Network Working Group
Internet-Draft
Intended status: Informational
Expires: 10 July 2026

A. Dulaunoy
A. Iklody
CIRCL

6 January 2026

MISP taxonomy format
draft-dulaunoy-misp-taxonomy-format-12

Abstract

This document outlines the MISP taxonomy format, a straightforward JSON structure designed to represent machine tags (also known as triple tags) vocabularies. A public directory, referred to as MISP taxonomies, is available and leverages this format. These taxonomies are used to classify cybersecurity events, threats, suspicious activities, and indicators.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 10 July 2026.

Table of Contents

1. Introduction

Sharing threat information has become a fundamental requirement in the Internet security and intelligence community at large. This information can include indicators of compromise, malicious file indicators, financial fraud indicators, or even detailed information about a threat actor. Classification plays a crucial role while sharing such indicators or information, ensuring adequate distribution, understanding, validation, or action regarding the shared information. The MISP taxonomies are a public repository of known vocabularies that can be utilized in threat information sharing.

Machine tags were introduced in 2007 [machine-tags] to allow users to be more precise when tagging their pictures with geolocation. So a machine tag is a tag which uses a special syntax to provide more information to users and machines. Machine tags are also known as triple tags due to their format.

In the MISP taxonomy context, machine tags help analysts to classify their cybersecurity events, indicators or threats. MISP taxonomies can be used for classification, filtering, triggering actions or visualisation depending on their use in threat intelligence platforms such as MISP [MISP-P].

1.1. Conventions and Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

2. Format

A machine tag is composed of a namespace (MUST), a predicate (MUST) and an optional value (OPTIONAL).

Machine tags are represented as a string. Below listed are a set of sample machine tags for different namespaces such as tlp, admiralty-scale and osint.

```
tlp:amber
admiralty-scale:information-credibility="1"
osint:source-type="blog-post"
```

The MISP taxonomy format describes how to define a machine tag namespace in a parseable format. The objective is to provide a simple format to describe machine tag (aka triple tag) vocabularies.

2.1. Overview

The MISP taxonomy format uses the JSON [RFC8259] format. Each namespace is represented as a JSON object with meta information including the following fields: namespace, description, version, type.

namespace defines the overall namespace of the machine tag. The namespace is represented as a string and MUST be present. The description is represented as a string and MUST be present. A version is represented as a unsigned integer MUST be present. A type defines where a specific taxonomy is applicable and a type can be applicable at event, user or org level. The type is represented as an array containing one or more type and SHOULD be present. If a type is not mentioned, by default, the taxonomy is applicable at event level only. An exclusive boolean property MAY be present and defines at namespace level if the predicates are mutually exclusive.

predicates defines all the predicates available in the namespace defined. predicates is represented as an array of JSON objects. predicates MUST be present and MUST at least content one element.

values defines all the values for each predicate in the namespace defined. values SHOULD be present.

2.2. predicates

The predicates array contains one or more JSON objects which lists all the possible predicates. The JSON object contains two fields: value and expanded. value MUST be present. expanded SHOULD be present. value is represented as a string and describes the predicate value. The predicate value MUST not contain spaces or colons. expanded is represented as a string and describes the human-readable version of the predicate value. An exclusive property MAY be present and defines at namespace level if the values are mutually exclusive.

2.3. values

The values array contain one or more JSON objects which lists all the possible values of a predicate. The JSON object contains two fields: predicate and entry. predicate is represented as a string and describes the predicate value. entry is an array with one or more JSON objects. The JSON object contains two fields: value and expanded. value MUST be present. expanded SHOULD be present. value is represented as a string and describes the machine parsable value. expanded is represented as a string and describes the human-readable version of the value.

2.4. uuid

uuid represents the Universally Unique IDentifier (UUID) [RFC4122] of the taxonomy. The uuid MUST be preserved for any updates of the same taxonomy. UUID version 4 or version 5 is RECOMMENDED when assigning it to a new taxonomy. uuid MUST be present at predicate and value level.

uuid is represented as a JSON string. uuid MUST be present.

2.5. optional fields

2.5.1. colour

colour fields MAY be used at predicates or values level to set a specify colour that MAY be used by the implementation. The colour field is described as an RGB colour fill in hexadecimal representation.

Example use of the colour field in the Traffic Light Protocol (TLP):


```
"predicates": [
    {
      "colour": "#FF2B2B",
      "description": "For the eyes and ears of individual recipients only, no further dis
closure. Sources may use TLP:RED when information cannot be effectively acted upon withou
t significant risk for the privacy, reputation, or operations of the organizations involv
ed. Recipients may therefore not share TLP:RED information with anyone else. In the conte
xt of a meeting, for example, TLP:RED information is limited to those present at the meet
ing.",
      "expanded": "(TLP:RED) For the eyes and ears of individual recipients only, no furt
her disclosure.",
      "value": "red",
      "uuid": "845de186-eefa-57a6-be53-a0d36b7c6d2e"
    },
    {
      "colour": "#FFC000",
      "description": "Limited disclosure, recipients can only spread this on a need-to-kn
ow basis within their organization and its clients. Sources may use TLP:AMBER when inform
ation requires support to be effectively acted upon, yet carries risk to privacy, reputat
ion, or operations if shared outside of the organizations involved. Recipients may share
TLP:AMBER information with members of their own organization and its clients, but only on
 a need-to-know basis to protect their organization and its clients and prevent further h
arm. Note that TLP:AMBER+STRICT restricts sharing to the organization only.",
      "expanded": "(TLP:AMBER) Limited disclosure, recipients can only spread this on a n
eed-to-know basis within their organization and its clients.",
      "value": "amber",
      "uuid": "8906fac2-2d9c-55fd-af11-0f35e91a6347"
    }...]
```


2.5.2. description

description fields MAY be used at predicates or values level to add a descriptive and human-readable information about the specific predicate or value. The field is represented as a string. Implementations MAY use the description field to improve more contextual information. The description at the namespace level is a MUST as described above.

2.5.3. numerical_value

numerical_value fields MAY be used at a predicate or value level to add a machine-readable numeric value to a specific predicate or value. The field is represented as a JSON number. Implementations SHOULD use the decimal value provided to support scoring or filtering.

The decimal range for numerical_value SHOULD use a range from 0 up to 100. The range is recommended to support common mathematical properties among taxonomies.

