

MISP taxonomies - Flexible Classification for Information Sharing

MISP taxonomies is a solution to use existing taxonomies (or create your own) to **classify your cybersecurity events, indicators and threat intelligence**. This technique is integrated as a default mechanism for tagging in MISP (Threat Intelligence Information Sharing Platform) and to support a distributed classification where organizations can share **common taxonomies in a local or distributed fashion**.

Classifications are distributed as simple JSON files to use with MISP but **can be easily integrated into any other information sharing software**. You can also propose new taxonomies to the community.

namespace	
predicate	
value	

Examples of machine tags and human readable tags :

`admiralty-scale:source-reliability="c"`
admiralty-scale:Source Reliability="Fairly reliable"

`admiralty-scale:information-credibility="3"`
admiralty-scale:Information Credibility="Possibly true"

`nato:classification="NU"`
nato:Classification="NATO UNCLASSIFIED"

`tlp:amber`

Traffic Light Protocol:(TLP:AMBER) Information exclusively given to an organization; sharing limited within the organization to be effectively acted upon.



<https://github.com/MISP/misp-taxonomies/>