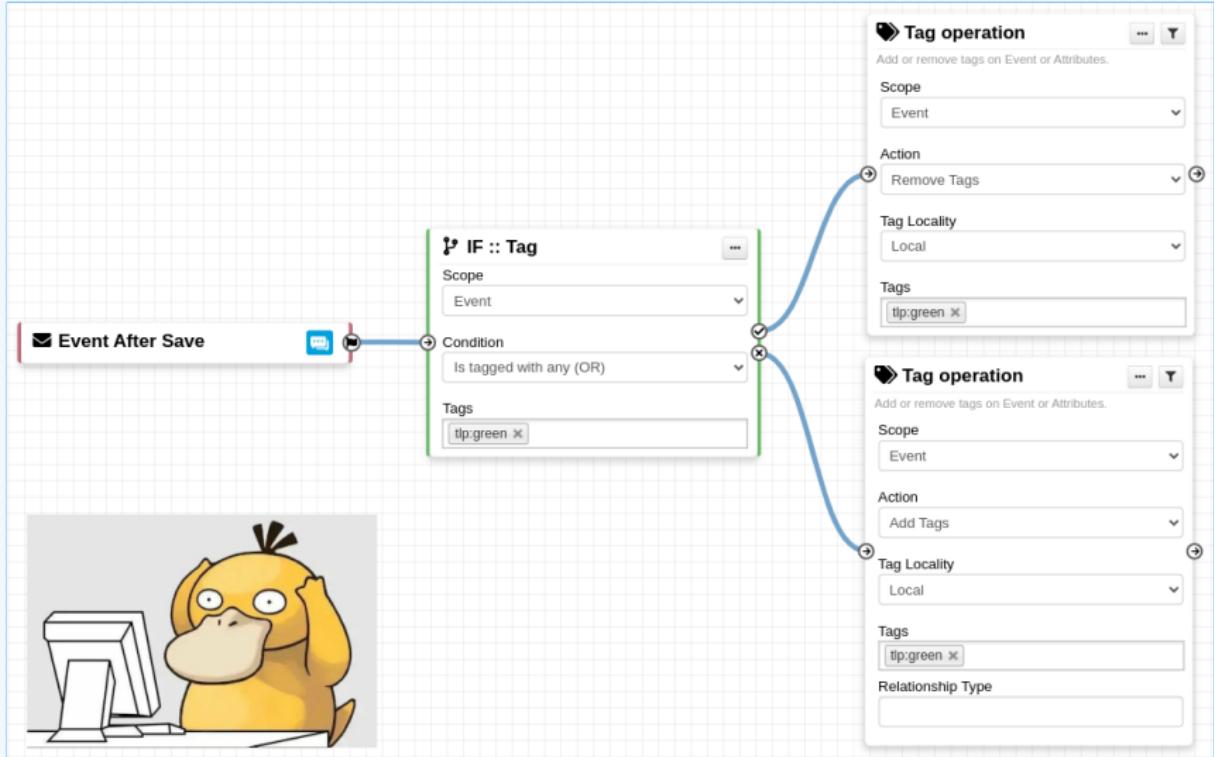


WORKING WITH THE EDITOR - OPERATIONS NOT ALLOWED

Execution loop are not authorized

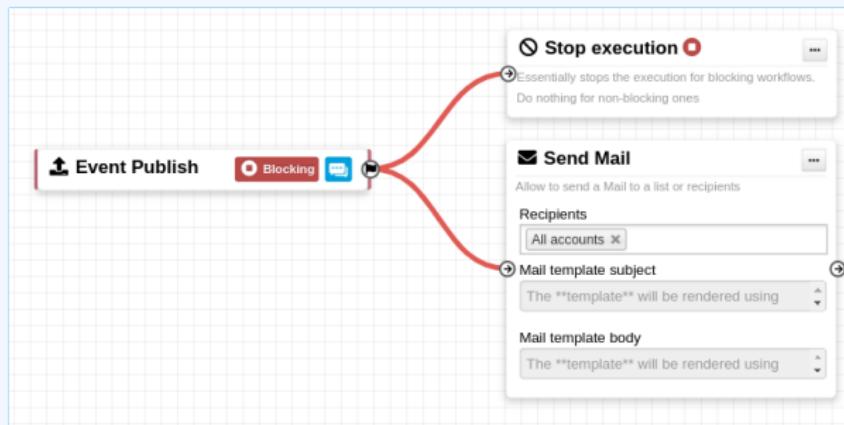


RECURSIVE WORKFLOWS



WORKING WITH THE EDITOR - OPERATIONS NOT ALLOWED

Multiple connections from the same output



- Execution order not guaranteed
- Confusing for users

ADVANCED USAGE

Objective: Overview of Blueprints, Data format and Filtering

WORKFLOW BLUEPRINTS

1. Blueprints allow to **re-use parts** of a workflow in another one
2. Blueprints can be saved, exported and **shared**

Debugging webhook v1656059209

9ff210dd-ee7e-49c8-a5af-10cd42cdadb6

Default: **X**

Blueprint Content: **1 node**

 1

Webhook module pre-configured for debugging purposes

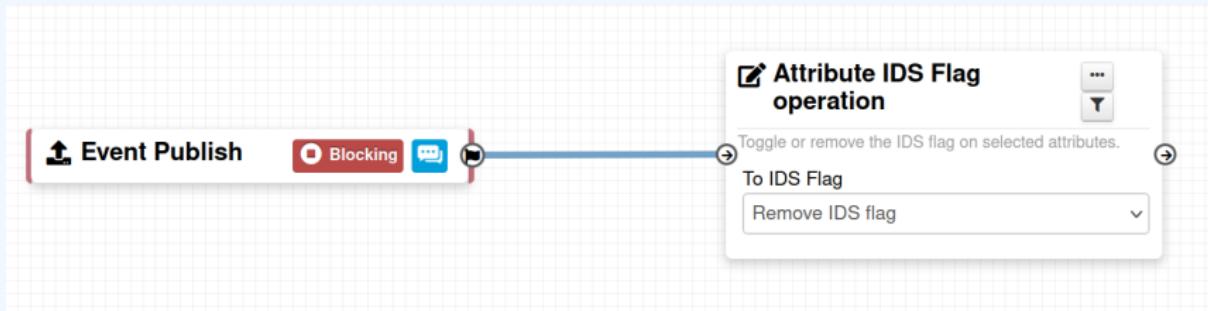
Blueprints sources: MISP/misp-workflow-blueprints repository¹

- Block actions if any attributes have the PAP:RED or tlp:red tag
- Curation pipeline
- Enrich data from 3rd-party

¹<https://github.com/MISP/misp-workflow-blueprints>

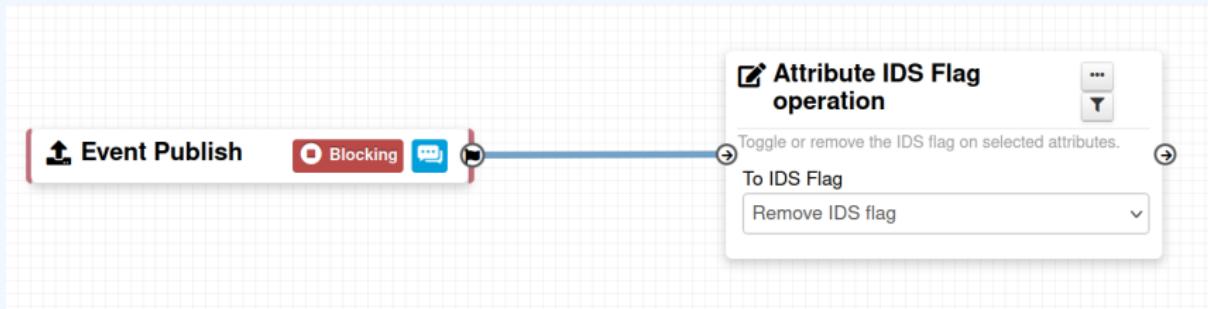
FITLERING DATA ON WHICH TO APPLY A MODULE

What is the outcome of executing this workflow?



FITLERING DATA ON WHICH TO APPLY A MODULE

What is the outcome of executing this workflow?

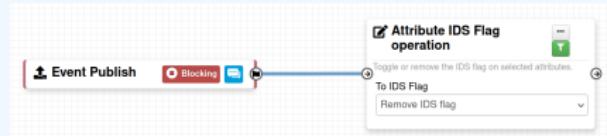


All Attributes get their to_ids turned off.

How could we force that action only on Attribute of type comment?

→ Hash path filtering!

FITLERING DATA ON WHICH TO APPLY A MODULE



Node Filtering

Element selector
Event._AttributeFlattened.{n}

Value
comment

Operator
In

Hash Path
type

FITLERING DATA ON WHICH TO APPLY A MODULE



Node Filtering

Element selector

Event._AttributeFlattened.{n}

Select elements on which
to apply the filtering

Value

comment

Fixed value

Operator

In

Comparison operator

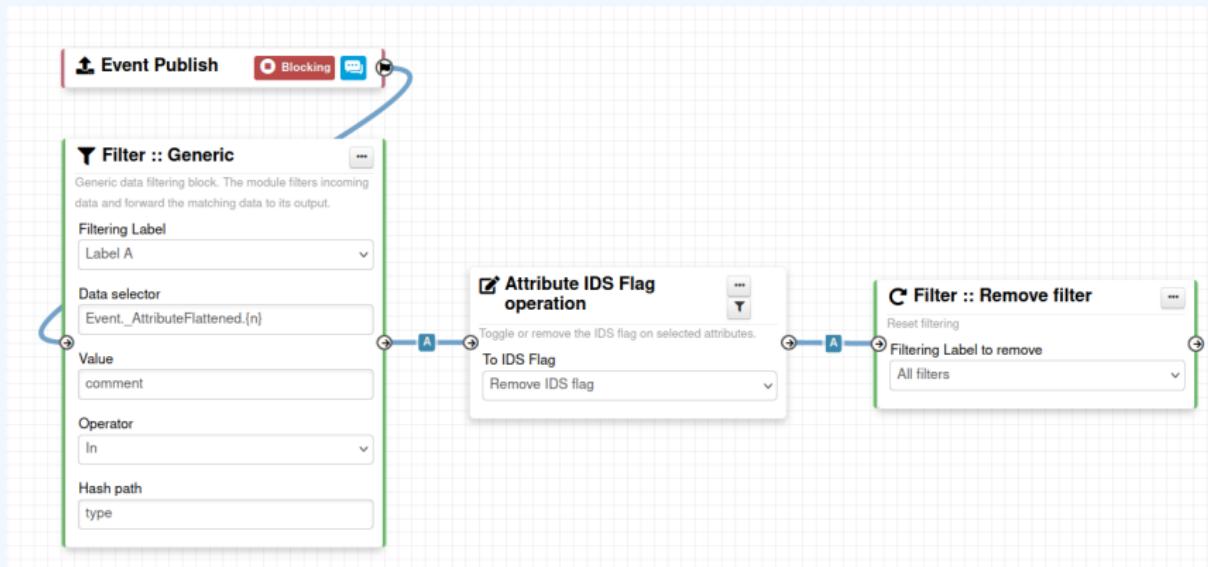
Hash Path

type

Data point to get the value

FITLERING DATA ON WHICH TO APPLY ON MULTIPLE MODULES

New feature as of **v2.4.171** allows setting filters on a path.



SHOULD I MIGRATE TO MISP WORKFLOWS

I have automation in place using the API/ZMQ. Should I move to Workflows?

- I have a curation pipeline using the API, should I port it to workflows?
 - ▶ **No** in general, but WF can be used to start the curation process or perform simple pre-processing
- What if I want to **block** some actions
 - ▶ Put the blocking logic in the WF, keep the remaining outside
- Bottom line is **Keep it simple** for you to maintain

FUTURE WORKS

- More 📽️ modules
- More ➔ modules
- More 🚨 triggers
- Recursion prevention system

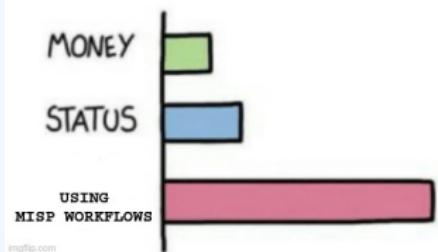


imgflip.com

FINAL WORDS

- Designed to **quickly** and **cheaply** integrate MISP in CTI pipelines
- **Beta** Feature unlikely to change.
But still..
- Waiting for feedback!
 - ▶ New triggers?
 - ▶ New modules?

