

Team CIRCL

MISP Project

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

CanSecWest 2020



MISP
Threat Sharing

- MISP¹ is a threat information sharing free & open source software.
- MISP has **a host of functionalities** that assist users in creating, collaborating & sharing threat information - e.g. flexible sharing groups, **automatic correlation**, free-text import helper, event distribution & proposals.
- Many export formats which support IDses / IPses (e.g. Suricata, Bro, Snort), SIEMs (eg CEF), Host scanners (e.g. OpenIOC, STIX, CSV, yara), analysis tools (e.g. Maltego), DNS policies (e.g. RPZ).
- A rich set of MISP modules² to add expansion, import and export functionalities.

¹<https://github.com/MISP/MISP>

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

- 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 Vandeplass (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 securitymadein.lu g.i.e.

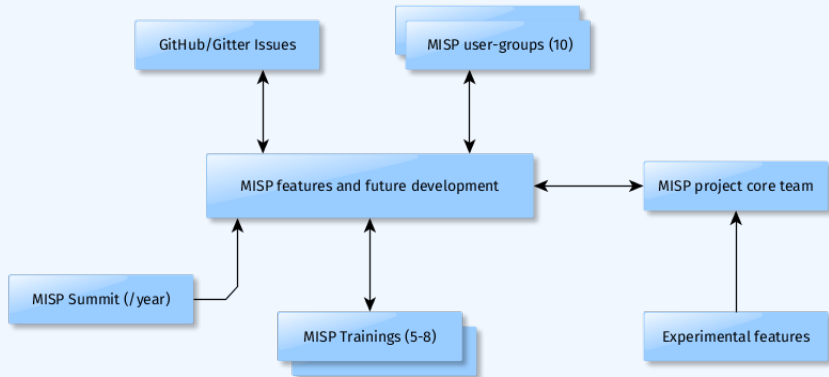
- CIRCL is mandated by the Ministry of Economy and acting as the Luxembourg National CERT for private sector.
- CIRCL leads the development of the Open Source MISP threat intelligence platform which is used by many military or intelligence communities, private companies, financial sector, National CERTs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



Co-financed by the European Union

Connecting Europe Facility

MISP MODEL OF GOVERNANCE



- 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.

- 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 950 organizations with more than 2400 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).

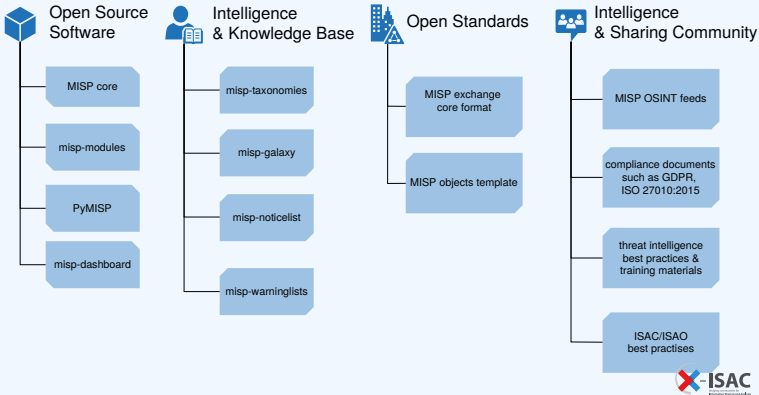
MANY OBJECTIVES FROM DIFFERENT USER-GROUPS

- 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)

- Sharing difficulties are not really technical issues but often it's a matter of **social interactions** (e.g. **trust**).
- Legal restriction³
 - ▶ "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."

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

MISP PROJECT OVERVIEW



- Contributors can use the UI, API or using the freetext import to add events and attributes.
 - ▶ Modules existing in Viper (a binary framework for malware reverser) to populate and use MISP from the vty or via your IDA.
- Contribution can be direct by creating an event but **users can propose attributes updates** to the event owner.
- **Users should not be forced to use a single interface to contribute.**

GETTING SOME NAMING CONVENTIONS OUT OF THE WAY...

■ Data layer

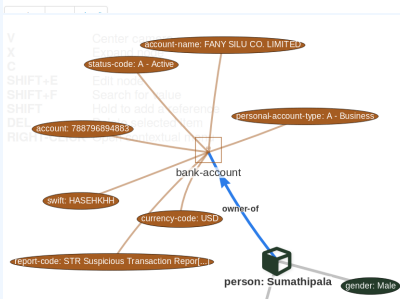
- ▶ **Events** are encapsulations for contextually linked information
- ▶ **Attributes** are individual data points, which can be indicators or supporting data.
- ▶ **Objects** are custom templated Attribute compositions
- ▶ **Object references** are the relationships between other building blocks

■ 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**.