Example use of the numerical_value in the MISP confidence level:

```
{
    "predicate": "confidence-level",
    "entry": [
      {
        "expanded": "Completely confident",
        "value": "completely-confident",
        "numerical_value": 100,
        "uuid": "34ef60ef-bb46-5810-9046-4add93559164"
      },
      {
        "expanded": "Usually confident",
        "value": "usually-confident",
        "numerical_value": 75,
        "uuid": "0df28ca0-7237-58e5-ba64-8f1fb6706571"
      },
      {
        "expanded": "Fairly confident",
        "value": "fairly-confident",
        "numerical_value": 50,
        "uuid": "ae8c1689-f9b5-54f9-a267-e87f545bb7af"
      },
      {
        "expanded": "Rarely confident",
        "value": "rarely-confident",
        "numerical_value": 25,
        "uuid": "173014d7-f408-5eb5-b9f6-ac530c04fc2e"
      },
      {
        "expanded": "Unconfident",
        "value": "unconfident",
        "numerical_value": 0,
        "uuid": "3e9826a6-535a-555b-8ee0-54668d6af6ff"
      },
      {
        "expanded": "Confidence cannot be evaluated",
        "value": "confidence-cannot-be-evaluated",
        "numerical_value": 50,
        "uuid": "021873dd-14cd-5c9b-bc2f-f4a5f7a6c1bc"
      }
    ]
  }
```

3. Directory

The MISP taxonomies directory is publicly available [MISP-T] in a git repository. The repository contains a directory per namespace then a file machinetag.json which contains the taxonomy as described in the format above. In the root of the repository, a MANIFEST.json exists containing a list of all the taxonomies.

The MANIFEST.json file is composed of an JSON object with metadata like version, license, description, url and path. A taxonomies array describes the taxonomy available with the description, name and version field.

3.1. Sample Manifest

```
 {
   "version": "20161009",
   "license": "CC-0",
   "description": "Manifest file of MISP taxonomies available.",
   "url":
     "https://raw.githubusercontent.com/MISP/misp-taxonomies/master/",
   "path": "machinetag.json",
   "taxonomies": [
     {
       "description": "The Admiralty Scale (also called the NATO System)
                       is used to rank the reliability of a source and
                       the credibility of an information.",
       "name": "admiralty-scale",
       "version": 1
     },
     {
       "description": "Open Source Intelligence - Classification.",
       "name": "osint",
       "version": 2
     }]
 }
```

4. Sample Taxonomy in MISP taxonomy format

4.1. Admiralty Scale Taxonomy

```
{
  "namespace": "admiralty-scale",
  "description": "The Admiralty Scale or Ranking (also called the NATO System) is used to
 rank the reliability of a source and the credibility of an information. Reference based
on FM 2-22.3 (FM 34-52) HUMAN INTELLIGENCE COLLECTOR OPERATIONS and NATO documents.",
  "version": 5,
  "predicates": [
    {
      "value": "source-reliability",
```

```
      "expanded": "Source Reliability",
      "exclusive": true,
      "uuid": "f7b68aff-8b01-517c-a272-13dc713d01e5"
    },
    {
      "value": "information-credibility",
      "expanded": "Information Credibility",
      "exclusive": true,
      "uuid": "78ceeb42-699a-5882-882a-5b8cdebb4565"
    }
  ],
  "values": [
    {
      "predicate": "source-reliability",
      "entry": [
        {
          "value": "a",
          "expanded": "Completely reliable",
          "description": "No doubt of authenticity, trustworthiness, or competency; has a
 history of complete reliability",
          "numerical_value": 100,
          "uuid": "bcb65b93-062a-5b9f-8d69-9a1f23d25827"
        },
        {
          "value": "b",
          "expanded": "Usually reliable",
          "description": "Minor doubt about authenticity, trustworthiness, or competency;
 has a history of valid information most of the time",
          "numerical_value": 75,
          "uuid": "61cbed64-0bdf-5467-9b28-e94aa3ee87c5"
        },
        {
          "value": "c",
          "expanded": "Fairly reliable",
          "description": "Doubt of authenticity, trustworthiness, or competency but has p
rovided valid information in the past",
          "numerical_value": 50,
          "uuid": "046949ad-cdc0-53a6-b3ae-762b7befbd77"
        },
        {
          "value": "d",
          "expanded": "Not usually reliable",
          "description": "Significant doubt about authenticity, trustworthiness, or co mp
etency but has provided valid information in the past",
          "numerical_value": 25,
          "uuid": "3125e574-7adc-5e08-b5ca-86d7d1afb2a3"
        },
        {
          "value": "e",
          "expanded": "Unreliable",
          "description": "Lacking in authenticity, trustworthiness, and competency; histo
ry of invalid information",
          "numerical_value": 0,
```

```
          "uuid": "6615786b-22e5-58d1-9bf5-4a790975e461"
        },
        {
          "value": "f",
          "expanded": "Reliability cannot be judged",
          "description": "No basis exists for evaluating the reliability of the source",
          "numerical_value": 50,
          "uuid": "5c877b09-bc69-5b92-bd34-099b4789d6ab"
        },
        {
          "value": "g",
          "expanded": "Deliberatly deceptive",
          "numerical_value": 0,
          "uuid": "47487617-8fe2-518a-9472-178e88a45e6f"
        }
      ]
    },
    {
      "predicate": "information-credibility",
      "entry": [
        {
          "value": "1",
          "expanded": "Confirmed by other sources",
          "description": "Confirmed by other independent sources; logical in itself; Cons
istent with other information on the subject",
          "numerical_value": 100,
          "uuid": "7bc7c468-23c2-5ecc-9e4b-709dc89a7763"
        },
        {
          "value": "2",
          "expanded": "Probably true",
          "description": "Not confirmed; logical in itself; consistent with other informa
tion on the subject",
          "numerical_value": 75,
          "uuid": "802dafc1-6d38-58d0-923b-569655cd0b93"
        },
        {
          "value": "3",
          "expanded": "Possibly true",
          "description": "Not confirmed; reasonably logical in itself; agrees with some o
ther information on the subject",
          "numerical_value": 50,
          "uuid": "c1553166-625b-5d93-9b9a-816f06663e28"
        },
        {
          "value": "4",
          "expanded": "Doubtful",
          "description": "Not confirmed; possible but not logical ; no other information
on the subject",
          "numerical_value": 25,
          "uuid": "ec23824e-c6ef-59d4-9949-643974ad32c1"
        },
```

```
        {
          "value": "5",
          "expanded": "Improbable",
          "description": "Not confirmed; not logical in itself; contradicted by other inf
ormation on the subject",
          "numerical_value": 0,
          "uuid": "5d6bc630-004a-54d9-b285-566361eea3bd"
        },
        {
          "value": "6",
          "expanded": "Truth cannot be judged",
          "description": "No basis exists for evaluating the validity of the information"
,
          "numerical_value": 50,
          "uuid": "ac88352a-20bb-5ba2-89b4-d5f0dcb78658"
        }
      ]
    }
  ],
  "uuid": "97c896f5-df57-517f-be3b-46f7c2dfcaf4"
}
```