WHAT GIVES PEOPLE
FEELINGS OF POWER



imgflip.com

MISP-STIX PROJECT

PYTHON LIBRARY TO CONVERT MISP <-> STIX

MISP CORE TEAM

TLP:WHITE

MISP PROJECT

<https://www.misp-project.org/>

MISP TRAINING



- Built-in integration
 - ▶ Available from the UI
 - ▶ Accessible via restSearch
- Export & Import features
 - ▶ Export MISP data collections
 - ▶ Import STIX files
- Supported version
 - ▶ STIX 1.1.1 & 1.2
 - ▶ STIX 2.0 & 2.1

MISP-STIX - KEY FEATURES

- MISP ↔ STIX conversion
 - ▶ Used by MISP core to handle the conversion ability
 - ▶ Preserve as much content & context as possible
- Support all the STIX versions
 - ▶ **STIX 2.1 Support**
 - ▶ 1.1.1, 1.2, 2.0 Support enhanced
- Mapping documentation¹
- Package available on PyPI²

¹<https://github.com/misp/misp-stix/tree/main/documentation#readme>

²<https://pypi.org/project/misp-stix/>

HANDLING THE CONVERSION WITH A PYTHON LIBRARY

■ Integration in python code

- ▶ Automation made easier by a close coupling with PyMISP

■ Export content from MISP

```
In [1]: import json
....: from misp_stix_converter import MISPtoSTIX21Parser
....: from pymisp import PyMISP
....: with open('tmp/config.json', 'r') as f:
....:     url, api_key, verify_cert = json.load(f)
....: misp = PyMISP(url, api_key, verify_cert)
....: misp.toggle_global_pythonify()
....: collection = misp.search(
....:     controller='attributes', page=1,
....:     type_attribute='ip-src', limit=10,
....:     tags=['tlp:white', 'tlp:clear']
....: )
....: parser = MISPtoSTIX21Parser()
....: parser.parse_misp_attributes(collection)
....: print(parser.bundle.serialize())
{"type": "bundle", "id": "bundle--a421897a-cafe-45ad-97ef-58761f6fac54", "objects": [{"type": "identity", "spec_version": "2.1", "id": "identity--55f6ea65-aa10-4c5a-bf01-4f84950d210f", "created": "2015-09-14T15:40:21.000Z", "modified": "2015-09-14T15:40:21.000Z", "name": "MISP", "identity_class": "organization"}, {"type": "indicator", "spec_version": "2.1", "id": "indicator--e4fce-21ac-46a7-9d82-06b3950d210b", "created": "2015-09-14T15:40:21.000Z", "modified": "2015-09-14T15:40:21.000Z", "pattern": "[network-traffic:src_ref.type = 'ipv4-addr' AND network-traffic:src_ref.value = '1.48.209.68']", "pattern_type": "stix", "pattern_version": "2.1", "valid_from": "2014-10-03T07:15:10.000Z", "kill_chain_phases": [{"kill_chain_name": "misp-category", "phase_name": "Network activity"}], "labels": ["misp:type\\\"Network activity\\\"", "misp:category\\\"Network activity\\\"", "misp:to_ids\\\"True\\\""], {"type": "indicator", "spec_version": "2.1", "id": "indicator--542e4fce-05f4-46ab-b5b8-06b3950d210b", "created": "2015-09-14T15:40:21.000Z", "modified": "2015-09-14T15:40:21.000Z", "pattern": "[network-traffic:src_ref.type = 'ipv4-addr' AND network-traffic:src_ref.value = '1.73.227.172']", "pattern_type": "stix", "pattern_version": "2.1", "valid_from": "2014-10-03T07:15:10.000Z", "kill_chain_phases": [{"kill_chain_name": "misp-category", "phase_name": "Network activity"}], "labels": ["misp:type\\\"Network activity\\\"", "misp:category\\\"Network activity\\\"", "misp:to_ids\\\"True\\\""], {"type": "indicator", "spec_version": "2.1", "id": "indicator--542e4fce-81c4-45f2-9e67-06b3950d210b", "created": "2015-09-14T15:40:21.000Z", "modified": "2015-09-14T15:40:21.000Z", "pattern": "[network-traffic:src_ref.type = 'ip-traffic' AND network-traffic:src_ref.value = '1.162.58.214']", "pattern_type": "stix", "pattern_version": "2.1", "valid_from": "2014-10-03T07:15:10.000Z", "kill_chain_phases": [{"kill_chain_name": "misp-category", "phase_name": "Network activity"}], "labels": ["misp:type\\\"Network activity\\\"", "misp:category\\\"Network activity\\\"", "misp:to_ids\\\"True\\\""]}], "spec_version": "2.1", "version": "2.1"}]
```

HANDLING THE CONVERSION WITH A PYTHON LIBRARY

■ Integration in python code

- ▶ Automation made easier by a close coupling with PyMISP

- Export content from MISP

- Using the STIX return format directly

```
In [2]: import json
.... from misp_stix_converter import MISPtoSTIX21Parser
.... from pymisp import PyMISP
.... with open('tmp/config.json', 'r') as f:
....     url, api_key, verify_cert = json.load(f)
.... misp = PyMISP(url, api_key, verify_cert)
.... misp.toggle_global_pythonify()
.... body = {
....     'returnFormat': 'stix2', 'stix-version': '2.1',
....     'type': 'ip-src', 'tags': ['tlp:white', 'tlp:clear'],
....     'page': 1, 'limit': 10
.... }
.... print(misp.direct_call('/attributes/restSearch', body))
{
'type': 'bundle', 'id': 'bundle--b8a39b06-219a-4f49-b46a-1ba30051a9bc', 'objects': [{'
'type': 'identity', 'spec_version': '2.1', 'id': 'identity--55f6ea65-aa10-4c5a-bf01-4f84950d210f', 'created': '2015-09-14T15:40:21.000Z', 'modified': '2015-09-14T15:40:21.000Z', 'name': 'MISP', 'identity_class': 'organization'}, {''
'type': 'indicator', 'spec_version': '2.1', 'id': 'indicator--55f6ea65-aa10-4c5a-bf01-4f84950d210f', 'created': '2015-09-14T15:40:21.000Z', 'modified': '2015-09-14T15:40:21.000Z', 'pattern': "[network-traffic:src_ref.type = 'ipv4-addr' AND network-traffic:src_ref.value = '1.48.209.68']", 'pattern_type': 'stix', 'pattern_version': '2.1', 'valid_from': '2014-10-03T07:15:10.000Z', 'valid_till': '2015-09-14T15:40:21.000Z', 'kill_chain_phases': [{"kill_chain_name": "misp-category", "phase_name": "Network activity"}], 'labels': ['misp:type=Network activity', 'misp:category=Network activity', 'misp:to_ids=True']}, {''
'type': 'indicator', 'spec_version': '2.1', 'id': 'indicator--55f6ea65-aa10-4c5a-bf01-4f84950d210f', 'created': '2014-10-03T07:15:10.000Z', 'modified': '2014-10-03T07:15:10.000Z', 'pattern': "[network-traffic:src_ref.type = 'ipv4-addr' AND network-traffic:src_ref.value = '1.73.227.172']", 'pattern_type': 'stix', 'pattern_version': '2.1', 'valid_from': '2014-10-03T07:15:10.000Z', 'valid_till': '2015-09-14T15:40:21.000Z', 'kill_chain_phases': [{"kill_chain_name": "misp-category", "phase_name": "Network activity"}], 'labels': ['misp:type=Network activity', 'misp:category=Network activity', 'misp:to_ids=True']}, {''
'type': 'indicator', 'spec_version': '2.1', 'id': 'indicator--55f6ea65-aa10-4c5a-bf01-4f84950d210f', 'created': '2014-10-03T07:15:10.000Z', 'modified': '2014-10-03T07:15:10.000Z', 'pattern': "[network-traffic:src_ref.type = 'ipv4-addr' AND network-traffic:src_ref.value = '1.162.58.214']", 'pattern_type': 'stix', 'pattern_version': '2.1', 'valid_from': '2014-10-03T07:15:10.000Z', 'valid_till': '2015-09-14T15:40:21.000Z', 'kill_chain_phases': [{"kill_chain_name": "misp-category", "phase_name": "Network activity"}], 'labels': ['misp:type=Network activity', 'misp:category=Network activity', 'misp:to_ids=True']}], 'labels': ['misp:type=Network activity', 'misp:category=Network activity']}, 'id': 'bundle--b8a39b06-219a-4f49-b46a-1ba30051a9bc', 'spec_version': '2.1', 'type': 'bundle'}
```

HANDLING THE CONVERSION WITH A PYTHON LIBRARY

■ Integration in python code

- ▶ Automation made easier by a close coupling with PyMISP
- Converting STIX content and adding the resulting Event

```
In [1]: import json
....: from misp_stix_converter import ExternalSTIX2toMISPParser
....: from pathlib import Path
....: from pymisp import PyMISP
....: with open('tmp/config.json', 'r') as f:
....:     url, api_key, verify_cert = json.load(f)
....: misp = PyMISP(url, api_key, verify_cert)
....: misp.toggle_global_pythonify()
....: parser = ExternalSTIX2toMISPParser()
....: parser.parse_stix_content(
....:     'tmp/AA23-263A_#StopRansomware_Snatch_Ransomware.stix21.json'
....: )
....: event = misp.add_event(parser.misp_event)
....: event.id
Out[1]: 1424
```

■ Using the API endpoint directly

```
In [2]: params = {'galaxies_as_tags': 0, 'debug': 1}
....: response = misp.upload_stix(
....:     'tmp/AA23-187A.stix21.json', kw_params=params
....: )
....: response.json()['Event']['id']
Out[2]: '1425'
```

HANDLING THE CONVERSION WITH A PYTHON LIBRARY

- Addressing the limitations of a MISP built-in integration
 - ▶ Export & import features available as a command-line application

```
oui chrissr3d ~/git/MISP/MISP-STIX-Converter
$ (git::dev) poetry run misp_stix_converter export -h
usage: misp_stix_converter export [-h] -f FILE [FILE ...] -v {1.1.1,1.2,2.0,2.1} [-s] [-m] [-o OUTPUT_DIR] [-o OUTPUT_NAME] [--level {attribute,event}]
                                [--format {json,xml}] [-n NAMESPACE] [-org ORG]

options:
-h, --help            show this help message and exit
-f FILE [FILE ...], --file FILE [FILE ...]
                    Path to the file(s) to convert.
-v {1.1.1,1.2,2.0,2.1}, --version {1.1.1,1.2,2.0,2.1}
                    STIX specific version.
-s, --single_output  Produce only one result file (in case of multiple input file).
-m, --in_memory       Store result in memory (in case of multiple result files) instead of storing it in tmp files.
--output_dir OUTPUT_DIR
                    Output path - used in the case of multiple input files when the 'single_output' argument is not used.
-o OUTPUT_NAME, --output_name OUTPUT_NAME
                    Output file name - used in the case of a single input file or when the 'single_output' argument is used.

STIX 1 specific arguments:
--level {attribute,event}
                    MISP data structure level.
--format {json,xml}  STIX 1 format.
-n NAMESPACE, --namespace NAMESPACE
                    Namespace to be used in the STIX 1 header.
-org ORG             Organisation name to be used in the STIX 1 header.
oui chrissr3d ~/git/MISP/MISP-STIX-Converter
$ (git::dev) poetry run misp_stix_converter import -h
usage: misp_stix_converter import [-h] -f FILE [FILE ...] -v {1,2} [-s] [-o OUTPUT_NAME] [-o OUTPUT_DIR] [-d DISTRIBUTION] [-sg SHARING_GROUP] [-galaxies_as_tags]

options:
-h, --help            show this help message and exit
-f FILE [FILE ...], --file FILE [FILE ...]
                    Path to the file(s) to convert.
-v {1,2}, --version {1,2}
                    STIX major version.
-s, --single_output  Produce only one MISP event per STIX file(in case of multiple Report, Grouping or Incident objects).
-o OUTPUT_NAME, --output_name OUTPUT_NAME
                    Output file name - used in the case of a single input file or when the 'single_output' argument is used.
--output_dir OUTPUT_DIR
                    Output path - used in the case of multiple input files when the 'single_output' argument is not used.
-d DISTRIBUTION, --distribution DISTRIBUTION
                    Distribution level for the imported MISP content.
-sg SHARING_GROUP, --sharing_group SHARING_GROUP
                    Sharing group ID when distribution is 4.
--galaxies_as_tags   Import MISP Galaxies as tag names instead of the standard Galaxy format.
oui chrissr3d ~/git/MISP/MISP-STIX-Converter
$ (git::dev) 
```

