OASIS TC - STIX - Open Points

MISP - Malware Information Sharing Platform & Threat Sharing

CIRCL
Computer Incident
Response Center
Luxembourg

Alexandre Dulaunoy -
Andras Iklody - *TLP:WHITE*

September 26, 2016

MISP and OASIS CTI TC

- MISP team is actively reviewing the current work within the TC (especially STIX).
- MISP data format are **misp-core** [fully implemented], **misp-taxonomies** [fully implemented], **misp-objects** [in design] and **misp-galaxy** [partialy implemented].
- Quick win for users would be the current misp-taxonomies as STIX marking.

Integrating MISP taxonomies in STIX marking

```
{
  "definition": {
    "machine-tag": "admiralty-scale:source-reliability=\"b\"",
    "type": "misp-taxonomies"
  },
  "external-reference": {
    "source_name": "misp-taxonomies",
    "external_id": "admiralty-scale",
    "url": "https://raw.githubusercontent.com/MISP/misp-
        taxonomies/master/admiralty-scale/machinetag.json"
  },

  "version": 1,
  "modified": "2016-08-01T00:00:00Z",
  "created": "2016-08-01T00:00:00Z",
  "id": "marking-definition--773875bb-01da-4dfc-b23c-cecc12621
      022",
  "type": "marking-definition"
}
```

MISP objects

- Current objects[1] (based on MISP usage statistics): **domain-ip**, **file**, **ip-port**, **passive-dns**, **vulnerability**, **whois**, **x509**.
- Our objective is to create MISP objects with CybOX 3.0 in mind to enable a smooth import and export.
- to ensure that all CybOX types and vocabularies can be replicated using MISP equivalents.

[1] https://github.com/MISP/misp-objects