4.2. Open Source Intelligence - Classification


```
{
  "predicates": [
    {
      "expanded": "Source Type",
      "value": "source-type",
      "uuid": "53268e72-c3c7-58c0-afa8-ab00a85b46e3"
    },
    {
      "expanded": "Lifetime of the information as Open Source Intelligence",
      "value": "lifetime",
      "uuid": "d14cfc15-c9bc-598b-829d-b757f4cb99cd"
    },
    {
      "expanded": "Certainty of the elements mentioned in this Open Source Intelligence",
      "value": "certainty",
      "uuid": "50358d08-be83-50ea-86c1-c305722c9f13"
    }
  ],
  "version": 11,
  "description": "Open Source Intelligence - Classification (MISP taxonomies)",
  "namespace": "osint",
  "values": [
    {
      "predicate": "source-type",
      "entry": [
        {
```

```
        "value": "blog-post",
        "expanded": "Blog post",
        "uuid": "6110e86a-1752-5b8a-a51b-9899367370d6"
      },
      {
        "value": "microblog-post",
        "expanded": "Microblog post like Twitter",
        "uuid": "a9bb1865-9680-586b-8e97-2ab133668df6"
      },
      {
        "value": "technical-report",
        "expanded": "Technical or analysis report",
        "uuid": "ec22778f-e7d6-5a2a-9a0d-5c402bf22921"
      },
      {
        "value": "presentation",
        "expanded": "Presentation or slidedeck",
        "uuid": "27c02224-598c-5817-8a63-813f659c7aa3"
      },
      {
        "value": "news-report",
        "expanded": "News report",
        "uuid": "61a0a580-f713-5eee-b6a1-bf130d52a92d"
      },
      {
        "value": "pastie-website",
        "expanded": "Pastie-like website",
        "uuid": "b2e6b620-eb8a-502d-91e3-d29f169c3cf9"
      },
      {
        "value": "electronic-forum",
        "expanded": "Electronic forum",
        "uuid": "201c07ce-d9a8-572f-8510-6fc1bb8a379d"
      },
      {
        "value": "mailing-list",
        "expanded": "Mailing-list",
        "uuid": "e4211c17-51a6-5c0b-9bad-8e325e1e8ed3"
      },
      {
        "value": "block-or-filter-list",
        "expanded": "Block or Filter List",
        "uuid": "e5586337-617e-5b78-a9c0-788eeee284d8"
      },
      {
        "value": "source-code-repository",
        "expanded": "Source code repository",
        "uuid": "f447bdf8-b074-5f52-a8e8-21ad064efeaa"
```

```
        },
        {
          "value": "accessible-evidence",
          "expanded": "Infrastructure allowing the gathering of the evidences such as ope
n directories, public web services or left over on public services",
          "uuid": "cd56c2e3-d1fb-5cae-bc63-2fd65f4c59ec"
        },
        {
          "value": "expansion",
          "expanded": "Expansion",
          "uuid": "66cd8968-ffb7-53bb-96ed-02f9e7b79225"
        },
        {
          "value": "automatic-analysis",
          "expanded": "Automatic analysis including dynamic analysis or sandboxes output"
,
          "uuid": "74b1ec26-7ef6-56a4-95fd-2a3eef1ec863"
        },
        {
          "value": "automatic-collection",
          "expanded": "Automatic collection including honeypots, spamtraps or equivalent
technologies",
          "uuid": "371a3857-c667-5a3a-8cdc-b0d661e6b116"
        },
        {
          "value": "manual-analysis",
          "expanded": "Manual analysis or investigation",
          "uuid": "c05f0a98-ae08-5eaf-8155-c95e67fce2d9"
        },
        {
          "value": "manual-collection",
          "expanded": "Manual collection from crawlers, honeypots, spamtraps, gathering t
ools or equivalent technologies",
          "uuid": "e02da304-217e-5745-88cd-6c7a8024af38"
        },
        {
          "value": "unknown",
          "expanded": "Unknown",
          "uuid": "c0ee6b06-cc26-5dfe-ad74-fe5acae742b7"
        },
        {
          "value": "other",
          "expanded": "Other source not specified in this list",
          "uuid": "8054767e-2eb7-53e4-9be6-8950236a192e"
        }
      ]
    },
    {
      "entry": [
        {
          "description": "Information available publicly on long-term",
          "expanded": "Perpetual",
```

```
          "value": "perpetual",
          "uuid": "cafad670-0b27-5818-b86a-757529e56eee"
        },
        {
          "description": "Information available publicly on short-term",
          "expanded": "Ephemeral",
          "value": "ephemeral",
          "uuid": "97adb94b-133d-5f5f-af8f-bf2387bd62ca"
        }
      ],
      "predicate": "lifetime"
    },
    {
      "entry": [
        {
          "description": "Certainty",
          "expanded": "Certainty (probability equals 1 - 100%)",
          "value": "100",
          "numerical_value": 100,
          "uuid": "d97bd9d3-5718-5cb3-890a-6f44c313877c"
        },
        {
          "description": "Almost certain",
          "expanded": "Almost certain (probability equals 0.93 - 93%)",
          "value": "93",
          "numerical_value": 93,
          "uuid": "dfc3f3c5-fb77-58e9-a6c8-5b2ea9414db8"
        },
        {
          "description": "Probable",
          "expanded": "Probable (probability equals 0.75 - 75%)",
          "value": "75",
          "numerical_value": 75,
          "uuid": "a386a237-ed7d-5e8d-9cb3-27cc71dabd0e"
        },
        {
          "description": "Chances about even",
          "expanded": "Chances about even (probability equals 0.50 - 50%)",
          "value": "50",
          "numerical_value": 50,
          "uuid": "f530059e-558f-5919-aa7e-c0dabc163fe4"
        },
        {
          "description": "Probably not",
          "expanded": "Probably not (probability equals 0.30 - 30%)",
          "value": "30",
          "numerical_value": 30,
          "uuid": "66f8af84-735a-5ef2-8dac-b07f3b0df498"
```

```
        },
        {
          "description": "Almost certainly not",
          "expanded": "Almost certainly not (probability equals 0.07 - 7%)",
          "value": "7",
          "numerical_value": 7,
          "uuid": "6e2f8efc-bac3-55ae-b7ee-b9a80a7dce73"
        },
        {
          "description": "Impossibility",
          "expanded": "Impossibility (probability equals 0 - 0%)",
          "value": "0",
          "numerical_value": 0,
          "uuid": "1479effb-9249-5503-8c63-a812d3bcb8b1"
        }
      ],
      "predicate": "certainty"
    }
  ],
  "uuid": "a86e35e6-b0cb-5b30-99df-013b40040cbc"
}
```