HANDLING THE CONVERSION WITH A PYTHON LIBRARY

- Addressing the limitations of a MISP built-in integration
 - ▶ Export & import features available as a command-line application

```
oui chrisr3d ~/git/MISP/MISP-STIX-Converter
$ (git:::dev) poetry run misp_stix_converter import -v 2 -f tmp/debug/STIX/playbook_json/*.json
Failed parsing the following - and the related error message:
- tmp/debug/STIX/playbook_json/automated-libra.json - Invalid value for Indicator 'pattern': FAIL: Error found at line 1:0. input is missing :
brackets
Successfully processed your files. Results available in:
- tmp/debug/STIX/playbook_json/adept-libra.json.out
- tmp/debug/STIX/playbook_json/agedlibra.json.out
- tmp/debug/STIX/playbook_json/agent-tesla.json.out
- tmp/debug/STIX/playbook_json/allotytaurus.json.out
- tmp/debug/STIX/playbook_json/api-hammering-technique.json.out
- tmp/debug/STIX/playbook_json/atlassian-confluence-CVE-2022-26134.json.out
- tmp/debug/STIX/playbook_json/avoslocker-ransomware.json.out
- tmp/debug/STIX/playbook_json/blackbasta-ransomware.json.out
- tmp/debug/STIX/playbook_json/blackcat-ransomware.json.out
- tmp/debug/STIX/playbook_json/bluesky-ransomware.json.out
- tmp/debug/STIX/playbook_json/boggserpens.json.out
- tmp/debug/STIX/playbook_json/brute-rate1.json.out
- tmp/debug/STIX/playbook_json/chromeloader.json.out
- tmp/debug/STIX/playbook_json/clean-ursa.json.out
- tmp/debug/STIX/playbook_json/cloaked-ursa.json.out
- tmp/debug/STIX/playbook_json/clop-ransomware.json.out
- tmp/debug/STIX/playbook_json/conti-ransomware.json.out
- tmp/debug/STIX/playbook_json/crawling-taurus.json.out
- tmp/debug/STIX/playbook_json/crooked-pisces.json.out
- tmp/debug/STIX/playbook_json/darkside-ransomware.json.out
- tmp/debug/STIX/playbook_json/dearcry-ransomware.json.out
- tmp/debug/STIX/playbook_json/egregor-ransomware.json.out
- tmp/debug/STIX/playbook_json/ekans-ransomware.json.out
- tmp/debug/STIX/playbook_json/emotet.json.out
- tmp/debug/STIX/playbook_json/evasive-serpens.json.out
- tmp/debug/STIX/playbook_json/f5-big-ip-cve-2022-1388.json.out
- tmp/debug/STIX/playbook_json/fighting-ursa.json.out
- tmp/debug/STIX/playbook_json/golfing-taurus.json.out
- tmp/debug/STIX/playbook_json/granite-taurus.json.out
- tmp/debug/STIX/playbook_json/hellokitty-ransomware.json.out
- tmp/debug/STIX/playbook_json/hermeticwiper.json.out
- tmp/debug/STIX/playbook_json/hive_ransomware.json.out
```

■ Improve the import feature

- ▶ Handle different content design from different sources
- ▶ Support of existing STIX objects libraries³
- ▶ Support custom STIX format
- ▶ **Handle validation issues**

■ Continuous MISP ⇔ STIX mapping improvement

■ More tests to avoid edge case issues

■ Participating in Oasis CTI TC



³<https://github.com/mitre/cti>

HOW TO REPORT BUGS/ISSUES

■ Github issues

- ▶ <https://github.com/MISP/misp-stix/issues>
- ▶ <https://github.com/MISP/MISP/issues>

■ Please provide details

- ▶ How did the issue happen
- ▶ **Recommendation:** provide samples

■ Any feedback welcome

TO GET IN TOUCH WITH US

- <https://github.com/MISP/misp-stix>
- <https://github.com/MISP/misp-stix/tree/main/documentation>

- <https://github.com/MISP>
- <https://www.misp-project.org/>
- <https://twitter.com/MISPPProject>
- https://twitter.com/chrisred_68

AUTOMATION IN MISP

TUTORIAL AND HANDS-ON

SAMI MOKADDEM

MISP PROJECT

<https://www.misp-project.org/>



CONTENT OF THE PRESENTATION

1. Automation in MISP
2. MISP API / PyMISP
3. PubSub channels (ZeroMQ)
4. MISP Workflows
 - ▶ Fundamentals
 - ▶ Demo with examples
 - ▶ Using the system
 - ▶ How it can be extended

AUTOMATION IN MISP: WHAT ALREADY EXISTS?



MISP API / PyMISP

- Needs CRON Jobs in place
- Potentially heavy for the server
- Not realtime



PubSub channels

- After the actions happen: No feedback to MISP
- Tougher to put in place & to share
- Full integration amounts to develop a new tool

MISP API / PyMISP - FUNDAMENTALS

Objective: Get to know how to use the MISP API PyMISP

MISP API / PyMISP - DEMO

- Generate an API key
- RestClient overview
- MISP API Overview notebook¹
- PyMISP Overview notebook²

¹<https://github.com/MISP/misp-training/blob/main/a.7-rest-API/Training%20-%20Using%20the%20API%20in%20MISP.ipynb>

²<https://github.com/MISP/PyMISP/blob/main/docs/tutorial/FullOverview.ipynb>

PUBSUB CHANNELS (ZEROMQ) - FUNDAMENTALS

Objective: Learn how to setup realtime automation using the ZeroMQ channel

ZEROMQ CHANNEL - DEMO

■ What is ZeroMQ?

- ▶ *N-to-N Asynchronous message-processing tasks*
- ▶ *Publisher (MISP) and consumer (scripts)*

■ Configuring ZeroMQ in MISP

■ Integrating with the ZeroMQ of MISP

MISP WORKFLOWS - FUNDAMENTALS

Objective: Learn how to use the MISP Workflow feature

AUTOMATION IN MISP: WHAT ALREADY EXISTS?



MISP API / PyMISP

- Needs CRON Jobs in place
- Potentially heavy for the server
- Not realtime



PubSub channels

- After the actions happen: No feedback to MISP
 - Tougher to put in place & to share
 - Full integration amounts to develop a new tool
- No way to **prevent** behavior
→ Difficult to setup **hooks** to execute callbacks

WHAT TYPE OF USE-CASES ARE WE TRYING TO SUPPORT?



- **Prevent** default MISP behaviors to happen
 - ▶ Prevent **publication of events** not passing sanity checks
 - ▶ Prevent **querying** third-party **services** with sensitive information
 - ▶ ...

- **Hook** specific actions to run callbacks
 - ▶ **Automatically run** enrichment services
 - ▶ Modify data on-the-fly: False positives, enable CTI-Pipeline
 - ▶ Send notifications in a chat rooms
 - ▶ ...

SIMPLE AUTOMATION IN MISP MADE EASY



- Why?
 - ▶ Everyone loves **simple automation**
 - ▶ **Visual** dataflow programming
 - ▶ Users want **more control**
- How?
 - ▶ **Drag & Drop** editor
 - ▶ Prevent actions **before they happen**
 - ▶ Flexible **Plug & Play** system
 - ▶ Share workflows, **debug** and **replay**

EXAMPLE OF USE-CASES

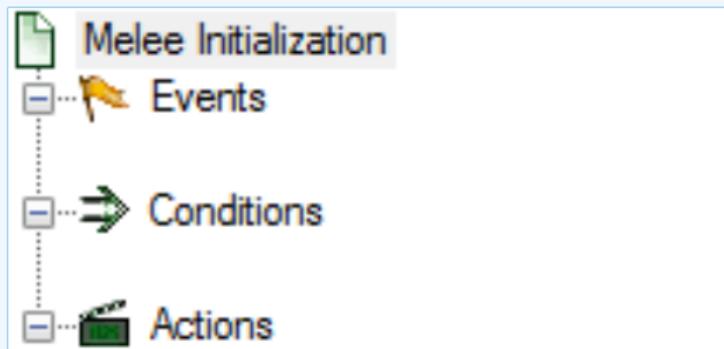
- **Notification** on specific actions
 - ▶ New events matching criteria
 - ▶ New users
 - ▶ Automated alerts for high-priority IOCs
- **Extend** existing MISP behavior
 - ▶ Push data to another system
 - ▶ Automatic enrichment
 - ▶ Sanity check to block publishing / sharing
- **Hook** capabilities
 - ▶ Assign tasks and notify incident response team members
 - ▶ Run curation pipeline
- ...

WORKFLOW - FUNDAMENTALS

Objective: Start with the foundation to understand the basics



HOW DOES IT WORK



1. An **event** happens in MISP
2. Check if all **conditions** are satisfied
3. Execute all **actions**
 - ▶ May prevent MISP to complete its original event

WHAT KIND OF EVENTS?

Events

- New MISP Event
- Attribute has been saved
- New discussion post
- New user created
- Query against third-party services
- ...

- ② Supported events in MISP are called **Triggers**
- ② A **Trigger** is associated with **1-and-only-1 Workflow**

TRIGGERS CURRENTLY AVAILABLE

Currently 10 triggers can be hooked. 3 being Blocking.

Triggers

List the available triggers that can be listened to by workflows.

Missing a trigger? Feel free to open a Github issue!

Documentation and concepts

« previous

next »

All	attribute	event	object	others	post	user	Blocking	Enabled	Disabled	Trigger name	Scope	Trigger overhead	Run counter	Blocking Workflow	MISP Core format	Workflow ID	Last Update	Debug enabled	Enabled	Actions		
											attribute		83			160	2022-08-03 09:00:41	<input type="checkbox"/>				
											others		1154			162	2022-10-17 12:35:57	<input type="checkbox"/>				
											event		49			175	2022-10-14 13:32:01	<input type="checkbox"/>				
											event		5			182	2022-10-17 09:12:14	<input checked="" type="checkbox"/>				
											event		6			183	2022-10-17 09:01:36	<input checked="" type="checkbox"/>				
											event		126			180	2022-10-13 10:42:53	<input checked="" type="checkbox"/>				
											object		35			161	2022-08-05 07:12:52	<input type="checkbox"/>				
											post		36			176	2022-07-28 13:59:51	<input type="checkbox"/>				
											user		0			181	2022-08-05 07:19:46	<input type="checkbox"/>				
											user		42			158	2022-07-28 14:00:32	<input type="checkbox"/>				

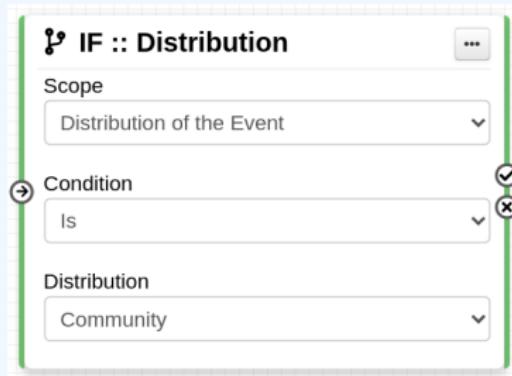
Page 1 of 1, showing 1 records out of 10 total, starting on record 1, ending on 10

WHAT KIND OF CONDITIONS?

Conditions

- A MISP Event is tagged with tlp:red
- The distribution of an Attribute is a sharing group
- The creator organisation is circl.lu
- Or any other **generic** conditions

? These are also called **Logic modules**



WORKFLOW - LOGIC MODULES

- ➔ logic modules: Allow to redirect the execution flow.
 - ▶ IF conditions
 - ▶ Delay execution

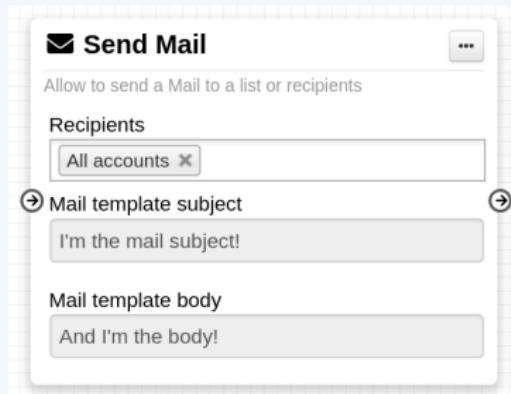
All	Action	Logic	misp-module	Custom	Blocking	Enabled	Disabled	Enter value to search	Filter	X	
					Type	Blocking	MISP Core format	misp-module	Custom	Enabled	Actions
<input type="checkbox"/>	Module name				logic	✗	✗	✗	✓	✗	► ⓘ
<input type="checkbox"/>	(Blueprint logic module)				logic	✗	✗	✗	✗	✓	■ ⓘ
<input type="checkbox"/>	.concurrent Task				logic	✗	✗	✗	✗	✓	■ ⓘ
<input type="checkbox"/>	IF :: Distribution				logic	✗	✓	✗	✗	✓	■ ⓘ
<input type="checkbox"/>	Filter :: Generic				logic	✗	✗	✗	✗	✗	► ⓘ
<input type="checkbox"/>	Filter :: Remove filter				logic	✗	✗	✗	✗	✗	► ⓘ
<input type="checkbox"/>	IF :: Generic				logic	✗	✗	✗	✗	✓	■ ⓘ
<input type="checkbox"/>	IF :: Organisation				logic	✗	✓	✗	✗	✓	■ ⓘ
<input type="checkbox"/>	IF :: Published				logic	✗	✓	✗	✗	✓	■ ⓘ
<input type="checkbox"/>	IF :: Tag				logic	✗	✓	✗	✗	✓	■ ⓘ
<input type="checkbox"/>	IF :: Threat Level				logic	✗	✗	✗	✗	✗	► ⓘ

WHAT KIND OF ACTIONS?

