

MISP WORKSHOP

INTRODUCTION INTO INFORMATION SHARING USING

TEAM CIRCL
TLP:WHITE

CIISI-IE



MISP
Threat Sharing

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

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

- 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

- 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

- 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/>

- 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

- 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 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 **AIL**⁵)

⁵<https://www.ail-project.org/>

- **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)

- 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)

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

- 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 IMITATE 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."

- 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**

- 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

- 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**

- 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)

- **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

- 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

- 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!

- 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>