Introduction to MISP and ISACs

The importance of sharing communities

Team CIRCL

TLP:CLEAR

AusCERT 2024

Agenda

- CIRCL, MISP and ISACs

- Motivations for sharing communities
- How to get going?
- Managing information sharing communities

- The importance of contextualisation
- False-positive handling
- Features for analysts

CIRCL, MISP and ISACs

CIRCL's involvement

- 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**

- We use MISP 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

Communities operated by CIRCL

- Private sector community
  - Our largest sharing community
  - Over **1900 organisations**
  - Over **4800 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**

Communities supported by CIRCL

- ISACs / specialised community MISPs
  - Topical or community specific instances hosted or co-managed by CIRCL
  - Examples, CIISI, GSMA, FIRST.org, CSIRT network, etc
  - Often come with their **own taxonomies and domain specific object definitions**
- Various ad-hoc communities for exercises
  - The ENISA exercise
  - Locked Shields exercise

Why creating a sharing community?

Development based on practical user feedback

- 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, likelyhood and occurences
  - **Fraud analysts** willing to share financial indicators to detect financial frauds

Usual sharing scenarios for ISACs

- Exchange of **IOCs** and **TTPs**
- Sharing the outcomes of **incidents**
- Information on the **attackers, techniques used**
- **Remediation** information / **prevention** information
- **Vulnerability** pre-disclosure
- Supporting **tools** / **scripts**

Examples of sharing scenarios for sectorial ISACs

- **Financial fraud** information sharing
- **Law enforcement** / Border control specific sharing
- **Disinformation** sharing
- **Health** related information sharing
- **Telecommunication** threat sharing

Objectives can be mixed

- Different use-cases have conflicting requirements for the data shared
  - **False positive** appetite
  - **Capability**/**Maturity** levels
  - **Topical** interests
  - **Detection rules** vs **threat intel** vs **remediation/prevention** support

Reconciling the different use-cases

- For inclusiveness, be lenient with what you allow
- Make **contextualisation** a requirement
- Users can then **filter** based on their needs
- Encourage the sharing of **supporting materials, scripts, guidance**
- Raise awareness about the benefits of well modelled, graph based information sharing

Bringing different sharing communities together

- Getting your community to be active takes **time and effort**, but with persistence your chances are great
- 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**

How to get going with your sharing community?

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...

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

Running a sharing community using MISP - How to get going?

- Planning ahead for future growth
  - Estimating requirements
  - Deciding early on common vocabularies
  - Offering services through MISP

- Different models for constituents
  - **Connecting to** a MISP instance hosted by the ISAC
  - **Hosting** their own instance and connecting to ISAC's MISP
  - **Becoming member** of a sectorial MISP community that is connected to ISAC's community

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 contextualised?
  - What do you consider as useful information?
  - What tools did you use to get your conclusions?
  - How the information could be used by the ISAC members?
- Side effect is that you will end up **raising the capabilities of your constituents**

Managing your sharing community

What counts as valuable data?

- Sharing comes in many shapes and sizes
  - Sharing results / reports is the classical example
  - Sighting of indicators
  - Sharing enhancements to existing data
  - Validating data / flagging false positives
  - Asking for support 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 that want to stay above the thresholds will start sharing junk / fake data
  - Organisations losing access are the ones who would possibily benefit the most from it
  - You lose organisations that might turn into valuable contributors in the future

- Constituents have access to and can **use the data**

So how does one convert the passive organisations into actively sharing ones?

- Rely on **organic growth**
- **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
- 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."
- 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."

A quick note on compliance...

- MISP project collaborated with legal advisory services
  - Information sharing and cooperation **enabled by GDPR**
  - **ISO/IEC 27010:2015** - Information security management for inter-sector and inter-organizational communications
  - How MISP enables stakeholders identified by the **NISD** to perform key activities
  - Guidelines to setting up an information sharing community such as an ISAC or ISAO
- For more information: https://www.misp-project.org/compliance/

The tough choice of separating a community

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 an ISAC 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!

The importance of contextualisation

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
  - 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

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)