Actions

- Send an email notification
- Perform enrichments
- Send a chat message on MS Teams
- Attach a local tag
- ...

 These are also called **Action modules**



WORKFLOW - ACTION MODULES

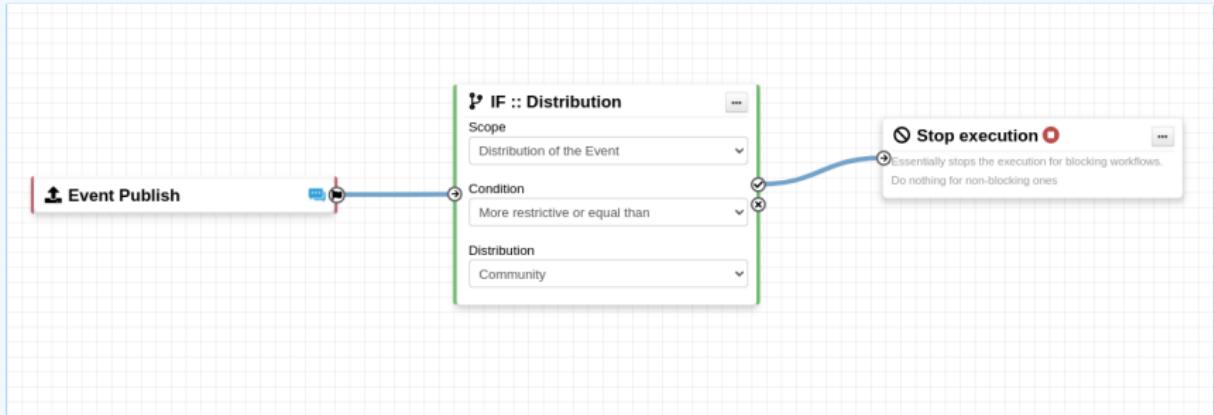
■ action modules: Allow to execute operations

- ▶ Tag operations
- ▶ Send notifications
- ▶ Webhooks & Custom scripts

All	Action	Logic	misp-module	Custom	Blocking	Enabled	Disabled	Enter value to search	Filter	X
Module name		Type	Blocking	MISP Core format	misp-module	Custom	Enabled	Actions		
<input type="checkbox"/>	* Attach enrichment	action	x	✓	x	x	✓	 		
<input type="checkbox"/>	 Attribute edition operation	action	x	✓	x	x	✓	 		
<input type="checkbox"/>	 Attribute IDS Flag operation	action	x	✓	x	x	✓	 		
<input type="checkbox"/>	 Blueprint action module	action	x	x	x	✓	✓	 		
<input type="checkbox"/>	* Enrich Event	action	x	✓	x	x	✓	 		
<input type="checkbox"/>	 mattermost	action	x	x	✓	x	✓	 		
<input type="checkbox"/>	 MS Teams Webhook	action	x	x	x	x	✓	 		
<input type="checkbox"/>	 Push to ZMQ	action	x	x	x	x	✓	 		
<input type="checkbox"/>	 Send Log Mail	action	x	x	x	x	x	 		
<input type="checkbox"/>	 Send Mail	action	x	x	x	x	✓	 		
<input type="checkbox"/>	> Splunk HEC export	action	x	✓	x	x	x	 		
<input type="checkbox"/>	 Stop execution	action	✓	x	x	x	✓	 		
<input type="checkbox"/>	 Tag operation	action	x	✓	x	x	✓	 		
<input type="checkbox"/>	 testaction	action	x	x	✓	x	✓	 		
<input type="checkbox"/>	 Webhook	action	x	x	x	x	✓	 		

WHAT IS A MISP WORKFLOW?

- Sequence of all nodes to be executed in a specific order
- Workflows can be enabled / disabled
- A Workflow is associated to **1-and-only-1 trigger**



WORKFLOW EXECUTION FOR EVENT PUBLISH



An Event is about to be published

- ▶ The workflow for the event-publish trigger starts



Conditions are evaluated

- ▶ They might change the path taken during the execution



Actions are executed

- ▶ **success:** Continue the publishing action

```
execute_workflow  Finished executing workflow for trigger `event-publish` (180). Outcome: success
```

- ▶ **failure | blocked:** Stop publishing and log the reason

```
execute_workflow  Execution stopped.
```

```
Node `stop-execution` (8) from Workflow `Workflow for trigger event-publish` (180) returned the following error: Execution stopped
```

BLOCKING AND NON-BLOCKING

Two types of workflows:

Blocking Workflows

- ▶ Can prevent / block the original event to happen
- ▶ If a **blocking module** blocks the action

Non blocking Workflows execution outcome has no impact

- ▶ No way to prevent something that happened in the past



SOURCES OF WORKFLOW MODULES (o)

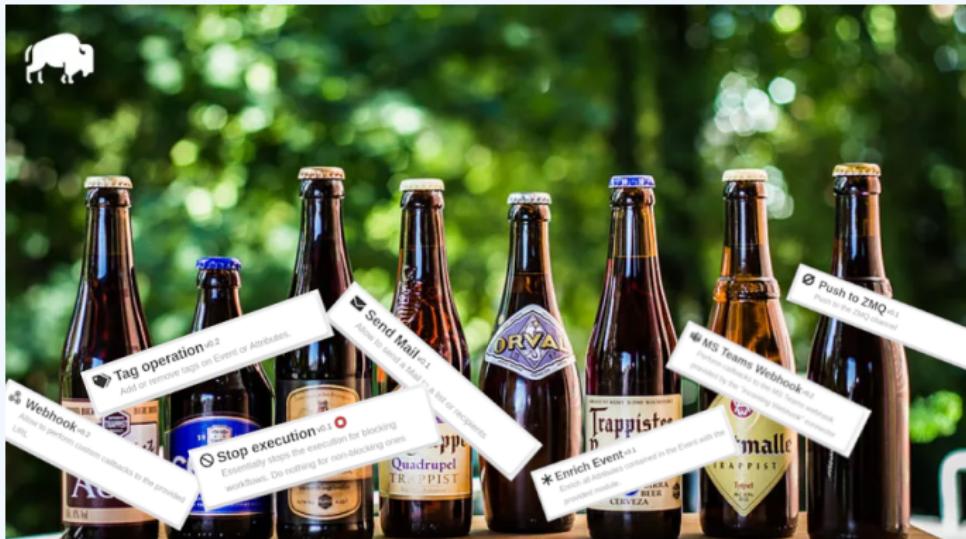
Currently 36 built-in modules.

- **Trigger** module (11): built-in **only**
 - ▶ Get in touch if you want more
- **Logic** module (10): built-in & **custom**
- **Action** module (15): built-in & **custom**

SOURCES OF WORKFLOW MODULES (1)

■ Built-in **default** modules

- ▶ Part of the MISP codebase
- ▶ Get in touch if you want us to increase the selection (or merge PR!)



SOURCES OF WORKFLOW MODULES (2)

User-defined **custom** modules

- Written in PHP
- Extend existing modules
- MISP code reuse

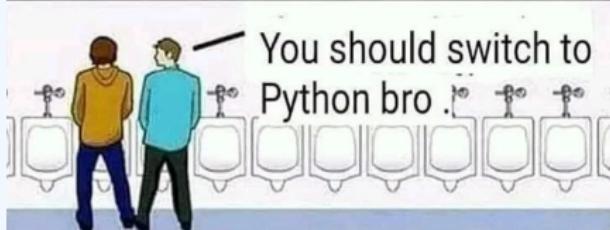
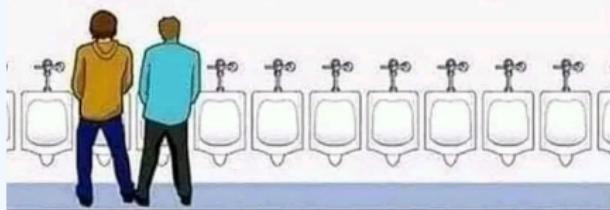


SOURCES OF WORKFLOW MODULES (3)

Modules from the

misp-module^{⊗⊗}

enrichment service



- Written in Python
- Can use any python libraries
- Plug & Play

DEMO BY EXAMPLES

WF-1. Send an email to **all** when a new event has been pulled

WF-2. Block queries on 3rd party services when **tlp:red** or **PAP:red**

- ▶ **tlp:red**: For the eyes and ears of individual recipients only
- ▶ **PAP:RED**: Only passive actions that are not detectable from the outside

WORKFLOW - GETTING STARTED

Objective: How to install & configure workflows



2.4.160 Epic summer release



iglocska released this 08 Aug 2022



v2.4.160



71d4e2c



1. Update your MISP server
2. Update all your sub-modules



GETTING STARTED WITH WORKFLOWS (2)

Review MISP settings:

1. Make sure MISP.background_jobs is turned on
2. Make sure workers are up-and-running and healthy
3. Turn the setting Plugin.Workflow_enable on

The screenshot shows the MISP configuration interface with the 'Plugin settings' tab selected. The top navigation bar includes links for Overview, MISP settings, Encryption settings, Proxy settings, Security settings, Plugin settings (465), SimpleBackgroundJobs settings, and Diagnos. Below the navigation is a sidebar with categories: Enrichment, Import, Export, Action, Cortex, Sightings, and Workflow. The 'Workflow' category is currently active. A table below lists a single setting: Recommended Plugin.Workflow_enable true Enable/disable workflow feature.

Recommended	Plugin.Workflow_enable	true	Enable/disable workflow feature

GETTING STARTED WITH WORKFLOWS (3)

Review MISP settings:

4. [optional:misp-module] Turn the setting `Plugin.Action_services_enable` on

Overview MISP settings (20 ▲) Encryption settings (7 ▲) Proxy settings (5) Security settings (8 ▲) Plugin settings (465 ▲) SimpleBackgroundJobs settings (11 ▲) Diagnos				
Enrichment				Filter the table(s) below
Import				
Export				
<u>Action</u>				
Critical	Plugin.Action_services_enable	true	Enable/disable the action services	
Recommended	Plugin.Action_services_url	http://host.docker.internal	The url used to access the action services. By default, it is accessible at http://127.0.0.1:6666	
Recommended	Plugin.Action_services_port	6677	The port used to access the action services. By default, it is accessible at 127.0.0.1:6666	
Recommended	Plugin.Action_timeout	10	Set a timeout for the action services	Value not set.

GETTING STARTED WITH WORKFLOWS (4)

If you wish to use action modules from misp-module, make sure to have:

- The latest update of misp-module
 - ▶ There should be an `action_mod` module type in `misp-modules/misp_modules/modules`
- Restarted your misp-module application

```
1 # This command should show all 'action' modules
2 $ curl -s http://127.0.0.1:6666/modules | \
3 jq '.[] | select(.meta.module-type == "action") | \
4 {name: .name, version: .meta.version}'
```

GETTING STARTED WITH WORKFLOWS (5)

Everything is ready?

Let's see how to build a workflow!



