An Introduction to Cybersecurity Information Sharing

MISP - Threat Sharing

Team CIRCL

MISP Project
https://www.misp-project.org/

MISP Virtual Covid Training

COVID-19 MISP INTRO

- COVID-19 MISP is a MISP instance retrofitted for COVID-19 info sharing
- We are focusing on two areas of sharing:
  - **Medical** information
  - **Cyber threats** related to / abusing COVID-19
- Low barrier of entry, aiming for wide spread
- Already a **massive community**

Why?

- We are obviously interested on a personal level, as is everyone
- **Information sharing is what we do anyway**
- The tools that we are building are expanding our capabilities for the future
- Bridging different domains affected in different ways can reveal correlations

Who is this meant for?

- Anyone wanting to gain **situational awareness** for the current situation
- Security practicioners trying to fend off covid related attacks
- Those wanting to share, collaborate, visualise, automate data
- All data is contextualised as **either medical or security** related information for easy filtering

What is MISP?

- MISP[1] 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 modules[2] to add expansion, import and export functionalities.

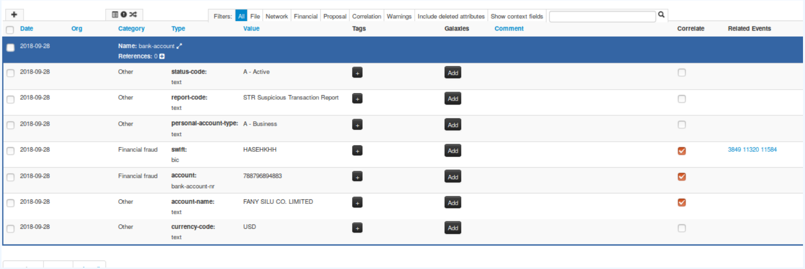
[1] https://github.com/MISP/MISP

[2] https://www.github.com/MISP/misp-modules

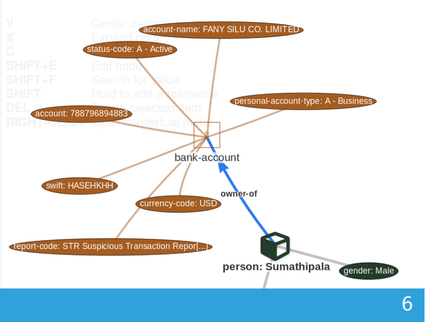
Getting some naming conventions out of the way...

- 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

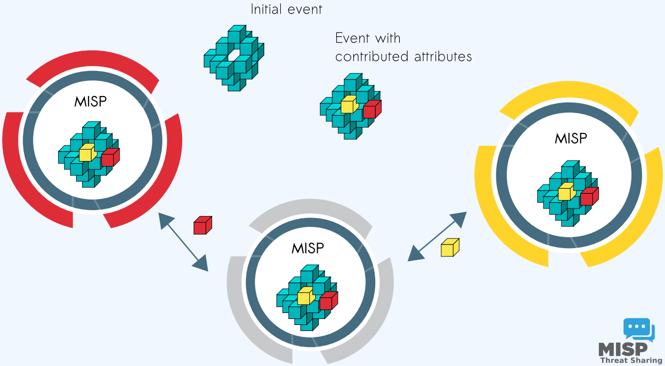

+
Filters: All File Network Financial Proposal Correlation Warnings Include deleted attributes Show context fields

□	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		☑	3849 11320 11584
□	2018-09-28		Financial fraud	account: bank-account-nr	788796894883	+	Add		☑	
□	2018-09-28		Other	account-name: text	FANY SILU CO. LIMITED	+	Add		☑	
□	2018-09-28		Other	currency-code: text	USD	+	Add		□	



MISP CORE DISTRIBUTED SHARING FUNCTIONALITY

- MISP is a **peer to peer** sharing software
- As such, everyone can be a **consumer** and/or a **producer** of information.
- Immediate benefit without the obligation to contribute.
- Low barrier of entry to get acquainted with the system.



Initial event

Event with
contributed attributes

MISP

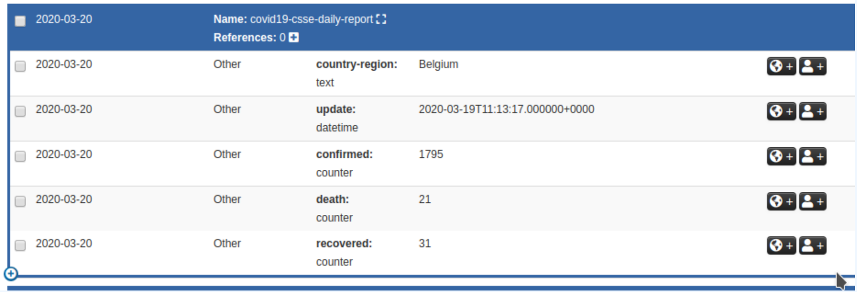
MISP

MISP

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**

Modelling new data structures for COVID-19



□	2020-03-20	**Name:** covid19-csse-daily-report **References:** 0		
□	2020-03-20	Other	**country-region:** text	Belgium
□	2020-03-20	Other	**update:** datetime	2020-03-19T11:13:17.000000+0000
□	2020-03-20	Other	**confirmed:** counter	1795
□	2020-03-20	Other	**death:** counter	21
□	2020-03-20	Other	**recovered:** counter	31

We are rapidly building new models for the different COVID-19 related information sources

Demo time

- View data
- Dashboards
- Create medical data
- Create cyber security data

How can you get involved?

- Join the COVID-19 community
- Either just use the data, or contribute data back, examples:
  - Ongoing Covid-19 phishing campaigns
  - Sharing warninglists of known valid covid-19 related websites
  - Local articles about the situation in your area
  - Best practice recommendations
  - Informations on travel restrictions
- Create **pull requests**
- Share your ideas

Contact us

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