CTI and Automation
Supporting CSIRT capabilities and reduce manual operations

CIRCL
Computer Incident
Response Center
Luxembourg

Alexandre Dulaunoy - *TLP:WHITE*

MISP
Threat Sharing

ENISA - CTI - Rome

Background

- CSIRTs/CERTs often rely on **small teams** and especially with **tight resources**.
- Retaining staff within the security field can be challenging especially for highly skilled and curious people.
- Diversity and versality are significant in incident response tasks.
- **Automation** can support CSIRTs/CERTs to reduce workload or **improve quality of the tasks to be performed**.
- Sharing and ratio of capability for processing at receiving CSIRT.

Common tasks where automation can help

- **Gathering intelligence** and information to discover vulnerable systems, compromised devices, active attacks or leaked information.
- **Notification** towards constituents and outside constituency about compromised or vulnerable infrastructures (e.g. **take-down**).
- Notification towards constituents about current threats, associated risks and potential remediations.
- Provide **situational awareness** including statistics or the trend about specific threats.

User groups and usage scenarios in cyber-threat intelligence

- As lead in the MISP project, the **usage scenarios and user groups increased significantly in the past years**.
- Cyber-threat "intelligence" sharing now encompasses a varity of new scenarios to support new types and approaches of sharing information.
- At CIRCL, information shared is no more limited to cyber-security indicators but also includes **financial fraud attributes, vulnerabilities, or even defense mechanisms along with the associated threat information**.
- By so, target groups evolved including security analysts but also financial fraud analysts, law enforcement officers, risk managers or often non-technical groups.

Information sharing and automation at CIRCL

- Automation of the CSIRT core activities including take-down notifications[1] via MISP acting as a CTI platform.
- Provide **actionable threat intelligence** for our constituency (including export NIDS rulesets (Suricata, Snort, Bro), RPZ, CSV, STIX or MISP format).
  - Level of capabilities from our partners or constituency are very different (from no automation to a complete CTI process).
  - Many **legacy tools** in different sectors. We usually try to support the legacy format to create an incentive for automation.
  - **Sighting** is a critical step to get feedback from the data shared including the handling of false-positive, true-positive or expiration.

[1] `https://github.com/rommelfs/misp-takedown`

Information sharing and sighting

- Adequate sightings can be an incredible source of information in order to describe the **life-time of an indicator**, its evolution and especially to ensure the understanding of indicators among a group of users using the information to detect, mitigate or block malicious activities in their infrastructures.
- **Sighting API** can be a challenge depending of the devices where the sighting comes from.
- Sighting in MISP now includes type[2] (e.g. false-positive, expiration) along with source and timestamp to **contextualise the sighting**.

[2] `http://www.misp.software/2017/02/16/Sighting-The-Next-Level.html`