CREATING A WORKFLOW WITH THE EDITOR

1. Prevent event publication if **tlp:red** tag
2. Send a mail to admin@admin.test about potential data leak
3. Otherwise, send a notification on **Mattermost, MS Teams, Telegram, ...**

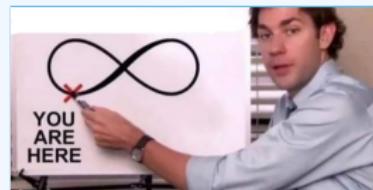
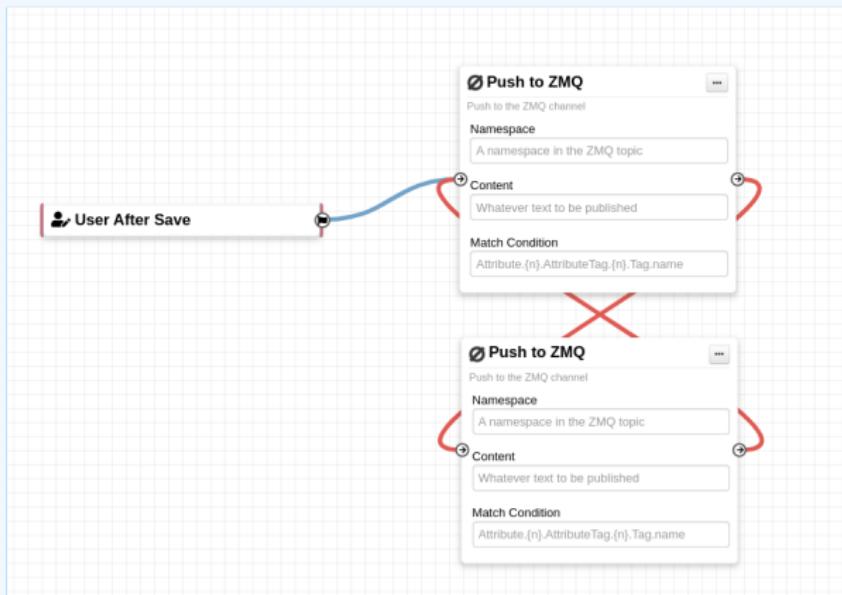
CONSIDERATIONS WHEN WORKING WITH WORKFLOWS

Objective: Overview of some common pitfalls

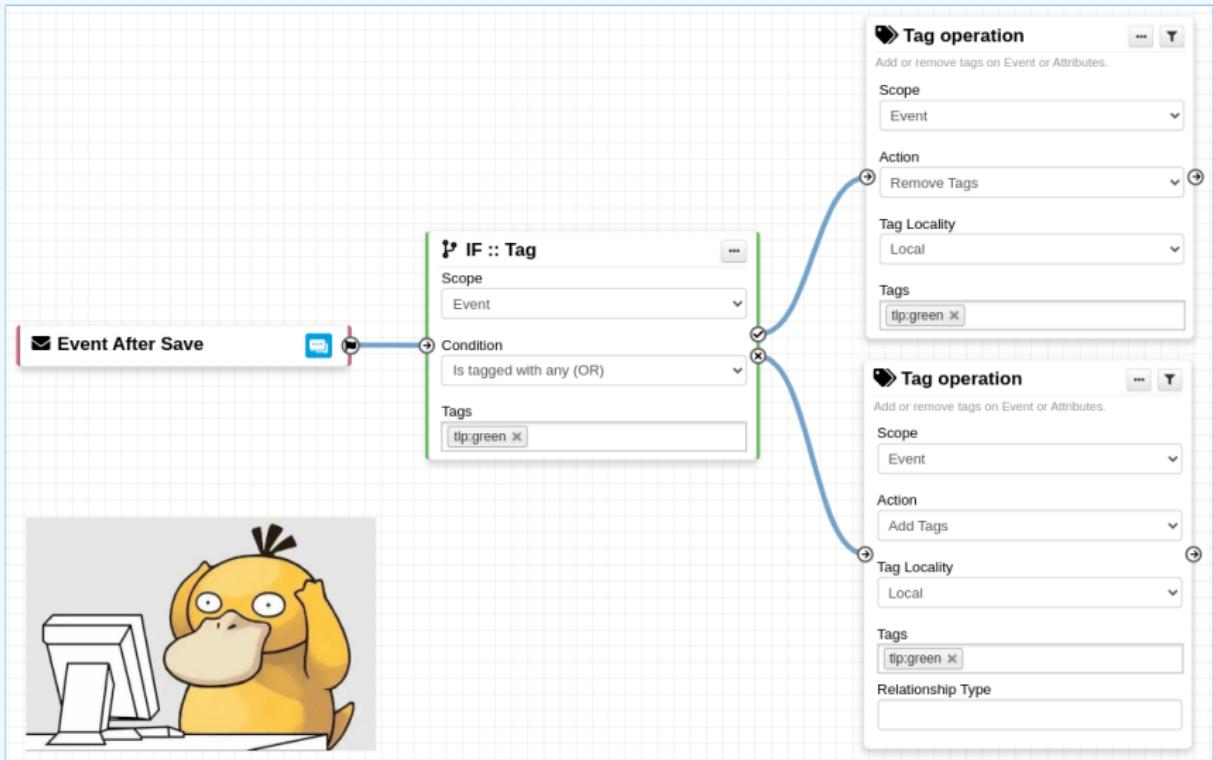


WORKING WITH THE EDITOR - OPERATIONS NOT ALLOWED

Execution loop are not authorized



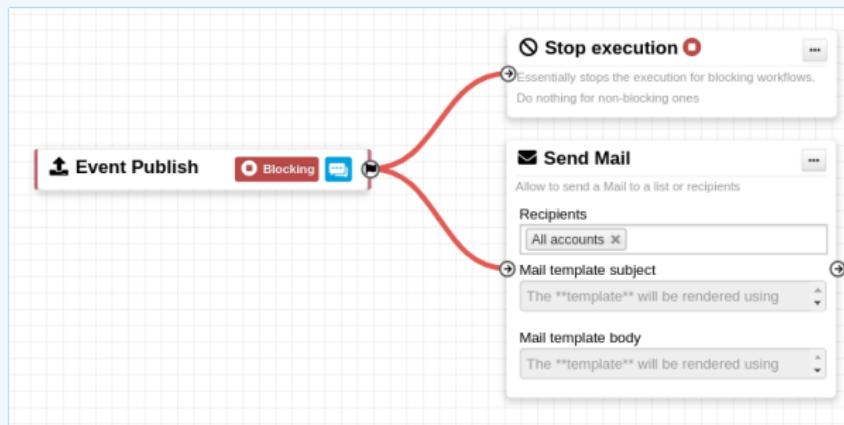
RECURSIVE WORKFLOWS



⚠ Recursion: If an action re-runs the workflow

WORKING WITH THE EDITOR - OPERATIONS NOT ALLOWED

Multiple connections from the same output

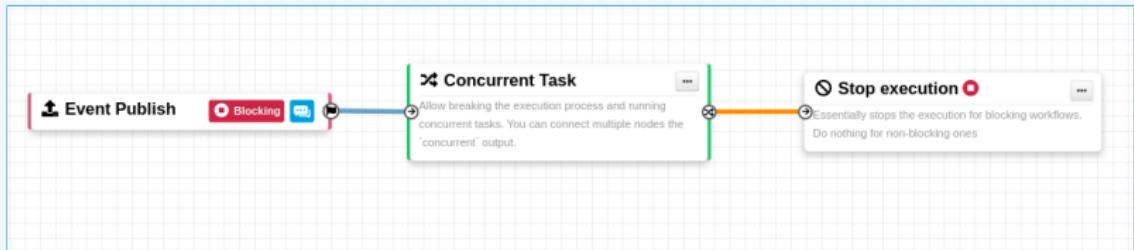


- Execution order not guaranteed
- Confusing for users

WORKING WITH THE EDITOR

Cases showing a warning:

- Blocking modules  in a  Non blocking workflow
- Blocking modules  after a concurrent tasks module



ADVANCED USAGE

Objective: Overview of Blueprints, Data format and Filtering

WORKFLOW BLUEPRINTS



1. Blueprints allow to **re-use parts** of a workflow in another one
2. Blueprints can be saved, exported and **shared**

Debugging webhook v1656059209

9ff210dd-ee7e-49c8-a5af-10cd42cdadb6

Default: **X**

Blueprint Content: **1 node**

 1

Webhook module pre-configured for debugging purposes

Blueprints sources:

1. Created or imported by users
2. From the MISP/misp-workflow-blueprints repository³

³<https://github.com/MISP/misp-workflow-blueprints>

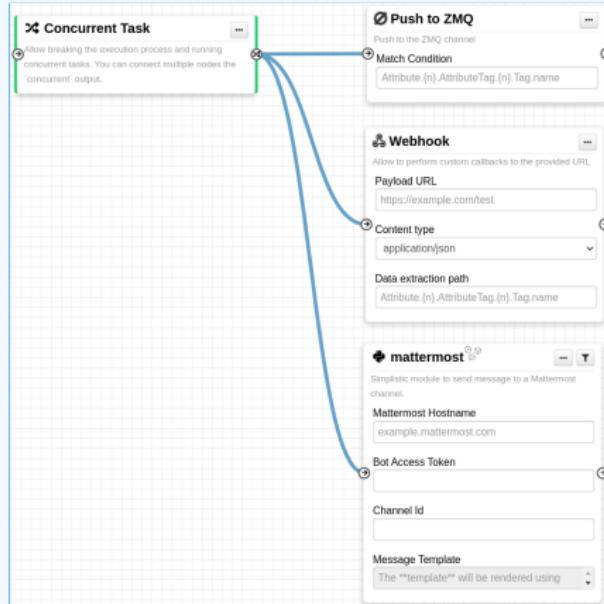
WORKFLOW BLUEPRINTS

Currently, 4 blueprints available:

- Attach the tlp:clear tag on elements having the tlp:white tag
- Block actions if any attributes have the PAP:RED or tlp:red tag
- Disable to_ids flag for existing hash in *hashlookup*
- Set tag based on *BGP Ranking* maliciousness level

LOGIC MODULE: CONCURRENT TASK

- Logic module allowing **multiple output** connections
- **Postpone the execution** for remaining modules
- Convert Blocking → Non blocking



DATA FORMAT IN WORKFLOWS



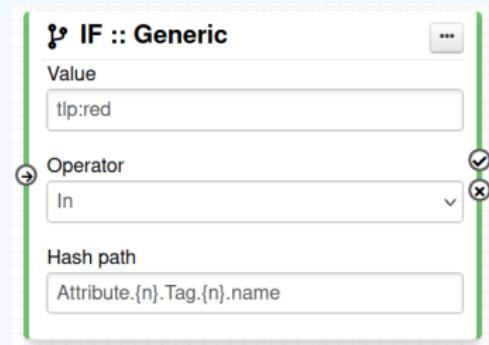
- In most cases, the format is the **MISP Core format**
 - ▶ Attributes are **always encapsulated** in the Event or Object
- But has **additional properties**
 - ▶ Additional key **_AttributeFlattened**
 - ▶ Additional key **_allTags**
 - ▶ Additional key **inherited** for Tags

HASH PATH FILTERING (1)

Filtering and checking conditions using hash path expression.

```
1 $path_expression = '{n}[name=fred].id';
2 $users = [
3     {'id': 123, 'name': 'fred', 'surname': 'bloggs'},
4     {'id': 245, 'name': 'fred', 'surname': 'smith'},
5     {'id': 356, 'name': 'joe', 'surname': 'smith'},
6 ];
7 $ids = Hash::extract($users, $path_expression);
8 // => $ids will be [123, 245]
```

```
{
    "Attribute": [
        {
            "type": "domain",
            "value": "cti-summit.org",
            "Tag": [
                {
                    "name": "tlp:red",
                    "colour": "#CC0033"
                }
            ]
        }
    ]
}
```



HASH PATH FILTERING (2)

Hash path filtering can be used to **filter** data **on the node** it is passed to or on the **execution path**.

Node Filtering

Element selector
Event._AttributeFlattened.{n}

Value
domain

Operator
Equals

Hash Path
type

Save **Close**

Filter :: Generic

Generic data filtering block. The module filters incoming data and forward the matching data to its output.

Filtering Label
Label A

Data selector
Event._AttributeFlattened.{n}

Value
tip:red

Operator
In

Hash path
Tag.{n}.name

HASH PATH FILTERING - EXAMPLE

```
1  {
2      "Event": {
3          "uuid": ...
4          "timestamp": ...
5          "distribution": 1,
6          "published": false,
7          "Attribute": [
8              {
9                  "type": "ip-src",
10                 "value": "8.8.8.8", ...
11             },
12             {
13                 "type": "domain",
14                 "value": "misp-project.org", ...
15             }
16         ],
17         ...
18     }
19 }
```

1. Access Event distribution
 - ▶ Event.distribution

HASH PATH FILTERING - EXERCISE (1)

```
1  {
2      "Event": {
3          "uuid": ...,
4          "distribution": 1,
5          "published": false,
6          "Attribute": [
7              {
8                  "type": "ip-src",
9                  "value": "8.8.8.8", ...
10             },
11             {
12                 "type": "domain",
13                 "value": "misp-project.org", ...
14             }
15         ],
16         ...
17     }
18 }
```

2. Access Event published state

HASH PATH FILTERING - EXERCISE (1)

```
1  {
2      "Event": {
3          "uuid": ...,
4          "distribution": 1,
5          "published": false,
6          "Attribute": [
7              {
8                  "type": "ip-src",
9                  "value": "8.8.8.8", ...
10             },
11             {
12                 "type": "domain",
13                 "value": "misp-project.org", ...
14             }
15         ],
16         ...
17     }
18 }
```

-
2. Access Event published state
 - ▶ Event.published

HASH PATH FILTERING - EXERCISE (2)

```
1  {
2      "Event": {
3          "uuid": ...,
4          "distribution": 1,
5          "published": false,
6          "Attribute": [
7              {
8                  "type": "ip-src",
9                  "value": "8.8.8.8", ...
10             },
11             {
12                 "type": "domain",
13                 "value": "misp-project.org", ...
14             }
15         ],
16         ...
17     }
18 }
```

-
3. Access all Attribute types
 - ▶ Hint: Use **{n}** to loop

HASH PATH FILTERING - EXERCISE (2)

```
1  {
2      "Event": {
3          "uuid": ...,
4          "distribution": 1,
5          "published": false,
6          "Attribute": [
7              {
8                  "type": "ip-src",
9                  "value": "8.8.8.8", ...
10             },
11             {
12                 "type": "domain",
13                 "value": "misp-project.org", ...
14             }
15         ],
16         ...
17     }
18 }
```

