MISP and the information sharing standards

CIRCL
Computer Incident
Response Center
Luxembourg

MISP
Threat Sharing

Alexandre Dulaunoy @adulau

TLP:WHITE

MISP Summit II

October 23, 2016

The nice thing about standards is that you have so many to choose from.

Computer Networks, 2nd ed., p. 254. Andrew S. Tanenbaum

(some) Threat sharing standards

- Structured Threat Information eXpression STIX 1.x, CybOX 2.x
- Structured Threat Information eXpression STIX 2.x (CybOX 3.x)
- Open Threat Partner eXchange OpenTPX 2.2.0
- Incident Object Description Exchange Format IODEF
- Facebook ThreatExchange format
- OpenIOC, ITU-T SG17, ...

Background of the MISP standard specifications

- The MISP standard specifications were not designed before implementation.
- MISP specifications are based from the real implementation cases ("code is law").
- **We received many requests of vendors or software developers willing to integrate MISP**.
- So we decided to write the specifications to support organizations who want to use and integrate MISP formats.
- $\rightarrow$ **to remove ambiguities and to scale better**.

Current specification status

- **misp-core-format** - the core JSON format of MISP. IETF Internet-Draft published.
  - Event format including meta-information, attributes, shadow attributes.
  - Manifest format to bundle MISP event.
- **misp-taxonomy-format** - the taxonomy JSON format of MISP. IETF Internet-Draft published.

Future specification

- **misp-galaxy-format** - format used to expand the threat actor modelling of MISP.
- **misp-modules-protocol** - protocol used between MISP and misp-modules.
- **misp-collaborative-voting-format** - describes the collaborative voting and scoring format for the feeds providers.

Q&A

- info@circl.lu (if you want to join the CIRCL MISP sharing community)
- OpenPGP fingerprint: 3B12 DCC2 82FA 2931 2F5B 709A 09E2 CD49 44E6 CBCD
- `https://github.com/MISP/misp-rfc`
- `https://github.com/MISP/` - `http://www.misp-project.org/`