4.3. Available taxonomies in the public repository

The public directory of MISP taxonomies [MISP-T] contains more than 150 taxonomies spanning various fields, including:

CERT-XLM: CERT-XLM Security Incident Classification.
DFRLab-dichotomies-of-disinformation: DFRLab Dichotomies of Disinformation.
DML: The Detection Maturity Level (DML) model is a capability maturity model for referencing ones maturity in detecting cyber attacks. It’s designed for organizations who perform intel-driven detection and response and who put an emphasis on having a mature detection program.
GrayZone: Gray Zone of Active defense includes all elements which lay between reactive defense elements and offensive operations. It does fill the gray spot between them. Taxo may be used for active defense planning or modeling.
PAP: The Permissible Actions Protocol - or short: PAP - was designed to indicate how the received information can be used.
access-method: The access method used to remotely access a system.
accessnow: Access Now classification to classify an issue (such as security, human rights, youth rights).
acn: Cyber taxonomy for Italian National Cybersecurity Agency (ACN)
acs-marking: The Access Control Specification (ACS) marking type

defines the object types required to implement automated access control systems based on the relevant policies governing sharing between participants.

- action-taken: Action taken in the case of a security incident (CSIRT perspective).
- admiralty-scale: The Admiralty Scale or Ranking (also called the NATO System) is used to rank the reliability of a source and the credibility of an information. Reference based on FM 2-22.3 (FM 34-52) HUMAN INTELLIGENCE COLLECTOR OPERATIONS and NATO documents.
- adversary: An overview and description of the adversary infrastructure
- ai-bias-terminology: A list of standalone definitions for each type of bias. Aggregate terms that are in common usage or relevance to AI bias. From NIST.SP.1270-draft (2021)
- ai-safety-benchmark: AI safety benchmark v0.5, that has been created by the MLCommons AI Safety Working Group (WG)
- ais-marking: The AIS Marking Schema implementation is maintained by the National Cybersecurity and Communication Integration Center (NCCIC) of the U.S. Department of Homeland Security (DHS)
- analyst-assessment: A series of assessment predicates describing the analyst capabilities to perform analysis. These assessment can be assigned by the analyst him/herself or by another party evaluating the analyst.
- anti-piracy: Taxonomy for anti-piracy
- approved-category-of-action: A pre-approved category of action for indicators being shared with partners (MIMIC).
- artificial-satellites: This taxonomy was designed to describe artificial satellites
- aviation: A taxonomy describing security threats or incidents against the aviation sector.
- binary-class: Custom taxonomy for types of binary file.
- cccs: Internal taxonomy for CCCS.
- ce-uas-classification: European Union (EASA) Drone Classification - C0 to C6.
- circl: CIRCL Taxonomy - Schemes of Classification in Incident Response and Detection.
- cnsd: La presente taxonomia es la primera versi坦n disponible para el Centro Nacional de Seguridad Digital del Per炭.
- coa: Course of action taken within organization to discover, detect, deny, disrupt, degrade, deceive and/or destroy an attack.
- collaborative-intelligence: Collaborative intelligence support language is a common language to support analysts to perform their analysis to get crowdsourced support when using threat intelligence sharing platform like MISP. The objective of this language is to advance collaborative analysis and to share earlier than later.
- common-taxonomy: Common Taxonomy for Law enforcement and CSIRTs
- copine-scale: The COPINE Scale is a rating system created in Ireland

and used in the United Kingdom to categorise the severity of images of child sex abuse. The scale was developed by staff at the COPINE (Combating Paedophile Information Networks in Europe) project. The COPINE Project was founded in 1997, and is based in the Department of Applied Psychology, University College Cork, Ireland.

course-of-action: A Course Of Action analysis considers six potential courses of action for the development of a cyber security capability.

crowdsec: Crowdsec IP address classifications and behaviors taxonomy.

cryptocurrency-threat: Threats targeting cryptocurrency, based on CipherTrace report.

csirt-americas: Taxonom鱈a CSIRT Am辿ricas.

csirt_case_classification: It is critical that the CSIRT provide consistent and timely response to the customer, and that sensitive information is handled appropriately. This document provides the guidelines needed for CSIRT Incident Managers (IM) to classify the case category, criticality level, and sensitivity level for each CSIRT case. This information will be entered into the Incident Tracking System (ITS) when a case is created. Consistent case classification is required for the CSIRT to provide accurate reporting to management on a regular basis. In addition, the classifications will provide CSIRT IM寰洰 with proper case handling procedures and will form the basis of SLA寰洰 between the CSIRT and other Company departments.

cssa: The CSSA agreed sharing taxonomy.

cti: Cyber Threat Intelligence cycle to control workflow state of your process.

current-event: Current events - Schemes of Classification in Incident Response and Detection

cyber-threat-framework: Cyber Threat Framework was developed by the US Government to enable consistent characterization and categorization of cyber threat events, and to identify trends or changes in the activities of cyber adversaries. https://www.dni.gov/index.php/cyber-threat-framework (https://www.dni.gov/index.php/cyber-threat-framework)

cycat: Taxonomy used by CyCAT, the Universal Cybersecurity Resource Catalogue, to categorize the namespaces it supports and uses.

cytomic-orion: Taxonomy to describe desired actions for Cytomic Orion

dark-web: Criminal motivation and content detection the dark web: A categorisation model for law enforcement. ref: Janis Dalins, Campbell Wilson, Mark Carman. Taxonomy updated by MISP Project and extended by the JRC (Joint Research Centre) of the European Commission.

data-classification: Data classification for data potentially at

risk of exfiltration based on table 2.1 of Solving Cyber Risk book.