3. Access all Attribute types

- ▶ Hint: Use **{n}** to loop
- ▶ Event.Attribute.{n}.type

HASH PATH FILTERING - EXERCISE (3)

```
1 {  
2     "Event": {  
3         "Attribute": [  
4             {  
5                 "type": "ip-src",  
6                 "value": "8.8.8.8",  
7                 "Tag": [  
8                     {  
9                         "name": "PAP:AMBER", ...  
10                    }  
11                ], ...  
12            }  
13        ], ...  
14    }  
15 }  
16 }
```

-
3. Access all Tags attached to Attributes

HASH PATH FILTERING - EXERCISE (3)

```
1 {  
2     "Event": {  
3         "Attribute": [  
4             {  
5                 "type": "ip-src",  
6                 "value": "8.8.8.8",  
7                 "Tag": [  
8                     {  
9                         "name": "PAP:AMBER", ...  
10                    }  
11                ], ...  
12            }  
13        ], ...  
14    }  
15 }  
16 }
```

3. Access all Tags attached to Attributes

- ▶ Event.Attribute.{n}.Tag.{n}.name

HASH PATH FILTERING - EXERCISE (4)

```
1  {
2      "Event": {
3          "Tag": [
4              {
5                  "name": "tlp:green", ...
6              }
7          ], ...
8          "Attribute": [
9              {
10                 "value": "8.8.8.8",
11                 "Tag": [
12                     {
13                         "name": "PAP:AMBER", ...
14                     }
15                 ], ...
16             }
17         ],
18     }
19 }
```

4. Access all Tags attached to Attributes and from the Event
 - ▶ Hint: Use `_allTags` to access **all** tags

HASH PATH FILTERING - EXERCISE (4)

```
1  {
2      "Event": {
3          "Tag": [
4              {
5                  "name": "tlp:green", ...
6              }
7          ], ...
8          "Attribute": [
9              {
10                 "value": "8.8.8.8",
11                 "Tag": [
12                     {
13                         "name": "PAP:AMBER", ...
14                     }
15                 ], ...
16             }
17         ],
18     }
19 }
```

4. Access all Tags attached to Attributes and from the Event
 - ▶ `Event.Attribute.{n}._allTags.{n}.name`

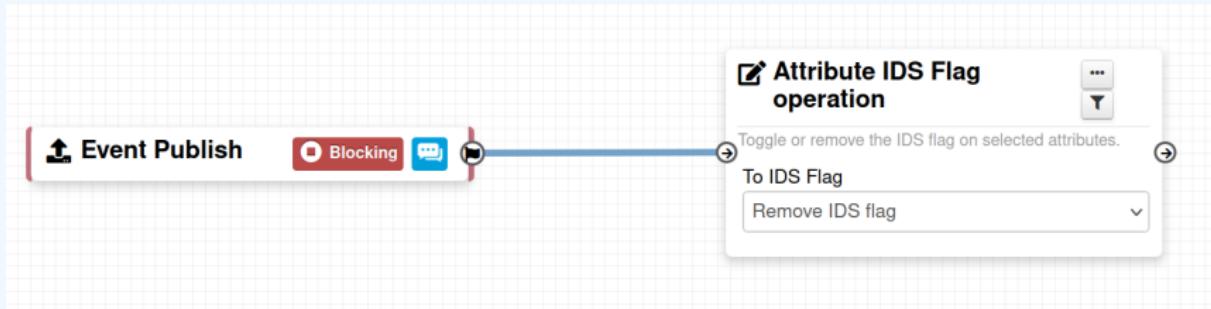
HASH PATH FILTERING - EXERCISE (4)

```
1  {
2      "Event": {
3          "Tag": [...],
4          "Attribute": [
5              {
6                  "value": "8.8.8.8",
7                  "_allTags": [
8                      {
9                          "name": "tlp:green",
10                         "inherited": true,
11                     },
12                     {
13                         "name": "PAP:AMBER",
14                         "inherited": false,
15                     }
16                 ],
17             },
18             ...
19 }
```

4. Access all Tags attached to Attributes and from the Event
 - ▶ `Event.Attribute.{n}._allTags.{n}.name`

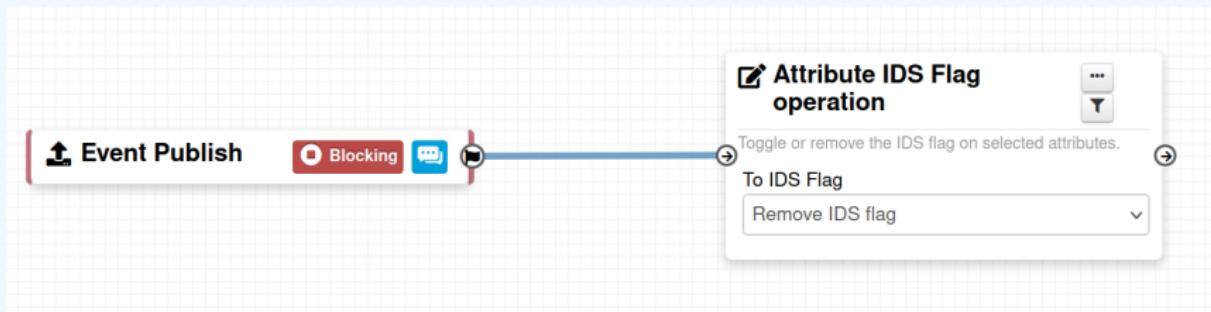
FITLERING DATA ON WHICH TO APPLY A MODULE

What happens when an Event is about to be published?



FITLERING DATA ON WHICH TO APPLY A MODULE

What happens when an Event is about to be published?

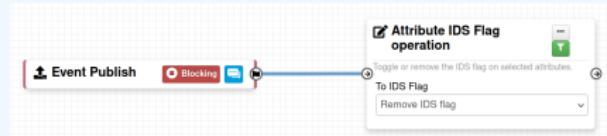


All Attributes get their `to_ids` turned off.

How could we force that action only on Attribute of type comment?

→ Hash path filtering!

FITLERING DATA ON WHICH TO APPLY A MODULE



Node Filtering

Element selector
Event._AttributeFlattened.{n}

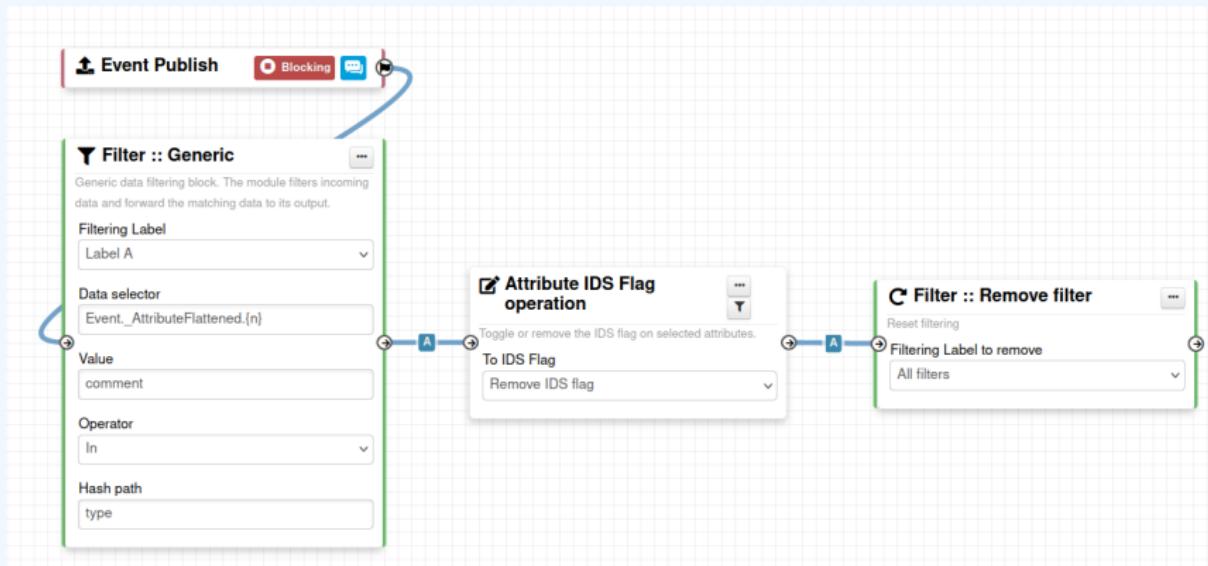
Value
comment

Operator
In

Hash Path
type

FITLERING DATA ON WHICH TO APPLY ON MULTIPLE MODULES

New feature as of **v2.4.171** allows setting filters on a path.



EXERCICES

EXERCISES

Try to build it in the training instance. **Do not save it!**.

1. PAP:RED and tlp:red blocking
2. Replace tlp:white by tlp:clear
3. Attach tag on attribute having a low value (<50) in bgp ranking
4. Remove to_ids flag for attribute having a match in hashlookup

DEBUGGING

DEBUGGING WORKFLOWS: LOG ENTRIES

- Workflow execution is logged in the application logs:
 - ▶ `/admin/logs/index`
 - ▶ Note: Might be phased out as its too verbose
- Or stored on disk in the following file:
 - ▶ `/app/tmp/logs/workflow-execution.log`

Logs

Logs							
Emails		Authentication issues		MISP Update results		Setting changes	
Warnings and errors							
Id ↑	Email	Org	Created	Model	Model ID	Action	Title
49146	SYSTEM	SYSTEM	2022-08-01 07:34:40	Workflow	162	execute_workflow	Finished executing workflow for trigger `enrichment-before-query` (162). Outcome: success
49144	SYSTEM	SYSTEM	2022-08-01 07:34:39	Workflow	162	execute_workflow	Started executing workflow for trigger `enrichment-before-query` (162)

DEBUGGING WORKFLOWS: DEBUG MODE

- The  Debug Mode: On can be turned on for each workflows
- Each nodes will send data to the provided URL
 - ▶ Configure the setting: `Plugin.Workflow_debug_url`
- Result can be visualized in
 - ▶ **offline:** `tools/misp-workflows/webhook-listener.py`
 - ▶ **online:** `requestbin.com` or similar websites

Today		
2:25:10 pm	POST	<code>/end?outcome=blocked</code>
2:25:09 pm	POST	<code>/exec/stop-execution?result=success</code>
2:25:09 pm	POST	<code>/exec/tag-if?result=success</code>
2:25:08 pm	POST	<code>/init?type=blocking</code>

DEBUGGING MODULES: STATELESS EXECUTION

■ Test custom modules with custom input

Stateless module execution

Module parameters

Payload URL

`https://localhost:8443`

Content type

`application/json`

Data extraction path

`Attribute.{n}.AttributeTag.{n}.Tag.name`

Input data

Convert input data into MISP core format

Module Input Data

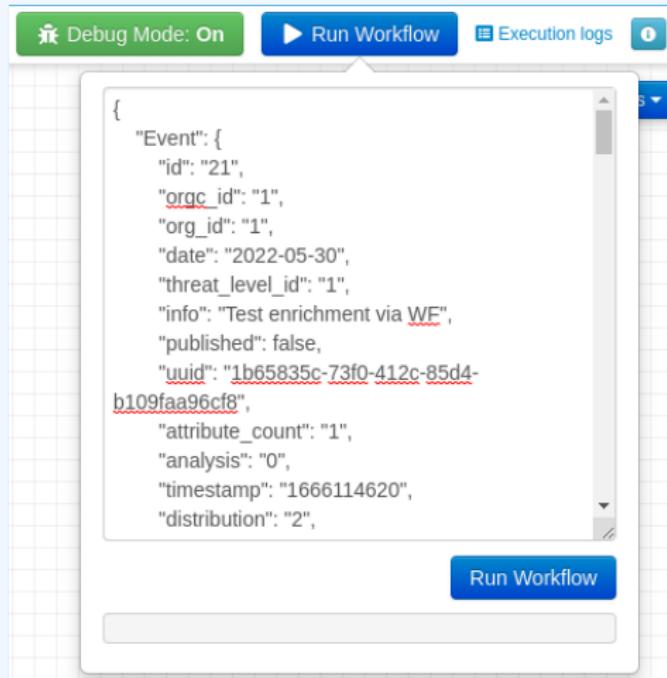
```
{  
    "foo": "bar"  
}
```

Execute module

Execution result: `200 [56 ms]`

DEBUGGING MODULES: RE-RUNNING WORKFLOWS

- Try workflows with custom input
- Re-run workflows to ease debugging

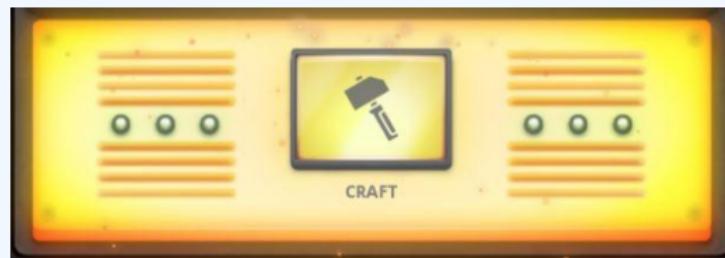


DEBUGGING OPTIONS

- Workflow **execution and outcome**
- Module **execution and outcome**
- **Live** workflow debugging with module inspection
- **Re-running/testing** workflows with custom data
- **Stateless** module execution



