Network Working Group
Internet-Draft
Intended status: Informational
Expires: June 3, 2019

A. Dulaunoy
A. Iklody
CIRCL
November 30, 2018

MISP taxonomy format
draft-dulaunoy-misp-taxonomy-format-06

Abstract

This document describes the MISP taxonomy format which describes a simple JSON format to represent machine tags (also called triple tags) vocabularies. A public directory of common vocabularies called MISP taxonomies is available and relies on the MISP taxonomy format. MISP taxonomies are used to classify cyber security events, threats, suspicious events, or 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 June 3, 2019.

Table of Contents

1. Introduction 2
1.1. Conventions and Terminology 3
2. Format 3
2.1. Overview 3
2.2. predicates 4
2.3. values 4
2.4. optional fields 4
2.4.1. colour 4
2.4.2. description 5
2.4.3. numerical_value 5
3. Directory 6
3.1. Sample Manifest 7
4. Sample Taxonomy in MISP taxonomy format 7
4.1. Admiralty Scale Taxonomy 7
4.2. Open Source Intelligence - Classification 9
4.3. Available taxonomies in the public directory 11
5. JSON Schema 19
6. Acknowledgements 22
7. References 22
7.1. Normative References 22
7.2. Informative References 22
7.3. URIs 23
Authors' Addresses 23

1. Introduction

Sharing threat information became a fundamental requirements on the Internet, security and intelligence community at large. Threat information can include indicators of compromise, malicious file indicators, financial fraud indicators or even detailed information about a threat actor. While sharing such indicators or information, classification plays an important role to ensure adequate distribution, understanding, validation or action of the shared information. MISP taxonomies is a public repository of known vocabularies that can be used 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 [RFC4627] 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 decimal and 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. optional fields

2.4.1. 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": "#CC0033",
          "expanded": "(TLP:RED) Information exclusively and directly
                      given to (a group of) individual recipients.
                      Sharing outside is not legitimate.",
          "value": "red"
        },
        {
          "colour": "#FFC000",
          "expanded": "(TLP:AMBER) Information exclusively given
                      to an organization; sharing limited within
                      the organization to be effectively acted upon.",
          "value": "amber"
        }...]
```

2.4.2. 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.

2.4.3. 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
    },
    {
      "expanded": "Usually confident",
      "value": "usually-confident",
      "numerical_value": 75
    },
    {
      "expanded": "Fairly confident",
      "value": "fairly-confident",
      "numerical_value": 50
    },
    {
      "expanded": "Rarely confident",
      "value": "rarely-confident",
      "numerical_value": 25
    },
    {
      "expanded": "Unconfident",
      "value": "unconfident",
      "numerical_value": 0
    },
    {
      "expanded": "Confidence cannot be evaluated",
      "value": "confidence-cannot-be-evalued"
    }
 ]
 }
```

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 (also called the NATO System)
                    is used to rank the reliability of a source and
                    the credibility of an information.",
    "version": 1,
    "predicates": [
      {
        "value": "source-reliability",
        "expanded": "Source Reliability"
      },
      {
        "value": "information-credibility",
        "expanded": "Information Credibility"
      }
    ],
    "values": [
      {
        "predicate": "source-reliability",
        "entry": [
          {
```

```
            "value": "a",
            "expanded": "Completely reliable"
          },
          {
            "value": "b",
            "expanded": "Usually reliable"
          },
          {
            "value": "c",
            "expanded": "Fairly reliable"
          },
          {
            "value": "d",
            "expanded": "Not usually reliable"
          },
          {
            "value": "e",
            "expanded": "Unreliable"
          },
          {
            "value": "f",
            "expanded": "Reliability cannot be judged"
          }
        ]
      },
      {
        "predicate": "information-credibility",
        "entry": [
          {
            "value": "1",
            "expanded": "Confirmed by other sources"
          },
          {
            "value": "2",
            "expanded": "Probably true"
          },
          {
            "value": "3",
            "expanded": "Possibly true"
          },
          {
            "value": "4",
            "expanded": "Doubtful"
          },
          {
            "value": "5",
            "expanded": "Improbable"
          },
```

```
            {
              "value": "6",
              "expanded": "Truth cannot be judged"
            }
          ]
        }
      ]
    }
```

4.2. Open Source Intelligence - Classification