- dcso-sharing: Taxonomy defined in the DCSO MISP Event Guide. It provides guidance for the creation and consumption of MISP events in a way that minimises the extra effort for the sending party, while enhancing the usefulness for receiving parties.
- ddos: Distributed Denial of Service - or short: DDoS - taxonomy supports the description of Denial of Service attacks and especially the types they belong too.
- de-vs: German (DE) Government classification markings (VS).
- death-possibilities: Taxonomy of Death Possibilities
- deception: Deception is an important component of information operations, valuable for both offense and defense.
- detection-engineering: Taxonomy related to detection engineering techniques
- dga: A taxonomy to describe domain-generation algorithms often called DGA. Ref: A Comprehensive Measurement Study of Domain Generating Malware Daniel Plohmann and others.
- dhs-ciip-sectors: DHS critical sectors as in https://www.dhs.gov/critical-infrastructure-sectors (https://www.dhs.gov/critical-infrastructure-sectors)
- diamond-model: The Diamond Model for Intrusion Analysis establishes the basic atomic element of any intrusion activity, the event, composed of four core features: adversary, infrastructure, capability, and victim.
- diamond-model-for-influence-operations: The diamond model for influence operations analysis is a framework that leads analysts and researchers toward a comprehensive understanding of a malign influence campaign by addressing the socio-political, technical, and psychological aspects of the campaign. The diamond model for influence operations analysis consists of 5 components: 4 corners and a core element. The 4 corners are divided into 2 axes: influencer and audience on the socio-political axis, capabilities and infrastructure on the technical axis. Narrative makes up the core of the diamond.
- dni-ism: A subset of Information Security Marking Metadata ISM as required by Executive Order (EO) 13526. As described by DNI.gov as Data Encoding Specifications for Information Security Marking Metadata in Controlled Vocabulary Enumeration Values for ISM
- domain-abuse: Domain Name Abuse - taxonomy to tag domain names used for cybercrime.
- doping-substances: This taxonomy aims to list doping substances
- drugs: A taxonomy based on the superclass and class of drugs. Based on https://www.drugbank.ca/releases/latest (https://www.drugbank.ca/releases/latest)
- economical-impact: Economic impact refers to a taxonomy used to

describe whether financial effects are positive or negative outcomes related to tagged information. For instance, data exfiltration loss represents a positive outcome for an adversary.

- ecsirt: Incident Classification by the ecsirt.net version mkVI of 31 March 2015 enriched with IntelMQ taxonomy-type mapping.
- enisa: The present threat taxonomy is an initial version that has been developed on the basis of available ENISA material. This material has been used as an ENISA-internal structuring aid for information collection and threat consolidation purposes. It emerged in the time period 2012-2015.
- estimative-language: Estimative language to describe quality and credibility of underlying sources, data, and methodologies based Intelligence Community Directive 203 (ICD 203) and JP 2-0, Joint Intelligence
- eu-marketop-and-publicadmin: Market operators and public administrations that must comply to some notifications requirements under EU NIS directive
- eu-nis-sector-and-subsectors: Sectors, subsectors, and digital services as identified by the NIS Directive
- euci: EU classified information (EUCI) means any information or material designated by a EU security classification, the unauthorised disclosure of which could cause varying degrees of prejudice to the interests of the European Union or of one or more of the Member States.
- europol-event: This taxonomy was designed to describe the type of events
- europol-incident: This taxonomy was designed to describe the type of incidents by class.
- event-assessment: A series of assessment predicates describing the event assessment performed to make judgement(s) under a certain level of uncertainty.
- event-classification: Classification of events as seen in tools such as RT/IR, MISP and other
- exercise: Exercise is a taxonomy to describe if the information is part of one or more cyber or crisis exercise.
- extended-event: Reasons why an event has been extended. This taxonomy must be used on the extended event. The competitive analysis aspect is from Psychology of Intelligence Analysis by Richard J. Heuer, Jr. ref:http://www.foo.be/docs/intelligence/PsychofIntelNew.pdf (http://www.foo.be/docs/intelligence/PsychofIntelNew.pdf)
- failure-mode-in-machine-learning: The purpose of this taxonomy is to

jointly tabulate both the of these failure modes in a single place. Intentional failures wherein the failure is caused by an active adversary attempting to subvert the system to attain her goals 寰either to misclassify the result, infer private training data, or to steal the underlying algorithm. Unintentional failures wherein the failure is because an ML system produces a formally correct but completely unsafe outcome.

false-positive: This taxonomy aims to ballpark the expected amount of false positives.

file-type: List of known file types.

financial: Financial taxonomy to describe financial services, infrastructure and financial scope.

flesch-reading-ease: Flesch Reading Ease is a revised system for determining the comprehension difficulty of written material. The scoring of the flesh score can have a maximum of 121.22 and there is no limit on how low a score can be (negative score are valid).

fpf: The Future of Privacy Forum (FPF) visual guide to practical de-identification (https://fpf.org/2016/04/25/a-visual-guide-to-practical-data-de-identification/) taxonomy is used to evaluate the degree of identifiability of personal data and the types of pseudonymous data, de-identified data and anonymous data. The work of FPF is licensed under a creative commons attribution 4.0 international license.

fr-classif: French gov information classification system

gdpr: Taxonomy related to the REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

gea-nz-activities: Information needed to track or monitor moments, periods or events that occur over time. This type of information is focused on occurrences that must be tracked for business reasons or represent a specific point in the evolution of ‘The Business’.

gea-nz-entities: Information relating to instances of entities or things.

gea-nz-motivators: Information relating to authority or governance.

gsma-attack-category: Taxonomy used by GSMA for their information sharing program with telco describing the attack categories

gsma-fraud: Taxonomy used by GSMA for their information sharing program with telco describing the various aspects of fraud

gsma-network-technology: Taxonomy used by GSMA for their information sharing program with telco describing the types of infrastructure. WiP

honeypot-basic: Updated (CIRCL, Seamus Dowling and EURECOM) from Christian Seifert, Ian Welch, Peter Komisarczuk, ‘Taxonomy of Honeypots’, Technical Report CS-TR-06/12, VICTORIA UNIVERSITY OF WELLINGTON, School of Mathematical and Computing Sciences, June