EXTENDING THE SYSTEM



CREATING A NEW MODULE IN PHP



- **app/Lib/WorkflowModules/action/[module_name].php**
- Designed to be easily extended
 - ▶ Helper functions
 - ▶ Module configuration as variables
 - ▶ Implement runtime logic
- Main benefits
 - ▶ Fast
 - ▶ Re-use existing functionalities
 - ▶ No need for misp-modules

CREATING A NEW MODULE IN PHP

```
app > Lib > WorkflowModules > action > 🏷 Module_blueprint_action_module.php > ...
1  <?php
2  include_once APP . . . 'Model/WorkflowModules/WorkflowBaseModule.php';
3
4  class Module_blueprint_action_module extends WorkflowBaseModule
5  {
6      public $is_blocking = false;
7      public $disabled = true;
8      public $id = 'blueprint-action-module';
9      public $name = 'Blueprint action module';
10     public $description = 'Lorem ipsum dolor, sit amet consectetur adipisicing elit.';
11     public $icon = 'shapes';
12     public $inputs = 1;
13     public $outputs = 1;
14     public $params = [];
15
16     public function exec(array $node, WorkflowRoamingData $roamingData, array &$errors = [])
17     : bool
18     {
19         parent::exec($node, $roamingData, $errors);
20         // If $this->is_blocking == true, returning `false` will stop the execution.
21         $errors[] = __('Execution stopped');
22         return false;
23     }
}
```

CREATING A NEW MODULE IN PYTHON



- Similar to how other misp-modules are implemented
 - ▶ Helper functions
 - ▶ Module configuration as variables
 - ▶ Implement runtime logic
- Main benefits
 - ▶ Easier than PHP
 - ▶ Lots of libraries for integration

CREATING A NEW MODULE IN PYTHON

```
home > sami > git > misp-modules > misp_modules > modules > action_mod > testaction.py > ...
1 > import json...
3
4 misperrors = {'error': 'Error'}
5
6 # config fields that your code expects from the site admin
7 moduleconfig = {
8     'foo': {
9         'type': 'string',
10        'description': 'blablabla',
11        'value': 'xyz'
12    },
13    'bar': {
14        'type': 'string',
15        'value': 'meh'
16    }
17};
18
19 # blocking modules break the execution of the chain of actions (such as publishing)
20 blocking = False
21
22 # returns either "boolean" or "data"
23 # Boolean is used to simply signal that the execution has finished.
24 # For blocking modules the actual boolean value determines whether we break execution
25 returns = 'boolean'
26
27 moduleinfo = {'version': '0.1', 'author': 'Andras Iklody',
28               'description': 'This module is merely a test, always returning true. Triggers on event publishing.',
29               'module-type': ['action']}
30
31
32 def handler(q=False):
33     if q is False:
34         return False
35     result = json.loads(q) # noqa
36     output = result # Insert your magic here!
37     r = {"data": output}
38     return r
```

SHOULD I MIGRATE TO MISP WORKFLOWS

I have automation in place using the API / ZMQ. Should I move to Workflows?

- I (have/am planning to create) a curation pipeline using the API, should I port them to workflows?
 - ▶ **No** in general, but WF can be used to start the curation process
- What if I want to **block** some actions
 - ▶ Put the blocking logic in the WF, the remaining outside
- Currently, workflows with **lots of node are not encouraged**
- Bottom line is **Keep it simple**

FUTURE WORKS

- More 📹 modules
- More ➔ modules
- More 🏷️ triggers
- More documentation
- Recursion prevention system
- On-the-fly data override?

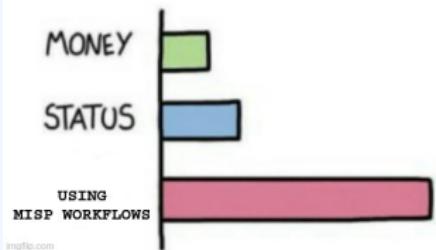


imgflip.com

FINAL WORDS

- Designed to **quickly** and **cheaply** integrate MISP in CTI pipelines
- **Beta** Feature unlikely to change.
But still..
- Waiting for feedback!
 - ▶ New triggers?
 - ▶ New modules?
 - ▶ What's achievable

WHAT GIVES PEOPLE
FEELINGS OF POWER



MISP Concepts Cheat sheet

Glossary

Correlations: Links created automatically whenever an **Attribute** is created or modified. They allow interconnection between **Events** based on their attributes.

Correlation Engine: Is the system used by MISP to create correlations between **Attribute**'s value. It currently supports strict string comparison, SSDEEP and CDIR blocks matches.

Caching: Is the process of *fetching* data from a MISP instance or feed but only storing hashes of the collected values for correlation and look-up purposes.

Delegation: Act of transferring the ownership of an **Event** to another organisation while hiding the original creator, thus providing anonymity.

Deletion (hard/soft): *Hard deletion* is the act of removing the element from the system; it will not perform revocation on other MISP instances. *Soft deletion* is the act flagging an element as deleted and propagating the revocation among the network of connected MISP instances.

Extended Event: Event that extends an existing **Event**, providing a combined view of the data contained in both **Events**. The owner of the extending **Event** is the organisation that created the extension. This allows anyone to extend any **Events** and have total control over them.

Galaxy Matrix: Matrix derived from **Galaxy Clusters** belonging to the same **Galaxy**. The layout (pages and columns) is defined at the **Galaxy** level and its content comes from the **Galaxy Clusters** meta-data themselves.

Indicators: Attribute containing a pattern that can be used to detect suspicious or malicious activity. These **Attributes** usually have their `to_ids` flag enabled.

Orgc / Org: *Creator Organisation (Orgc)* is the organisation that created the data and the one allowed to modify it. *Owner Organisation (Org)* is the organisation owning the data on a given instance and is allowed to view it regardless of the distribution level. The two are not necessarily the same.

Publishing: Action of declaring that an **Event** is ready to be synchronised. It may also send e-mail notifications and makes it available to some export formats.

Pulling: Action of using a user on a remote instance to fetch the accessible data and storing it locally.

Pushing: Action of using an uplink connection via a `sync. user` to send data to a remote instance.

Synchronisation: Is the exchange of data between two (or more) MISP instances through the *pull* or *push* mechanisms.

Sync. filtering rule: Can be applied on a synchronisation link for both the *pull* and *push* mechanisms to block or allow data to be transferred.

Sync. User: Special role of a user granting additional sync permissions. The recommended way to setup *push* synchronisation is to use *sync users*.

Proposals: Are a mechanism to propose modifications to the creating organisations (**Orgc**). If a path of connected MISP instances exists, the **Proposal** will be synchronised allowing the creator to accept or discard it.

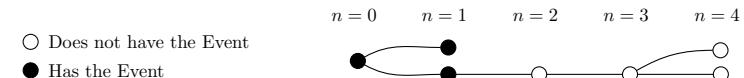
Distribution

Controls who can see the data and how it should be synchronised.

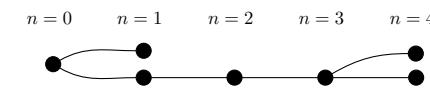
Organisation only: Only members of your organisation

This community: Organisations on this MISP instance

Connected Communities: Organisations on this 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. ($n \leq 1$)



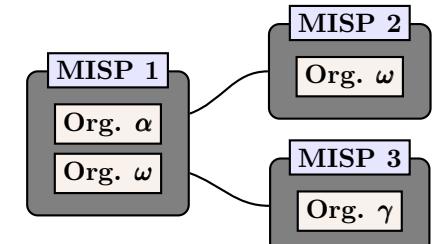
All Communities: Anyone having access. Data will be freely propagated in the network of connected MISP instances. ($n = \infty$)



Sharing Groups: Distribution list that exhaustively keeps track of which organisations can access the data and how it should be synchronised.

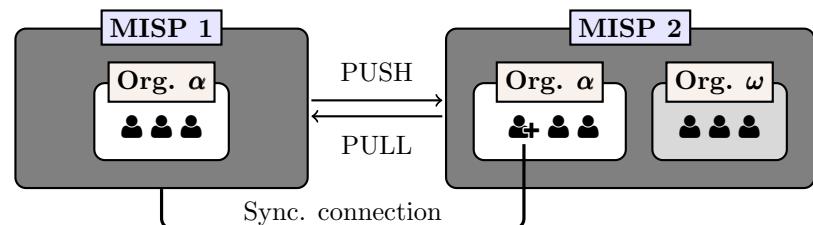
Sharing Group configuration	
Organisations	Org. α Org. ω Org. γ
Instances*	MISP 1 MISP 2 MISP 3

*Or enable roaming mode instead



Synchronisation

The act of sharing where everyone can be a consumer and/or a producer. A one way synchronisation link between two MISP instances. Organisation α created a *sync user* on MISP 2 and noted down the generated API Key. 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 *push* data to MISP 2.



MISP Data Model Cheat Sheet

- ☞ Context such as Taxonomies or Galaxy Clusters can be attached to the element
- ☞ Has a distribution level
- ☞ Can be synchronised to/from other instances

Event

 Encapsulations for contextually linked information.

Purpose: Group datapoints and context together. Acting as an envelop, it allows setting distribution and sharing rules for itself and its children.

Usecase: Encode incidents/events/reports/...

► Events can contain other elements such as Attributes, MISP Objects and Event Reports .

► The distribution level and any context added on an Event (such as Taxonomies) are propagated to its underlying data.

Attribute

 Basic building block to share information.

Purpose: Individual data point. Can be an indicator or supporting data.

Usecase: Domain, IP, link, sha1, attachment, ...

► Attributes cannot be duplicated inside the same Event and can have Sightings .

► The difference between an indicator or supporting data is usually indicated by the state of the attribute's to_ids flag.

MISP Object

 Advanced building block providing Attribute compositions via templates.

Purpose: Groups Attributes that are intrinsically linked together.

Usecase: File, person, credit-card, x509, device, ...

► MISP Objects have their attribute compositions described in their respective template. They are instantiated with Attributes and can Reference other Attributes or MISP Objects .

► MISP is not required to know the template to save and display the object. However, edits will not be possible as the template to validate against is unknown.

Object Reference

 Relationships between individual building blocks.

Purpose: Allows to create relationships between entities, thus creating a graph where they are the edges and entities are the nodes.

Usecase: Represent behaviours, similarities, affiliation, ...

► References can have a textual relationship which can come from MISP or be set freely.

Sightings

 Means to convey that an Attribute has been seen.

Purpose: Allows to add temporality to the data.

Usecase: Record activity or occurrence, perform IoC expiration, ...

► Sightings are the best way to express that something has been seen. They can also be used to mark false positives.

Event Report

 Advanced building block containing formatted text.

Purpose: Supporting data point to describe events or processes.

Usecase: Encode reports, provide more information about the Event , ...

► Event Reports are markdown-aware and include a special syntax to reference data points or context.

Proposals

 Clone of an Attribute containing information about modification to be done.

Purpose: Allow the correction or the creation of Attributes for Events your organisation does not own.

Usecase: Disable the IDS flag, Correct errors

► As Proposals are sync., if the creator organisation is connected to the MISP instance from where the Proposal has been created, it will be able to either accept or discard it.

Taxonomies

 Machine and human-readable labels standardised on a common set of vocabularies.

Purpose: Enable efficient classification globally understood, easing consumption and automation.

Usecase: Provide classification such as: TLP, Confidence, Source, Workflows, Event type, ...

► Even though MISP allows the creation of free-text tags, it's always preferable to use those coming from Taxonomies , if they exist.

Galaxies

 Act as a container to group together context described in Galaxy Clusters by their type.

Purpose: Bundle Galaxy Clusters by their type to avoid confusion and to ease searches.

Usecase: Bundle types: Exploit-Kit, Preventive Measures, ATT&CK, Tools, Threat-actors, ...

Galaxy Clusters

 Knowledge base items used as tags with additional complex meta-data aimed for human consumption.

Purpose: Enable description of complex high-level information for classification.

Usecase: Extensively describe elements such as: threat actors, countries, technique used, ...

► Galaxy Clusters can be seen as an enhanced Taxonomy as they can have meta-data and relationships with other Galaxy Clusters .

► Any Galaxy Clusters can contain the following:

- Cluster Elements: Key-Value pair forming the meta-data.

Example: Country:LU, Synonym:APT28,
Currency:Dollar,
refs:https://*
...

• Cluster Relations (): Enable the creation of relationships between one or more Galaxy Clusters .

Example: Threat actor X is similar to threat actor Y with high-likelihood.

