CTI
How to get your community sharing

CIRCL
Computer Incident
Response Center
Luxembourg

Andras Iklody - *TLP:WHITE*

MISP
Threat Sharing

ENISA - CTI - Rome

How to get your community sharing

- One of the biggest challenges for any sharing community is **getting your user-base to start sharing**
- As CIRCL, we operate sharing communities for the private sector, CERT community, financial sector and more, spanning 850+ organisations
- One of the largest challenges was getting an important message across:
- **Sharing isn't only about sharing fully vetted, final, 100 percent accurate reports**

How can low maturity organisations start sharing?

- Organisations lacking the capability to do the analysis themselves still have **valuable input**!
  - **Validating the information** they receive (pointing out false positives for example)
  - **Proposing improvements** to the information they receive (based on other data source, experience with the data)
  - Providing **sightings**
- But most importantly perhaps, by **pre-sharing** and **collaborating on ongoing analysis efforts**

Collaboration and pre-sharing, or why we should kill the feed provider/consumer model

- We have to realise that it's rare that anyone has the **full picture** in regards to a threat
- **Crowd sourcing** information vetting and enhancing the information gives massive benefits
- Always **treat your threat intel information as incomplete and evolving**
- Leverage **your community's analysis power**, share whatever you can **as early as you can**. If you have a malicious file that looks interesting, share it before you know what's really going on

Show your community the value of sharing as opposed to requiring them to share

- We have been running and interacting with various sharing communities for over 5 years now
- Failed models to motivate the userbase to share that we've encountered:
    - **Requirements** of sharing to receive information
    - Using the potential effects of **peer pressure** as an argument to share
- Conclusion: Focus on the **added value** instead. Crowd sourced analysis, vetting, feedback loop

Cross-sectoral sharing

- Sharing communities and ISACs / governmental institutions / Vendors often stuck in **silos**
- Threats often affect **multiple sectors / communities**
- Try to ensure that these sectors/communities are **able** to exchange data
- **Provide facilities for them to share whatever is their day to day activity** in addition to what you are interested in
- **X-ISAC** operated by CIRCL, aiming to bridge communities. E-mail us at info@circl.lu