2006, http://www.mcs.vuw.ac.nz/comp/Publications/archive/CS-TR-06/CS-TR-06-12.pdf (http://www.mcs.vuw.ac.nz/comp/Publications/archive/CS-TR-06/CS-TR-06-12.pdf)

ics: FIRST.ORG CTI SIG - MISP Proposal for ICS/OT Threat Attribution (IOC) Project

iep: Forum of Incident Response and Security Teams (FIRST) Information Exchange Policy (IEP) framework

iep2-policy: Forum of Incident Response and Security Teams (FIRST) Information Exchange Policy (IEP) v2.0 Policy

iep2-reference: Forum of Incident Response and Security Teams (FIRST) Information Exchange Policy (IEP) v2.0 Reference

ifx-vetting: The IFX taxonomy is used to categorise information (MISP events and attributes) to aid in the intelligence vetting process

incident-disposition: How an incident is classified in its process to be resolved. The taxonomy is inspired from NASA Incident Response and Management Handbook. https://www.nasa.gov/pdf/589502main_ITS-HBK-2810.09-02%20%5bNASA%20Information%20Security%20Incident%20Management%5d.pdf#page=9 (https://www.nasa.gov/pdf/589502main_ITS-HBK-2810.09-02%20%5bNASA%20Information%20Security%20Incident%20Management%5d.pdf#page=9)

infoleak: A taxonomy describing information leaks and especially information classified as being potentially leaked. The taxonomy is based on the work by CIRCL on the AIL framework. The taxonomy aim is to be used at large to improve classification of leaked information.

information-origin: Taxonomy for tagging information by its origin: human-generated or AI-generated.

information-security-data-source: Taxonomy to classify the information security data sources.

information-security-indicators: A full set of operational indicators for organizations to use to benchmark their security posture.

interactive-cyber-training-audience: Describes the target of cyber training and education.

interactive-cyber-training-technical-setup: The technical setup consists of environment structure, deployment, and orchestration.

interactive-cyber-training-training-environment: The training environment details the environment around the training, consisting of training type and scenario.

interactive-cyber-training-training-setup: The training setup further describes the training itself with the scoring, roles, the training mode as well as the customization level.

interception-method: The interception method used to intercept traffic.

ioc: An IOC classification to facilitate automation of malicious and

non malicious artifacts

iot: Internet of Things taxonomy, based on IOT UK report https://iotuk.org.uk/wp-content/uploads/2017/01/IOT-Taxonomy-Report.pdf (https://iotuk.org.uk/wp-content/uploads/2017/01/IOT-Taxonomy-Report.pdf)

kill-chain: The Cyber Kill Chain, a phase-based model developed by Lockheed Martin, aims to help categorise and identify the stage of an attack.

maec-delivery-vectors: Vectors used to deliver malware based on MAEC 5.0

maec-malware-behavior: Malware behaviours based on MAEC 5.0

maec-malware-capabilities: Malware Capabilities based on MAEC 5.0

maec-malware-obfuscation-methods: Obfuscation methods used by malware based on MAEC 5.0

malware_classification: Classification based on different categories. Based on https://www.sans.org/reading-room/whitepapers/incident/malware-101-viruses-32848 (https://www.sans.org/reading-room/whitepapers/incident/malware-101-viruses-32848)

meteorstorm: Multiple Environment Threat Evaluation of Resources Space Threats and Operational Risk to Missions (meteorstorm) taxonomy for modeling space, cyber, and multi-domain threats and resilience across five layers: Primary Capability Environment (PCE), Segment (SEG), Service (SVC), Asset (AST), and Analytic (AN).

misinformation-website-label: classification for the identification of type of misinformation among websites. Source:False, Misleading, Clickbait-y, and/or Satirical News Sources by Melissa Zimdars 2019

misp: MISP taxonomy to infer with MISP behavior or operation.

misp-workflow: MISP workflow taxonomy to support result of workflow execution.

monarc-threat: MONARC Threats Taxonomy

ms-caro-malware: Malware Type and Platform classification based on Microsoft’s implementation of the Computer Antivirus Research Organization (CARO) Naming Scheme and Malware Terminology. Based on https://www.microsoft.com/en-us/security/portal/mmpc/shared/malwarenaming.aspx (https://www.microsoft.com/en-us/security/portal/mmpc/shared/malwarenaming.aspx), https://www.microsoft.com/security/portal/mmpc/shared/glossary.aspx (https://www.microsoft.com/security/portal/mmpc/shared/glossary.aspx), https://www.microsoft.com/security/portal/mmpc/shared/objectivecriteria.aspx (https://www.microsoft.com/security/portal/mmpc/shared/objectivecriteria.aspx), and http://www.caro.org/definitions/index.html (http://www.caro.org/definitions/index.html). Malware

families are extracted from Microsoft SIRs since 2008 based on https://www.microsoft.com/security/sir/archive/default.aspx (https://www.microsoft.com/security/sir/archive/default.aspx) and https://www.microsoft.com/en-us/security/portal/threat/threats.aspx (https://www.microsoft.com/en-us/security/portal/threat/threats.aspx). Note that SIRs do NOT include all Microsoft malware families.

ms-caro-malware-full: Malware Type and Platform classification based on Microsoft's implementation of the Computer Antivirus Research Organization (CARO) Naming Scheme and Malware Terminology. Based on https://www.microsoft.com/en-us/security/portal/mmpc/shared/malwarenaming.aspx (https://www.microsoft.com/en-us/security/portal/mmpc/shared/malwarenaming.aspx), https://www.microsoft.com/security/portal/mmpc/shared/glossary.aspx (https://www.microsoft.com/security/portal/mmpc/shared/glossary.aspx), https://www.microsoft.com/security/portal/mmpc/shared/objectivecriteria.aspx (https://www.microsoft.com/security/portal/mmpc/shared/objectivecriteria.aspx), and http://www.caro.org/definitions/index.html (http://www.caro.org/definitions/index.html). Malware families are extracted from Microsoft SIRs since 2008 based on https://www.microsoft.com/security/sir/archive/default.aspx (https://www.microsoft.com/security/sir/archive/default.aspx) and https://www.microsoft.com/en-us/security/portal/threat/threats.aspx (https://www.microsoft.com/en-us/security/portal/threat/threats.aspx). Note that SIRs do NOT include all Microsoft malware families.

mwdb: Malware Database (mwdb) Taxonomy - Tags used across the platform

nato: NATO classification markings.

nato-uas-classification: NATO UAS Classification.

nis: The taxonomy is meant for large scale cybersecurity incidents, as mentioned in the Commission Recommendation of 13 September 2017, also known as the blueprint. It has two core parts: The nature of the incident, i.e. the underlying cause, that triggered the incident, and the impact of the incident, i.e. the impact on services, in which sector(s) of economy and society.

