MISP 8 Commandments

Recommendations and Best Practices when encoding data

Ressource

- Best practices in threat intelligence document
  - https://www.misp-project.org/best-practices-in-threat-intelligence.html

C.1 - Event creation

- Use English if you ever think the data will be shared with others
  - `Event.info` is meant for human
  - Concise & self-explanatory title
- Cluster the data properly
  - An event is meant to group contextually linked data
  - Do not merge multiple incidents / reports into one event
- Take time to **properly encode**
  - This is what everyone see and get notified about
  - Make things easier to filter, export, aggregate and compute trends
  - Once you are at ease with the manual work, automate it!

C.2 - Prefer to use object rather than attributes

- You can group attribute and make things **more readable**
- You can turn flat data into a **connected graph** that tells a story
- You have more freedom to **express non-standard** technical indicators thanks to the flexible templating system

C.3 - Review the `to_ids` & `correlation` flags

- `to_ids`: Should it be marked to be used for automation and fed to protective tools
- `correlation`: Should it (not?) correlate

C.4 - Contextualize your data

- Start with the Event: Attributes and Objects **inherit** this context when searching / exporting data
- If possible, **attach context to attributes** as well
  - E.g. c2 server, exfiltration URL, techniques
- Once you **agree on which taxonomy/galaxy** to use, keep using it
  - Makes it easier for you & recipients for understanding, parsing and automation

Priority when contextualizing:

1. Releasability and Permissible actions
2. Adversary tactics and techniques
3. Event class (`misp:event-type`, `event-classification`)
4. If malware involved -> malware-type / family
5. If incident -> Incident type

C.5 - Add a time component (`first_seen`/`last_seen`)

- You get **automatic timelines** for free
- Useful to quickly describe a sequence of actions or when something was active
- These data point **can be leveraged** by the life-cycle management system

C.6 - Check the warninglist hits

- Allow to avoid common false positives
- Do not make SOC and partners angry

C.7 - Create a small write-up with an event report

- Event reports cannot be automated…
- **But**, for incident-response and/or analysts can help them understand in-depth what this event is about

C.8 - Review distribution and publish

- Avoid data leak & make sure everything will be shared as intended
  - Protect potential victims, hide internal references, …
- Publishing is needed for
  - Synchronization to other MISP instances
  - Exposing the data to (some) export format such as suricata, snort, …