False-positives 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**

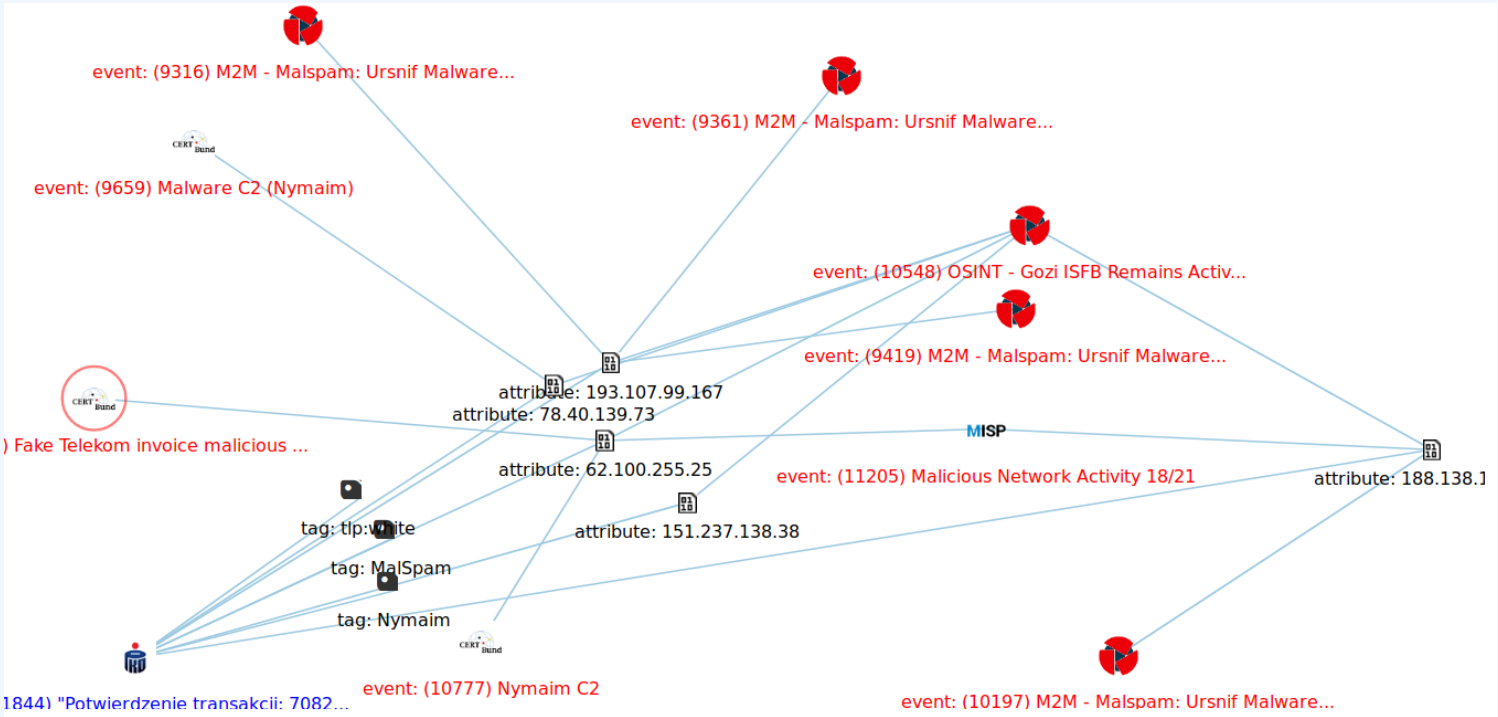
False-positive handling

- **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

Interesting visual features for analysts

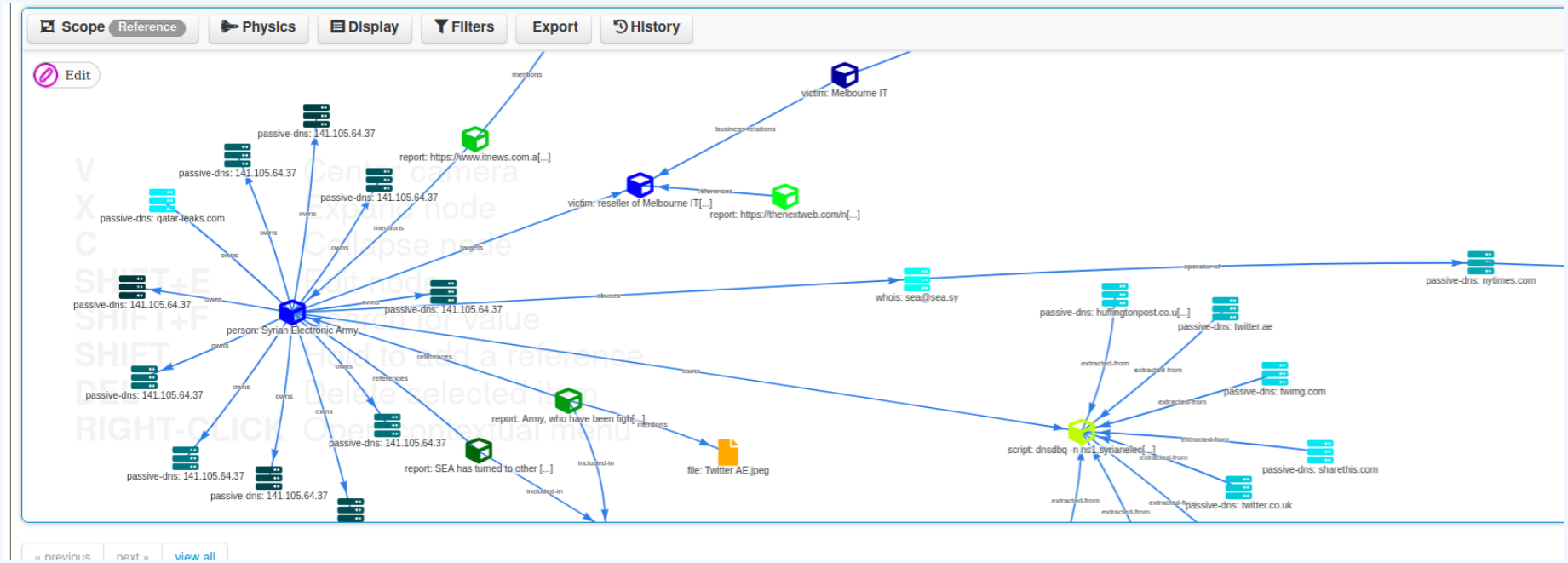
MISP FEATURE - CORRELATION

- MISP includes a **powerful engine for correlation** which allows analysts to discover correlating values between attributes
- Getting a direct benefit from shared information by other ISAC members



MISP FEATURE - EVENT GRAPH

- **Analysts can create stories** based on graph relationships between objects, attributes
- ISACs users can directly understand the information shared



Conclusion

Conclusion and additional challenges

- MISP is a complete and advanced tool ...
- ... but also **just one part of the puzzle** in any sharing community
- Information sharing presumes knowledge of **contacts**
- Member to Member direct **exchanges between MISPs and other tools** requires some know how
- Creating reusable community-specific **distribution lists** need to be maintained
- Maintaining common **community specific information knowledgebases** can be challenging
- **Fleet management** for larger organisations needs additional work
- There's a European project and an open-source tool we are developing to address these points

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://github.com/MISP
  https://gitter.im/MISP/MISP
  https://twitter.com/MISPProject