nis2: The taxonomy is meant for large scale cybersecurity incidents, as mentioned in the Commission Recommendation of 13 May 2022, also known as the provisional agreement. It has two core parts: The nature of the incident, i.e. the underlying cause, that triggered the incident, and the impact of the incident, i.e. the impact on services, in which sector(s) of economy and society.

open_threat: Open Threat Taxonomy v1.1 base on James Tarala of SANS

http://www.auditscripts.com/resources/
open_threat_taxonomy_v1.1a.pdf
(http://www.auditscripts.com/resources/
open_threat_taxonomy_v1.1a.pdf), https://files.sans.org/summit/
Threat_Hunting_Incident_Response_Summit_2016/PDFs/Using-Open-
Tools-to-Convert-Threat-Intelligence-into-Practical-Defenses-
James-Tarala-SANS-Institute.pdf (https://files.sans.org/summit/
Threat_Hunting_Incident_Response_Summit_2016/PDFs/Using-Open-
Tools-to-Convert-Threat-Intelligence-into-Practical-Defenses-
James-Tarala-SANS-Institute.pdf), https://www.youtube.com/
watch?v=5rdGOOFC_yE (https://www.youtube.com/watch?v=5rdGOOFC_yE),
and
https://www.rsaconference.com/writable/presentations/file_upload/
str-r04_using-an-open-source-threat-model-for-prioritized-defense-
final.pdf
(https://www.rsaconference.com/writable/presentations/file_upload/
str-r04_using-an-open-source-threat-model-for-prioritized-defense-
final.pdf)

organizational-cyber-harm: A taxonomy to classify organizational cyber harms based on categories like physical, economic, psychological, reputational, and social/societal impacts.

osint: Open Source Intelligence - Classification (MISP taxonomies)

pandemic: Pandemic

passivetotal: Tags from RiskIQ’s PassiveTotal service

pentest: Penetration test (pentest) classification.

pfc: Le Protocole des feux de circulation (PFC) est bas sur le standard Traffic Light Protocol (TLP) conu par le FIRST. Il a pour objectif d’ informer sur les limites autorises pour la diffusion des informations. Il est class selon des codes de couleurs.

phishing: Taxonomy to classify phishing attacks including techniques, collection mechanisms and analysis status.

poison-taxonomy: Non-exhaustive taxonomy of natural poison

political-spectrum: A political spectrum is a system to characterize and classify different political positions in relation to one another.

priority-level: After an incident is scored, it is assigned a priority level. The six levels listed below are aligned with NCCIC, DHS, and the CISS to help provide a common lexicon when discussing incidents. This priority assignment drives NCCIC urgency, pre-approved incident response offerings, reporting requirements, and recommendations for leadership escalation. Generally, incident priority distribution should follow a similar pattern to the graph below. Based on https://www.cisa.gov/news-events/news/cisa-national-cyber-incident-scoring-system-nciss (https://www.cisa.gov/news-events/news/cisa-national-cyber-incident-scoring-system-nciss).

pyoti: PyOTI automated enrichment schemes for point in time

classification of indicators.
ransomware: Ransomware is used to define ransomware types and the elements that compose them.
ransomware-roles: The seven roles seen in most ransomware incidents.
retention: Add a retention time to events to automatically remove the IDS-flag on ip-dst or ip-src attributes. We calculate the time elapsed based on the date of the event. Supported time units are: d(ays), w(eeks), m(onths), y(ears). The numerical_value is just for sorting in the web-interface and is not used for calculations.
rsit: Reference Security Incident Classification Taxonomy
rt_event_status: Status of events used in Request Tracker.
runtime-packer: Runtime or software packer used to combine compressed or encrypted data with the decompression or decryption code. This code can add additional obfuscations mechanisms including polymorphic-packer, virtualization or other obfuscation techniques. This taxonomy lists all the known or official packer used for legitimate use or for packing malicious binaries.
scrippsco2-fgc: Flags describing the sample
scrippsco2-fgi: Flags describing the sample for isotopic data (C14, O18)
scrippsco2-sampling-stations: Sampling stations of the Scripps CO2 Program
sentinel-threattype: Sentinel indicator threat types.
smart-airports-threats: Threat taxonomy in the scope of securing smart airports by ENISA. https://www.enisa.europa.eu/publications/securing-smart-airports (https://www.enisa.europa.eu/publications/securing-smart-airports)
social-engineering-attack-vectors: Attack vectors used in social engineering as described in 'A Taxonomy of Social Engineering Defense Mechanisms' by Dalal Alharthi and others.
srbcert: SRB-CERT Taxonomy - Schemes of Classification in Incident Response and Detection
state-responsibility: A spectrum of state responsibility to more directly tie the goals of attribution to the needs of policymakers.
stealth_malware: Classification based on malware stealth techniques. Described in https://vxheaven.org/lib/pdf/Introducing%20Stealth%20Malware%20Taxonomy.pdf (https://vxheaven.org/lib/pdf/Introducing%20Stealth%20Malware%20Taxonomy.pdf)
stix-ttp: TTPs are representations of the behavior or modus operandi of cyber adversaries.
targeted-threat-index: The Targeted Threat Index is a metric for

assigning an overall threat ranking score to email messages that deliver malware to a victim's computer. The TTI metric was first introduced at SecTor 2013 by Seth Hardy as part of the talk "RATastrophe: Monitoring a Malware Menagerie" along with Katie Kleemola and Greg Wiseman.

thales_group: Thales Group Taxonomy - was designed with the aim of enabling desired sharing and preventing unwanted sharing between Thales Group security communities.

threatmatch: The ThreatMatch Sectors, Incident types, Malware types and Alert types are applicable for any ThreatMatch instances and should be used for all CIISI and TIBER Projects.

threats-to-dns: An overview of some of the known attacks related to DNS as described by Torabi, S., Boukhtouta, A., Assi, C., & Debbabi, M. (2018) in Detecting Internet Abuse by Analyzing Passive DNS Traffic: A Survey of Implemented Systems. IEEE Communications Surveys & Tutorials, 11. doi:10.1109/comst.2018.2849614

tlp: The Traffic Light Protocol (TLP) (v2.0) was created to facilitate greater sharing of potentially sensitive information and more effective collaboration. Information sharing happens from an information source, towards one or more recipients. TLP is a set of four standard labels (a fifth label is included in amber to limit the diffusion) used to indicate the sharing boundaries to be applied by the recipients. Only labels listed in this standard are considered valid by FIRST. This taxonomy includes additional labels for backward compatibility which are no more validated by FIRST SIG.

