Quick intro into Information Sharing using MISP for CSIRTs

Team CIRCL
TLP:WHITE

FIRST and AfricaCERT Virtual Symposium 2021 December
What is MISP?

- MISP is a **threat information sharing** platform (TISP) 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
MISP AND CIRCL

Who are we?
- Luxembourg National CERT for private sector
- Funded by the Ministry of Economy to build security for the community
- Also co-funded by the EU for various projects, including MISP

What is our involvement with MISP?
- We are leading the development of the OSS platform and related projects
- Manage a large set of communities (Cyber security, LAE, Military, intelligence, financial sector, etc)
- Are both heavy users and data producers as a national CERT
Why would you choose OSS?

- We all operate with set budgets
- Different ways of spending the budget on tooling:
  - **Purchase services**
    - At the *mercy of service provider*
    - Data often *not* kept in *own network*
    - Least own effort involved
  - **Purchase tools**
    - Involves *some maintenance effort*
    - Data kept in *own network*
    - Budget spent mostly on *licensing and support*
  - **Use OSS**
    - Most effort required
    - Budget goes into *growing staff, building expertise*
    - *Reusable skills*, ability to custom tailor the tooling
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
- CSIRTs being enablers of information sharing
MISP as part of the Core services

- **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 **AIL**¹)

¹https://github.com/CIRCL/AIL-framework
Proactive services

- **Contextualising** both internal and external data
- **Collection** and **dissemination** 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)
Advanced services

- 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
  - We’re planning on starting a series of hackathons to find
Report non-identifying information about incidents

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, border control, etc)
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!
Information sharing, besides the obvious benefits, is a great tool to **raise maturity**.

Besides sharing data, share analysis methods, classification standards.

Include guidance on how to make use of the data.

Share homegrown scripts, detection tools along with your analysis.

Realise that CTI information sharing has one main requirement: Trust.

Make sure your sharing programme is accompanies by **offline community building**.
What do I need to get started?

- For FIRST members, log into the FIRST.org MISP instance
- Join national, sectorial, topical MISP communities
- **Set up your own instance.** All you need is a server you can spare.
- **Interconnect** your MISP with the instances or your MISP, or simply give them access
Also, MISP is just one tool of many out there.

Full chain of OSS tools, covering most CSIRT needs

For community management, have a look at Cerebrate²

▶ New project, still heavily WiP - help us shape the tool!
▶ Part of Melicertes II - toolkit for CSIRTs
▶ Community management, tool interconnection orchestration, fleet management

²https://github.com/cerebrate-project/cerebrate
So what do you get out of all of this?

- A structured, actionable yet expressive knowledge-base of relevant threat intel
- Data from your internal work, OSINT, data shared by your partners and vendors
- A way to collaborate rapidly on ongoing incidents
- The tools and methods to raise the maturity of your community.
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://github.com/MISP
https://gitter.im/MISP/MISP
https://twitter.com/MISPProject