Analyst Notes



Text element that can be attached to many element

Purpose: Share and add an analysis to any MISP data

Usecase: Describe information about specific details, annotate elements

- Any user can attach **Analyst Notes** to data they don't own. For example: **Events** , **Attributes** , **Galaxy Clusters** , ...

- The note is actually attached to the target's UUID

Analyst Opinions



Text element with a numerical opinion that can be attached to many element

Purpose: Share and add an opinion to any MISP data

Usecase: Provide feedback to third-parties, Coordinate and Collaborate

- Basically the same as a **Analyst Note**
- The numerical value of the **Analyst Opinion** is $\in [0, 100]$. where 50 is the neutral point. Any values < 50 are considered negatives, values > 50 are considered positives.

Analyst Relationships



Link between two entities using a verb

Purpose: Create a relationship between elements

Usecase: Manually create correlation link, add similarities

- Basically the same as a **Analyst Note** but includes the target element

- Example could be an **Event** → **Event** relationship where one is *Suspected to be part of the same campaign based on HUMINT sources*

Element Collection



Group element into collection

Purpose: Allow grouppping multiple elements into a single collection

Usecase: Grouping **Events** together if they are part of the same campaing

Failed spear-phishing attempt

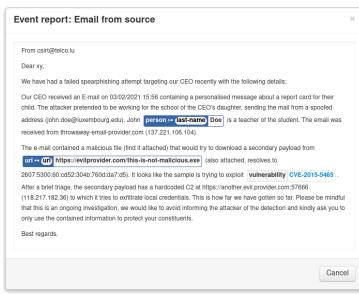
UUID 28b1cd2e-46a7-4ee2-a364-c3d26451b089

Date 2021-12-09

Creator Org. CIRCL.lu
Distribution Connected Communities
Published ✓



> Intelligence Visualization Widgets



> 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: malware-sample	malicious.exe f1a3e62de12faece82bf4599cc1fdcd
□ 2021-12-09	Payload delivery	filename: filename	malicious.exe
□ 2021-12-09	Payload delivery	md5: md5	f1a3e62de12faece82bf4599cc1fdcd
□ 2021-12-09	Payload delivery	sha1: sha1	d836f2ee449b74913d1efc615eb459b65e4f791
□ 2021-12-09	Payload delivery	sha256: sha256	d90401420908dbb43488a306467e8fffc7577ce9d5eee016578ff6a3ada
□ 2021-12-09	Other	size-in-bytes: size-in-bytes	751328

Representation of an incident in MISP

Event: Encapsulates contextually linked information.

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

Event Report: Markdown-aware supporting text document to describe events or incidents. Here: The report describes 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

MISP User & Admin Cheat Sheet

- User -

API

Wildcard searches:

```
POST /attributes/restSearch
{"value": "1.2.3.%"}
```

Or and Negation searches:

```
POST /attributes/restSearch
{"tags": ["tlp:white", "!tlp:green"]}
```

And and Negation searches:

```
POST /attributes/restSearch
{"tags": {"AND": ["tlp:green", "Malware"], "NOT": ["%ransomware%"]}}
```

Galaxy Cluster metadata searches:

```
POST /attributes/restSearch
{
    "galaxy.synonyms": "APT29",
    "galaxy.cfr-target-category": "Financial sector"
}
```

Attach tags:

```
POST /tags/attachTagToObject
{
    "uuid": "[Could be UUID from Event, Attribute, ...]",
    "tag": "tlp:amber"
}
```

Timestamps:

`timestamp`: Time of the last modification on the data

- Usecase: Get data was modified in the last t
- E.g.: Last updated data from a feed

`publish_timestamp`: Time at which the event was published

- Usecase: Get data that arrived in my system since t
- E.g.: New data from a feed

`event_timestamp`: Used in the Attribute scope

- Usecase: Get events modified in the last t

Usage:

```
{"timestamp": 1521846000}
{"timestamp": "7d"}
{"timestamp": ["2d", "1h"]}
```

Tips & Tricks

Get JSON Representation: Append `.json` to any URLs to get their content in JSON format. Example: `/events/view/42.json`

- Admin -

Reset Password

API: POST /users/initiatePasswordReset/[id] {"password": "***"}

CLI: MISP/app/Console/cake Password [email] [password]

Reset Brute-force login protection

CLI: MISP/app/Console/cake Admin clearBruteforce [email]

Upgrade to the latest version

All in 1-shot: MISP/app/Console/cake Admin updateMISP

Manually:

1. cd /var/www/MISP
2. git pull origin 2.4
3. git submodule update --init --recursive
4. MISP/app/Console/cake Admin updateJSON
5. Check live update progress GET /servers/updateProgress

Workers

Restart All: MISP/app/Console/cake Admin restartWorkers

Add: MISP/app/Console/cake Admin startWorker [queue]

Stop: MISP/app/Console/cake Admin stopWorker [pid]

Settings

Get: MISP/app/Console/cake Admin getSetting [setting]

Set: MISP/app/Console/cake Admin setSetting [setting] [value]

Base URL: MISP/app/Console/cake Baseurl [baseurl]

Miscellaneous

Clean Caches: MISP/app/Console/cake Admin cleanCaches

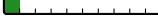
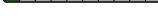
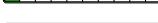
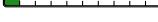
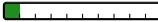
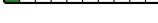
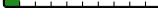
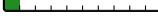
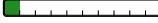
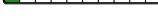
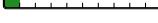
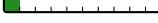
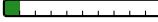
Get IPs For User ID: MISP/app/Console/cake Admin UserIP [user_id]

Get User ID For User IP: MISP/app/Console/cake Admin IPUUser [ip]

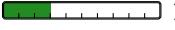
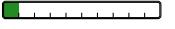
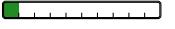
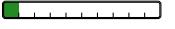
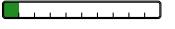
Documentation: /events/automation

Logs files location: MISP/app/tmp/logs

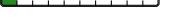
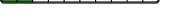
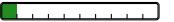
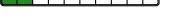
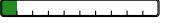
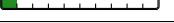
User

Check	Description	Length
<input type="checkbox"/>	Add events	
<input type="checkbox"/>	- via Standard UI	
<input type="checkbox"/>	- Distribution levels and publication	
<input type="checkbox"/>	- Different timestamps & publish_timestamp	
<input type="checkbox"/>	Add attributes	
<input type="checkbox"/>	- Freetext	
<input type="checkbox"/>	- Standard UI	
<input type="checkbox"/>	- Template	
<input type="checkbox"/>	- ReST API	
<input type="checkbox"/>	- via EventGraph	
<input type="checkbox"/>	Object	
<input type="checkbox"/>	- add Object	
<input type="checkbox"/>	- add References	
<input type="checkbox"/>	- show via EventGraph	
<input type="checkbox"/>	*-lists	
<input type="checkbox"/>	- Warninglists: show warnings raised in steps above	
<input type="checkbox"/>	- Noticelists: show warnings when adding data	
<input type="checkbox"/>	- Import Regexp: avoid leaking private/personal data	
<input type="checkbox"/>	Correlations	
<input type="checkbox"/>	- show correlations that were added	
<input type="checkbox"/>	- pivot to events via correlations	
<input type="checkbox"/>	- show correlations graph	
<input type="checkbox"/>	- feeds & servers correlation	
<input type="checkbox"/>	Tags and Galaxies	
<input type="checkbox"/>	- Tag from Taxonomy	
<input type="checkbox"/>	- GalaxyCluster	
<input type="checkbox"/>	- ATT&CK pattern & Galaxy matrix	
<input type="checkbox"/>	- Tag Collection	
<input type="checkbox"/>	Sighting	
<input type="checkbox"/>	- via UI & API	
<input type="checkbox"/>	Delegation	
<input type="checkbox"/>	Proposal	
<input type="checkbox"/>	Delete (including soft versus hard delete)	
<input type="checkbox"/>	- Event blocklist when deleting	
<input type="checkbox"/>	Extending event (how and when to use it)	
<input type="checkbox"/>	Exporting data	
<input type="checkbox"/>	- download from	
<input type="checkbox"/>	- download from via modules	
<input type="checkbox"/>	- .json routing	
<input type="checkbox"/>	- RestSearch	
<input type="checkbox"/>	Searching for data	
<input type="checkbox"/>	- Attribute search	
<input type="checkbox"/>	- Event index filter search	
<input type="checkbox"/>	Advanced features	
<input type="checkbox"/>	- Event graph, Event timeline, Event report	
<input type="checkbox"/>	- Decaying of IoC	
<input type="checkbox"/>	- Galaxy 2.0	
<input type="checkbox"/>	Enrichments	
<input type="checkbox"/>	- Hover & persistent	

Administrator (Community)

Check Description	Length
<input type="checkbox"/> Organisations	 10m
<input type="checkbox"/> - local and remote	
<input type="checkbox"/> - administration: Creation and merge	
<input type="checkbox"/> User	 5m
<input type="checkbox"/> - administration and contact via standard UI	
<input type="checkbox"/> - Pasword/Auth key reset	
<input type="checkbox"/> - Disabling (never remove)	
<input type="checkbox"/> Roles and permissions	 3m
<input type="checkbox"/> - Constraints & special sync-user	
<input type="checkbox"/> Sharing group	 10m
<input type="checkbox"/> - administration via standard UI	
<input type="checkbox"/> Block listing	 3m
<input type="checkbox"/> - Events & Organisations	
<input type="checkbox"/> Synchronisation	 35m
<input type="checkbox"/> - MISP to MISP (sync_user, test & preview, flow control)	
<input type="checkbox"/> - Feeds to MISP (Options, overlap)	
<input type="checkbox"/> - Pub-Sub	
<input type="checkbox"/> Collaboration settings	
<input type="checkbox"/> - 'proposal_block_attributes', 'sanitise_attribute_on_delete', 'Sightings_anonymise'	
<input type="checkbox"/> Templates	
<input type="checkbox"/> - administration via standard UI	

Administrator (Instance)

Check	Description	Length
<input type="checkbox"/>	Advanced Auth keys	 3m
<input type="checkbox"/>	- Migration from old system	
<input type="checkbox"/>	- Usage	
<input type="checkbox"/>	Server settings	 5m
<input type="checkbox"/>	Maintenance	 15m
<input type="checkbox"/>	- Updating & release process	
<input type="checkbox"/>	- Submodules and populate DB	
<input type="checkbox"/>	- Diagnostic	
<input type="checkbox"/>	Jobs and Workers	 10m
<input type="checkbox"/>	- Administration via standard UI	
<input type="checkbox"/>	- Scheduled Tasks and CRON jobs	
<input type="checkbox"/>	User settings & User management	 5m
<input type="checkbox"/>	- User settings	
<input type="checkbox"/>	- User monitoring, self-management, auto-registration	
<input type="checkbox"/>	Logging & auditing	 10m
<input type="checkbox"/>	- Logs (and purge: event history)	
<input type="checkbox"/>	- Paranoid, IP & Auth log, Sync audit	
<input type="checkbox"/>	Troubleshooting	 5m
<input type="checkbox"/>	- Clean cache & DB Schema diagnostic	
<input type="checkbox"/>	- Stuck workers	
<input type="checkbox"/>	- Update in progress	
<input type="checkbox"/>	- Apache logs & workers logs	

MISP Training Slide Decks

MISP¹ is a threat intelligence platform for gathering, sharing, storing and correlating Indicators of Compromise of targeted attacks, threat intelligence, financial fraud information, vulnerability information or even counter-terrorism information.

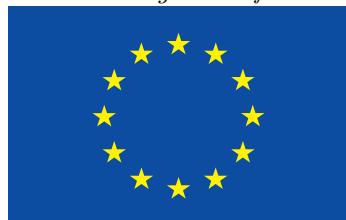
This document includes the slides which are the support materials² used for MISP trainings. The content is dual-licensed under CC-BY-SA version 4 license or GNU Affero General Public License version 3 which allows you to freely use, remixes and share-alike the slides while still mentioning the contributors under the same conditions.

Contributors

- Steve Clement <https://github.com/SteveClement>
- Alexandre Dulaunoy <https://github.com/adulau>
- Andras Iklody <https://github.com/iglocska>
- Sami Mokaddem <https://github.com/mokaddem>
- Sascha Rommelfangen <https://github.com/rommelfs>
- Christian Studer <https://github.com/chrisr3d>
- Raphaël Vinot <https://github.com/rafiot>
- Gerard Wagener <https://github.com/haegardev>

Acknowledgment

The MISP project is co-financed and resource supported by CIRCL Computer Incident Response Center Luxembourg³ and co-financed by a CEF (Connecting Europe Facility) funding under CEF-TC-2016-3 - Cyber Security as *Improving MISP as building blocks for next-generation information sharing*.



Co-financed by the Connecting Europe Facility of the European Union

¹<https://www.misp-project.org/>

²<https://github.com/MISP/misp-training>

³<https://www.circl.lu/>



CIRCL
Computer Incident
Response Center
Luxembourg