tor: Taxonomy to describe Tor network infrastructure

trust: The Indicator of Trust provides insight about data on what can be trusted and known as a good actor. Similar to a whitelist but on steroids, reusing features one would use with Indicators of Compromise, but to filter out what is known to be good.

type: Taxonomy to describe different types of intelligence gathering discipline which can be described the origin of intelligence.

unified-kill-chain: The Unified Kill Chain is a refinement to the Kill Chain.

unified-ransomware-kill-chain: The Unified Ransomware Kill Chain, a intelligence driven model developed by Oleg Skulkin, aims to track every single phase of a ransomware attack.

use-case-applicability: The Use Case Applicability categories reflect standard resolution categories, to clearly display alerting rule configuration problems.

veris: Vocabulary for Event Recording and Incident Sharing (VERIS)

vmray: VMRay taxonomies to map VMRay Thread Identifier scores and artifacts.

vocabulaire-des-probabilites-estimatives: Ce vocabulaire attribue des valeurs en pourcentage certains noncs de probabilit

vulnerability: A taxonomy for describing vulnerabilities (software,

hardware, or social) on different scales or with additional available information.

workflow: Workflow support language is a common language to support intelligence analysts to perform their analysis on data and information.

5. JSON Schema

The JSON Schema [JSON-SCHEMA] below defines the structure of the MISP taxonomy document as literally described before. The JSON Schema is used validating a MISP taxonomy. The validation is a _MUST_ if the taxonomy is included in the MISP taxonomies directory.

```
{
  "$schema": "http://json-schema.org/schema#",
  "title": "Validator for misp-taxonomies",
  "id": "https://www.github.com/MISP/misp-taxonomies/schema.json",
  "defs": {
    "non-empty-string": {
      "type": "string",
      "minLength": 1
    },
    "entry": {
      "type": "array",
      "minItems": 1,
      "uniqueItems": true,
      "items": {
        "type": "object",
        "additionalProperties": false,
        "properties": {
          "numerical_value": {
            "type": "number"
          },
          "expanded": {
            "$ref": "#/defs/non-empty-string"
          },
          "description": {
            "$ref": "#/defs/non-empty-string"
          },
          "colour": {
            "$ref": "#/defs/non-empty-string"
          },
          "value": {
            "$ref": "#/defs/non-empty-string"
          },
          "uuid": {
            "$ref": "#/defs/non-empty-string"
          },
```

```
            "required": [
              "value"
            ]
          }
        }
      },
      "values": {
        "type": "array",
        "minItems": 1,
        "uniqueItems": true,
        "items": {
          "type": "object",
          "additionalProperties": false,
          "properties": {
            "entry": {
              "$ref": "#/defs/entry"
            },
            "predicate": {
              "$ref": "#/defs/non-empty-string"
            },
            "uuid": {
              "$ref": "#/defs/non-empty-string"
            }
          },
          "required": [
            "predicate"
          ]
        }
      },
      "predicates": {
        "type": "array",
        "minItems": 1,
        "uniqueItems": true,
        "items": {
          "type": "object",
          "additionalProperties": false,
          "properties": {
            "numerical_value": {
              "type": "number"
            },
            "colour": {
              "$ref": "#/defs/non-empty-string"
            },
            "description": {
              "$ref": "#/defs/non-empty-string"
            },
            "expanded": {
              "$ref": "#/defs/non-empty-string"
```

```
            },
            "value": {
              "$ref": "#/defs/non-empty-string"
            },
            "exclusive": {
              "type": "boolean"
            },
            "uuid": {
              "$ref": "#/defs/non-empty-string"
            },
            "required": [
              "value"
            ]
          }
        }
      }
    },
    "type": "object",
    "additionalProperties": false,
    "properties": {
      "version": {
        "type": "integer"
      },
      "description": {
        "$ref": "#/defs/non-empty-string"
      },
      "expanded": {
        "$ref": "#/defs/non-empty-string"
      },
      "namespace": {
        "$ref": "#/defs/non-empty-string"
      },
      "uuid": {
        "$ref": "#/defs/non-empty-string"
      },
      "exclusive": {
        "type": "boolean"
      },
      "type": {
        "type": "array",
        "minItems": 1,
        "uniqueItems": true,
        "items": {
          "type": "string",
          "enum": [
            "org",
            "user",
            "attribute",
```

```
            "event"
          ]
        }
      },
      "refs": {
        "type": "array",
        "minItems": 1,
        "uniqueItems": true,
        "items": {
          "$ref": "#/defs/non-empty-string"
        }
      },
      "predicates": {
        "$ref": "#/defs/predicates"
      },
      "values": {
        "$ref": "#/defs/values"
      }
    },
    "required": [
      "namespace",
      "description",
      "version",
      "predicates"
    ]
  }
```

6. Acknowledgements

The authors wish to thank all the MISP community who are supporting the creation of open standards in threat intelligence sharing.

7. References

7.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC4122] Leach, P., Mealling, M., and R. Salz, "A Universally Unique IDentifier (UUID) URN Namespace", RFC 4122, DOI 10.17487/RFC4122, July 2005, <https://www.rfc-editor.org/info/rfc4122>.

[RFC8259] Bray, T., Ed., "The JavaScript Object Notation (JSON) Data Interchange Format", STD 90, RFC 8259, DOI 10.17487/RFC8259, December 2017, <https://www.rfc-editor.org/info/rfc8259>.

7.2. Informative References

[JSON-SCHEMA] Wright, A., "JSON Schema: A Media Type for Describing JSON Documents", 2016, <https://tools.ietf.org/html/draft-wright-json-schema>.

[MISP-P] Community, M., "MISP Project - Open Source Threat Intelligence Platform and Open Standards For Threat Information Sharing", <https://github.com/MISP>.

[MISP-T] Community, M., "MISP Taxonomies - shared and common vocabularies of tags", <https://github.com/MISP/misp-taxonomies>.

[machine-tags] Cope, A. S., "Machine tags", 2007, <https://www.flickr.com/groups/51035612836@N01/discuss/72157594497877875/>.

Authors' Addresses

Alexandre Dulaunoy
Computer Incident Response Center Luxembourg
122, rue Adolphe Fischer
L-L-1521 Luxembourg
Luxembourg
Phone: +352 247 88444
Email: alexandre.dulaunoy@circl.lu

Andras Iklody
Computer Incident Response Center Luxembourg
122, rue Adolphe Fischer
L-L-1521 Luxembourg
Luxembourg
Phone: +352 247 88444
Email: andras.iklody@circl.lu