MISP workshop

Introduction into Information Sharing using

Team CIRCL

TLP:CLEAR

MISP Project

Plan for this session

- Explanation of the CSIRT use case for information sharing and what CIRCL does
- Building an information sharing community and best practices[1]
- Quick demo of MISP capabilities

[1] We 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-ISAC[2]
  - **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 community[3]
  - Work on attacker modelling
  - With the assistance of MITRE themselves
  - Unique opportunity to **standardise on TTPs**
  - Increasing the use of TTPs[4] especially in sharing community like MITRE ATT&CK
  - Major increase of MITRE ATT&CK context in sharing communities

[3] https://www.attack-community.org/
[4] Tactics, Techniques and Procedures

Communities supported by CIRCL

- ISAC / specialised community MISPs
  - 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

CSIRT core services

- 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 **AIL**[5])

[5] https://www.ail-project.org/

CSIRT PROACTIVE SERVICES

- **Contextualising** both internal and external data
- **Collection** and **dissimination** 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)

CSIRT 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

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**

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 immitation
- 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 possibily 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 valueable 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 MISPProject 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?'
- $\rightarrow$ 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

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 bootstraping 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/MISPProject