```
 {
   "values": [
     {
       "entry": [
         {
           "expanded": "Blog post",
           "value": "blog-post"
         },
         {
           "expanded": "Technical or analysis report",
           "value": "technical-report"
         },
         {
           "expanded": "News report",
           "value": "news-report"
         },
         {
           "expanded": "Pastie-like website",
           "value": "pastie-website"
         },
         {
           "expanded": "Electronic forum",
           "value": "electronic-forum"
         },
         {
           "expanded": "Mailing-list",
           "value": "mailing-list"
         },
         {
           "expanded": "Block or Filter List",
           "value": "block-or-filter-list"
         },
         {
           "expanded": "Expansion",
           "value": "expansion"
         }
       ],
```

```
      "predicate": "source-type"
    },
    {
      "predicate": "lifetime",
      "entry": [
        {
          "value": "perpetual",
          "expanded": "Perpetual",
          "description": "Information available publicly on long-term"
        },
        {
          "value": "ephemeral",
          "expanded": "Ephemeral",
          "description": "Information available publicly on short-term"
        }
      ]
    },
    {
      "predicate": "certainty",
      "entry": [
        {
          "numerical_value": 100,
          "value": "100",
          "expanded": "100% Certainty",
          "description": "100% Certainty"
        },
        {
          "numerical_value": 93,
          "value": "93",
          "expanded": "93% Almost certain",
          "description": "93% Almost certain"
        },
        {
          "numerical_value": 75,
          "value": "75",
          "expanded": "75% Probable",
          "description": "75% Probable"
        },
        {
          "numerical_value": 50,
          "value": "50",
          "expanded": "50% Chances about even",
          "description": "50% Chances about even"
        },
        {
          "numerical_value": 30,
          "value": "30",
          "expanded": "30% Probably not",
```

```
          "description": "30% Probably not"
        },
        {
          "numerical_value": 7,
          "value": "7",
          "expanded": "7% Almost certainly not",
          "description": "7% Almost certainly not"
        },
        {
          "numerical_value": 0,
          "value": "0",
          "expanded": "0% Impossibility",
          "description": "0% Impossibility"
        }
      ]
    }
  ],
  "namespace": "osint",
  "description": "Open Source Intelligence - Classification",
  "version": 3,
  "predicates": [
    {
      "value": "source-type",
      "expanded": "Source Type"
    },
    {
      "value": "lifetime",
      "expanded": "Lifetime of the information
                  as Open Source Intelligence"
    },
    {
      "value": "certainty",
      "expanded": "Certainty of the elements mentioned
                  in this Open Source Intelligence"
    }
  ]
}
```

4.3. Available taxonomies in the public directory

The public directory of MISP taxonomies [MISP-T] contains a variety of taxonomy in various fields such as:

CERT-XLM:
   CERT-XLM Security Incident Classification.

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.

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).

action-taken:
Action taken in the case of a security incident (CSIRT perspective).

admiralty-scale:
The Admiralty Scale (also called the NATO System) is used to rank the reliability of a source and the credibility of an information.

adversary:
An overview and description of the adversary infrastructure.

ais-marking:
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.

approved-category-of-action:
A pre-approved category of action for indicators being shared with partners (MIMIC).

binary-class:
Custom taxonomy for types of binary file.

cccs:
Internal taxonomy for CCCS.

circl:
CIRCL Taxonomy is a simple scheme for incident classification and area topic where the incident took place.

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.

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.

csirt_case_classification:
FIRST CSIRT Case Classification.

cssa:
The CSSA agreed sharing taxonomy.

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>

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:
Taxonomy for the handling of protectively marked information in MISP with German (DE) Government classification markings (VS)

dhs-ciip-sectors:
DHS critical sectors as described in <https://www.dhs.gov/critical-infrastructure-sectors>.

diamond-model:
The Diamond Model for Intrusion Analysis, a phase-based model developed by Lockheed Martin, aims to help categorise and identify the stage of an attack.

dni-ism:
ISM (Information Security Marking Metadata) V13 as described by DNI.gov (Director of National Intelligence - US).

domain-abuse:
Taxonomy to tag domain names used for cybercrime.

economical-impact:
Economical impact is a taxonomy to describe the financial impact as positive or negative gain to the tagged information.

ecsirt:
eCSIRT incident classification Appendix C of the eCSIRT EU project including IntelMQ updates.

enisa:
ENISA Threat Taxonomy - A tool for structuring threat information as published in <https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape/etl2015/enisa-threat-taxonomy-a-tool-for-structuring-threat-information>

estimative-language:
Estimative language - including likelihood or probability of event based on the Intelligence Community Directive 203 (ICD 203) (6.2.(a)) 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 and sub sectors 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 as described in CELEX 32013D0488

europol-event:
EUROPOL type of events taxonomy.

europol-incident:
EUROPOL class of incident taxonomy.

event-assessment:
A series of assessment predicates describing the event assessment performed to make judgement(s) under a certain level of uncertainty.

event-classification:

Event Classification.

exercise:
Exercise is a taxonomy to describe if the information is part of one or more cyber or crisis exercise

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

file-type:
List of known file types.

fpf:
The Future of Privacy Forum (FPF) visual guide to practical de-identification [1] 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)

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:
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>

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

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.

infoleak:
A taxonomy describing information leaks and especially information classified as being potentially leaked.

information-security-indicators:
Information security indicators have been standardized by the ETSI Industrial Specification Group (ISG) ISI. These indicators provide the basis to switch from a qualitative to a quantitative culture in IT Security Scope of measurements: External and internal threats (attempt and success), user's deviant behaviours, nonconformities and/or vulnerabilities (software, configuration, behavioural, general security framework). ETSI GS ISI 001-1 (V1.1.2): ISI Indicators

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

kill-chain:
Cyber Kill Chain from Lockheed Martin as described in Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains.

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:
Malware classification based on a SANS whitepaper about malware.

misp:
Internal MISP taxonomy.

monarc-threat:
MONARC threat 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.

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.

nato:
Marking of Classified and Unclassified materials as described by the North Atlantic Treaty Organization, NATO.

nis:
NIS Cybersecurity Incident Taxonomy.

open_threat:
Open Threat Taxonomy v1.1 base on James Tarala of SANS ref. - <http://www.auditscripts.com/resources/open_threat_taxonomy_v1.1a.pdf>

osint:
Open Source Intelligence - Classification (MISP taxonomies).

passivetotal:
Tags for RiskIQ's passivetotal service

pentest:
Penetration test (pentest) classification.

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.us-cert.gov/NCCIC-Cyber-Incident-Scoring-System>.

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 data with the decompression code. The decompression code can add additional obfuscations mechanisms including polymorphic-packer or other obfuscation techniques. This taxonomy lists all the known or official packer used for legitimate use or for packing malicious binaries.

smart-airports-threats:
Threat taxonomy in the scope of securing smart airports by ENISA.

stealth_malware:
Classification based on malware stealth techniques.

stix-ttp:
Representation of the behavior or modus operandi of cyber adversaries (a.k.a TTP) as normalized in STIX

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.

tlp:
The Traffic Light Protocol - or short: TLP - was designed with the objective to create a favorable classification scheme for sharing sensitive information while keeping the control over its distribution at the same time. Extended with TLP:EX:CHR.

tor:
Taxonomy to describe Tor network infrastructure

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

vocabulaire-des-probabilites-estimatives:
Vocabulaire des probabilites estimatives

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": {
    "entry": {
      "type": "array",
      "uniqueItems": true,
      "items": {
        "type": "object",
        "additionalProperties": false,
        "properties": {
          "numerical_value": {
            "type": "number"
          },
          "expanded": {
            "type": "string"
          },
          "description": {
            "type": "string"
          },
          "colour": {
            "type": "string"
          },
          "value": {
            "type": "string"
          },
          "required": [
            "value"
          ]
        }
      }
    },
```

