

OASIS TC - STIX - Open Points

MISP - Malware Information Sharing Platform & Threat Sharing



CIRCL

Computer Incident
Response Center
Luxembourg



MISP
Threat Sharing

Alexandre Dulaunoy -
Andras Iklody - *TLP:WHITE*

September 12, 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** [partially implemented].
- Quick win for users would be the current misp-taxonomies as STIX marking.

Integrating MISP taxonomies in STIX marking

```
1 {
2   "definition": {
3     "machine-tag": "admiralty-scale:source-reliability=\"b\"",
4     "type": "misp-taxonomies"
5   },
6   "external-reference": {
7     "source_name": "misp-taxonomies",
8     "external_id": "admiralty-scale",
9     "url": "https://raw.githubusercontent.com/MISP/misp-
10      taxonomies/master/admiralty-scale/machinetag.json"
11   },
12   "version": 1,
13   "modified": "2016-08-01T00:00:00Z",
14   "created": "2016-08-01T00:00:00Z",
15   "id": "marking-definition—773875bb-01da-4dfc-b23c-cecc12621
16     022",
17   "type": "marking-definition"
18 }
```

MISP objects

- Current objects¹ (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>