A RICH DATA-MODEL: TELLING STORIES VIA RELATIONSHIPS

Date	Org	Category	Type	Value	Tags	Galaxies	Comment	Correlate	Related Events
2018-09-28		Other	status-code:	A - Active		Add		<input type="checkbox"/>	
2018-09-28		Other	report-code:	STR Suspicious Transaction Report		Add		<input type="checkbox"/>	
2018-09-28		Other	personal-account-type:	A - Business		Add		<input type="checkbox"/>	
2018-09-28		Financial fraud	swift:	HASEH09H		Add		<input checked="" type="checkbox"/>	3849 11320 11584
2018-09-28		Financial fraud	account:	788796894883		Add		<input checked="" type="checkbox"/>	
2018-09-28		Other	account-name:	FANY SILU CO. LIMITED		Add		<input checked="" type="checkbox"/>	
2018-09-28		Other	currency-code:	USD		Add		<input type="checkbox"/>	



CONTEXTUALISATION AND AGGREGATION

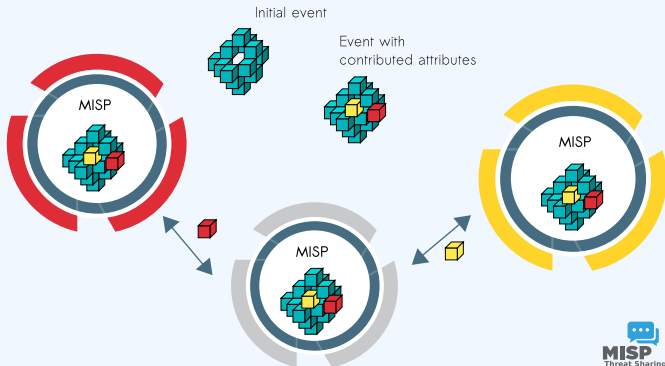
- MISP integrates at the event and the attribute levels MITRE's Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK).

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	Secured 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 Shimring	Rookit	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 Doppelgänger	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	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 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

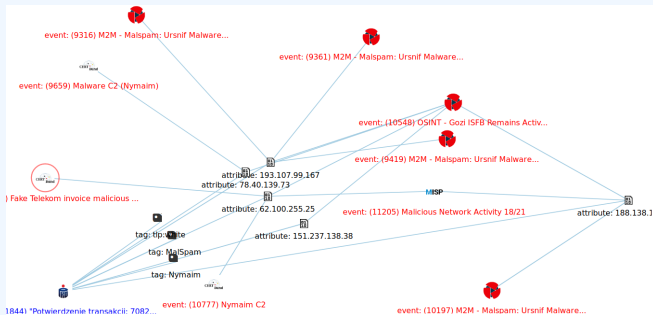
MISP CORE DISTRIBUTED SHARING FUNCTIONALITY

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



- 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



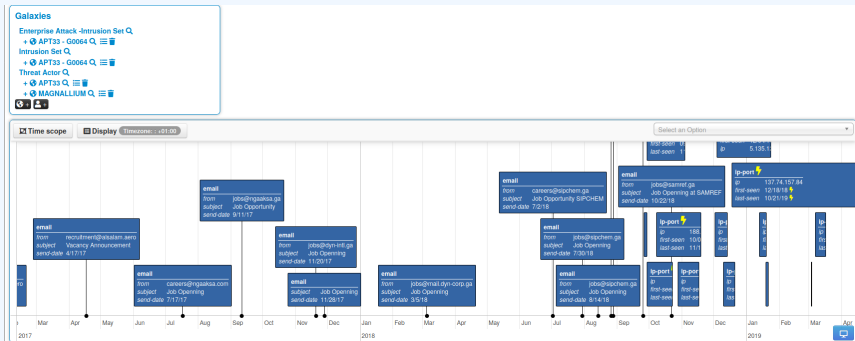
- To **corroborate a finding** (e.g. is this the same campaign?), **reinforce an analysis** (e.g. do other analysts have the same hypothesis?), **confirm a specific aspect** (e.g. are the sinkhole IP addresses used for one campaign?) or just find if this **threat is new or unknown in your community**.

The screenshot displays a user interface for managing sightings. At the top, there is a table with the following columns: 'Events', 'No', and 'Inherit'. The table contains three rows, each with a checkmark in the 'Events' column and a 'No' in the 'No' column. A tooltip is visible over the first row, showing the text 'Sightings' and 'CIRCL: 2 (2017-03-19 16:17:59)'. Below the table, there is a 'Tags' section with a plus sign, a 'Date' field with the value '2016-02-24', a 'Threat Level' field with the value 'High', an 'Analysis' field with the value 'Initial', and a 'Distribution' field with the value 'Connected communities'. A 'Sighting Details' section is also visible, showing a 'No' status, 'MISP: 2', 'CIRCL: 2', and a 'Discussion' button.