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

```
        }
      }
    },
    "type": "object",
    "additionalProperties": false,
    "properties": {
      "version": {
        "type": "integer"
      },
      "description": {
        "type": "string"
      },
      "expanded": {
        "type": "string"
      },
      "namespace": {
        "type": "string"
      },
      "exclusive": {
        "type": "boolean"
      },
      "type": {
        "type": "array",
        "uniqueItems": true,
        "items": {
          "type": "string",
          "enum": [
            "org",
            "user",
            "attribute",
            "event"
          ]
        }
      },
      "refs": {
        "type": "array",
        "uniqueItems": true,
        "items": {
          "type": "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>.

[RFC4627] Crockford, D., "The application/json Media Type for JavaScript Object Notation (JSON)", RFC 4627, DOI 10.17487/RFC4627, July 2006, <https://www.rfc-editor.org/info/rfc4627>.

7.2. Informative References

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

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

[MISP-P] MISP, "MISP Project - Malware Information Sharing Platform and Threat Sharing", <https://github.com/MISP>.

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

7.3. URIs

[1] https://fpf.org/2016/04/25/a-visual-guide-to-practical-data-de-identification/

Authors' Addresses

Alexandre Dulaunoy
Computer Incident Response Center Luxembourg
16, bd d'Avranches
Luxembourg L-1611
Luxembourg

Phone: +352 247 88444
Email: alexandre.dulaunoy@circl.lu

Andras Iklody
Computer Incident Response Center Luxembourg
16, bd d'Avranches
Luxembourg L-1611
Luxembourg

Phone: +352 247 88444
Email: andras.iklody@circl.lu