- 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

The screenshot shows a web interface for managing indicators. At the top, there are navigation tabs: "Photos", "Galaxy", "Event graph", "Correlation graph", "ATTACK matrix", "Attributes", and "Discussion". Below these is a search bar containing "45: Decay...". A "Galaxies" section is visible with a search icon and a plus sign. Below that are navigation buttons: "previous", "next >", and "view all".

The main content is a table with columns: "Date", "Org", "Category", "Type", "Value", "Tags", "Galaxies", "Comment", "Correlate", "Related Events", "Feed hits", "IDS", "Distribution", "Sightings", "Activity", "Score", and "Actions". The table is filtered by "Decay score" (indicated by a blue toggle button). The table contains five rows of indicators, each with a "Score" column and a "Model 5" button. The scores are: 65.26, 54.6, 37.43, 37.41, and 23.31.

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								Inherit	(0/0)		65.26	
2019-08-13		Network activity	ip-src	8.8.8.8	admirelly-scale:source-reliability="A" x retention:expired x				1 2 2 2 Show S1.1 S1.2 11 more...			Inherit	(5/0)	54.6		
2019-08-13		Network activity	ip-src	9.9.9.9	admirelly-scale:source-reliability="C" x misp:confidence-level="completely-confident" x Ipnumber				1 3 1 9 Show S1.1 28 more...			Inherit	(4/1)	37.43		
2019-08-13		Network activity	ip-src	7.7.7.7	admirelly-scale:information-credibility="4" x retention:20 x				41			Inherit	(3/0)	37.41		
2019-07-18		Network activity	ip-src	6.6.6.6					41			Inherit	(0/0)	23.31		

■ Decay score toggle button

- ▶ Shows Score for each Models associated to the Attribute type

DECAYING OF INDICATORS: FINE TUNING TOOL

Decaying Of Indicator Fine Tuning Tool

Attribute Type | Category | Model ID

Attribute Type	Category	Model ID
aba-rtn	Financial fraud	
authen@hash	Payload delivery	
bank-account-ir	Financial fraud	
bc	Financial fraud	
bin	Financial fraud	
bro	Network activity	10-11
bc	Financial fraud	11
cc-number	Financial fraud	
cd@hash	Payload delivery	
community-id	Network activity	
domain	Network activity	
domain@ip	Network activity	10-94
email-attachment	Payload delivery	
email-otp	Network activity	11
email-otp	Payload delivery	
headers	Payload delivery	
headers/authen@hash	Payload delivery	
headers@ipfuzzy	Payload delivery	
headers@ip@hash	Payload delivery	
headers@ip@f5	Payload delivery	13
headers@ip@hash	Payload delivery	13
headers@ip@h1	Payload delivery	13

Polynomial

Score

Days

Lifetime: 3 days

Decay speed: 2.3

Cutoff threshold: 30

Expire after (lifetime): 1 days and 7 hours

Score halved after (Half-life): 0 day and 6 hours

Adjust base score | Simulate this model

Phishing model | Simple model to rapidly decay | Rate

Parameters														
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 phishing website	Polynomial	3	2.3	30	80	estimate-language phishing	0.5	0.5	9	✓	Test 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,
  "includeDecayed": 0,
  "decayingModel": [8],
  "tag_id": 1,
  "tags": ["estimative-language"], "priority-levels": ["interior"], "timestamp.timezone": ""
}
```

[Search](#)

Base score Base score configuration not set. Use default value 80.

Tag	Computation	ERT Ratio	Value	Result
<code>reap.confidence-level="usually-confident"</code>	0	X	75.00	0
<code>reap.confidence-level="fairly-confident"</code>	0	X	50.00	0
<code>generally-scale:source-reliability="x"</code>	0	X	100.00	0
<code>retention:expired</code>	0	X	NaN	0
<code>base_score</code>				80.00

Sighting: [Wed Sep 4 12:18:09 2019](#) Current score: [54.60](#)

Date	Score
Aug 1	80
Aug 15	55
Aug 25	80
Aug 30	55
Sep 10	80
Sep 15	50
Sep 25	80
Sep 30	50
Oct 10	55
Oct 20	45
Nov 1	30
Dec 1	10
Dec 31	0

← previous next →

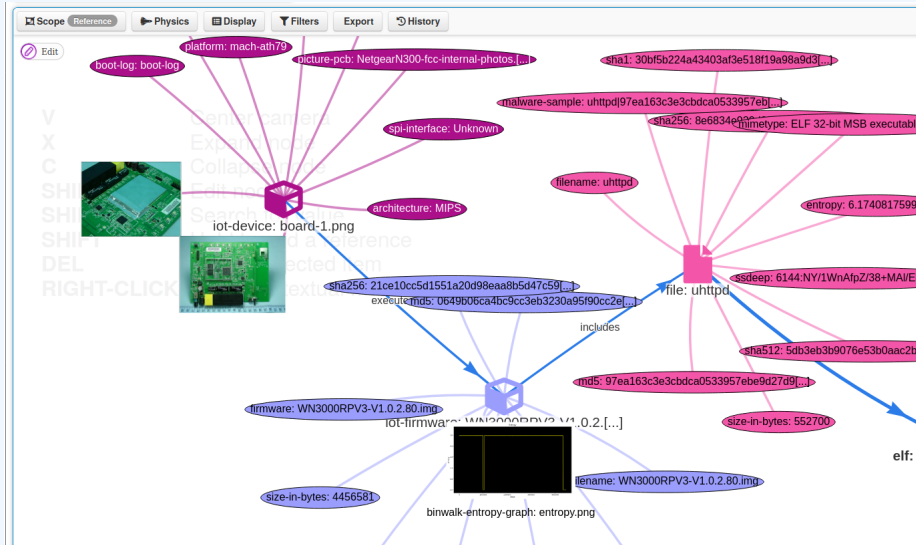
ID	Event #	Date	Org	Category	Type	Value	Tags	Event Tags	Galaxies	Comment	IDS	Sightings	Score
36758	45	2019-08-13	ORIGNAME	Network activity	ip-sic	7.7.7.7	<code>generally-scale:information-credibility="x"</code> <code>retention:2d</code>	<code>reap.confidence-level="usually-confident"</code> <code>reap.confidence-level="fairly-confident"</code>			✓		NIDS Simple Decaying ... 37.41
36757	45	2019-08-13	ORIGNAME	Network activity	ip-sic	8.8.8.8	<code>generally-scale:source-reliability="x"</code> <code>retention:expired</code>	<code>reap.confidence-level="usually-confident"</code> <code>reap.confidence-level="fairly-confident"</code>			✓		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*

DOCUMENTING IOT HARDWARE REVERSING IN MISP



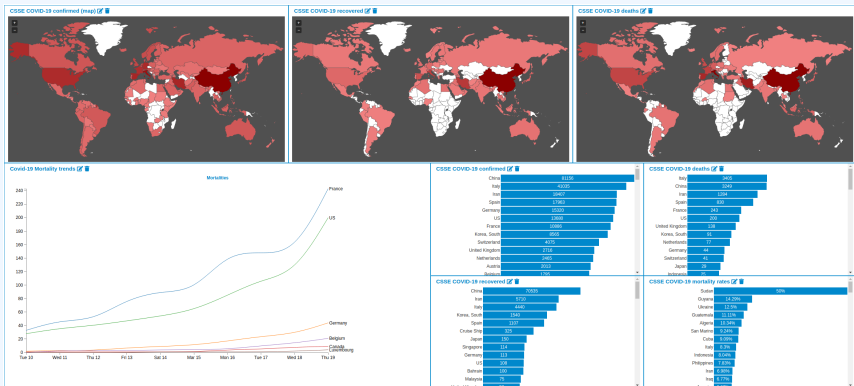
<https://github.com/Cookie-/workshop-materials>

ALTERNATE USE-CASES OF MISP... COVID-19

2020-03-20		Name: covid19-csse-daily-report [🔗]		
		References: 0 [🔗]		
<input type="checkbox"/>	2020-03-20	Other	country-region: Belgium text	 
<input type="checkbox"/>	2020-03-20	Other	update: 2020-03-19T11:13:17.000000+0000 datetime	 
<input type="checkbox"/>	2020-03-20	Other	confirmed: 1795 counter	 
<input type="checkbox"/>	2020-03-20	Other	death: 21 counter	 
<input type="checkbox"/>	2020-03-20	Other	recovered: 31 counter	 

Build objects for completely different use-cases

ALTERNATE USE-CASES OF MISPP... COVID-19



DM us via <https://twitter.com/MISPPProject> for access to the COVID-19 community

- **Information sharing practices come from usage** and by example (e.g. learning by imitation from the shared information).
- MISIP 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 MISIP to meet their community's use-cases.
- MISIP project combines open source software, open standards, best practices and communities to make information sharing a reality.

- <https://www.misp-project.org/>
- <https://www.misp-standard.org/>
- <https://github.com/MISP>
- info@misp-project.org
- <https://twitter.com/MISPProject>