Authors: A. Dulaunoy   A. Iklody
         CIRCL   CIRCL

MISP core format

Abstract

This document describes the MISP core format used to exchange
indicators and threat information between MISP (Open Source Threat
Intelligence Sharing Platform formerly known as Malware Information
Sharing Platform) instances. The JSON format includes the overall
structure along with the semantic associated for each respective
key. The format is described to support other implementations which
reuse the format and ensuring an interoperability with existing MISP
[MISP-P] software and other Threat Intelligence Platforms.

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 30 August 2023.

Copyright Notice

Table of Contents

1. Introduction

Sharing threat information became a fundamental requirements in 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. MISP [MISP-P] started as an open source project in late 2011 and the MISP format started to be widely used as an exchange format within the community in the past years. The aim of this document is to describe the specification and the MISP core format.

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

2.1. Overview

The MISP core format is in the JSON [RFC8259] format. In MISP, an event is composed of a single JSON object.

A capitalized key (like Event, Org) represent a data model and a non-capitalised key is just an attribute. This nomenclature can support an implementation to represent the MISP format in another data structure.

2.2. Event

An event is a simple meta structure scheme where attributes and meta-data are embedded to compose a coherent set of indicators. An event can be composed from an incident, a security analysis report or a specific threat actor analysis. The meaning of an event only depends of the information embedded in the event.

2.2.1. Event Attributes

2.2.1.1. uuid

uuid represents the Universally Unique IDentifier (UUID) [RFC4122] of the event. The uuid **MUST** be preserved for any updates or transfer of the same event. UUID version 4 is **RECOMMENDED** when assigning it to a new event.

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

2.2.1.2. id

id represents the human-readable identifier associated to the event for a specific MISP instance. A human-readable identifier **MUST** be represented as an unsigned integer.

id is represented as a JSON string. id **SHALL** be present.

2.2.1.3. published

published represents the event publication state. If the event was published, the published value **MUST** be true. In any other publication state, the published value **MUST** be false.

published is represented as a JSON boolean. published **MUST** be present.

2.2.1.4. info

info represents the information field of the event. info is a free-text value to provide a human-readable summary of the event. info **SHOULD** NOT be bigger than 256 characters and **SHOULD** NOT include new-lines.

info is represented as a JSON string. info **MUST** be present.

2.2.1.5. threat_level_id

threat_level_id represents the threat level.

4: Undefined
3: Low
2: Medium
1: High

If a higher granularity is required, a MISP taxonomy applied as a Tag **SHOULD** be preferred.

threat_level_id is represented as a JSON string. threat_level_id **SHALL** be present.

2.2.1.6. analysis

analysis represents the analysis level.

0: Initial
1: Ongoing
2: Complete

If a higher granularity is required, a MISP taxonomy applied as a
Tag **SHOULD** be preferred.

analysis is represented as a JSON string. analysis **SHALL** be present.

2.2.1.7. date

date represents a reference date to the event in ISO 8601 format
(date only: YYYY-MM-DD). This date corresponds to the date the event
occurred, which may be in the past.

date is represented as a JSON string. date **MUST** be present.

2.2.1.8. timestamp

timestamp represents a reference time when the event, or one of the
attributes within the event was created, or last updated/edited on
the instance. timestamp is expressed in seconds (decimal) since 1st
of January 1970 (Unix timestamp). The time zone **MUST** be UTC.

timestamp is represented as a JSON string. timestamp **MUST** be
present.

2.2.1.9. publish_timestamp

publish_timestamp represents a reference time when the event was
published on the instance. published_timestamp is expressed in
seconds (decimal) since 1st of January 1970 (Unix timestamp). At
each publication of an event, publish_timestamp **MUST** be updated. The
time zone **MUST** be UTC. If the published_timestamp is present and the
published flag is set to false, the publish_timestamp represents the
previous publication timestamp. If the event was never published,
the published_timestamp **MUST** be set to 0.

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

2.2.1.10. org_id

org_id represents a human-readable identifier referencing an Org
object of the organisation which generated the event. A human-
readable identifier **MUST** be represented as an unsigned integer.

The org_id **MUST** be updated when the event is generated by a new
instance.

org_id is represented as a JSON string. org_id **MUST** be present.

2.2.1.11. orgc_id

orgc_id represents a human-readable identifier referencing an Orgc object of the organisation which created the event.

The orgc_id and Org object **MUST** be preserved for any updates or transfer of the same event.

orgc_id is represented as a JSON string. orgc_id **MUST** be present.

2.2.1.12. attribute_count

attribute_count represents the number of attributes in the event. attribute_count is expressed in decimal.

attribute_count is represented as a JSON string. attribute_count **SHALL** be present.

2.2.1.13. distribution

distribution represents the basic distribution rules of the event. The system must adhere to the distribution setting for access control and for dissemination of the event.

distribution is represented by a JSON string. distribution **MUST** be present and be one of the following options:

0 Your Organisation Only
1 This Community Only
2 Connected Communities
3 All Communities
4 Sharing Group

2.2.1.14. sharing_group_id

sharing_group_id represents a human-readable identifier referencing a Sharing Group object that defines the distribution of the event, if distribution level "4" is set. A human-readable identifier **MUST** be represented as an unsigned integer.

sharing_group_id is represented by a JSON string and **SHOULD** be present. If a distribution level other than "4" is chosen the sharing_group_id **MUST** be set to "0".

2.2.1.15. extends_uuid

extends_uuid represents which event is extended by this event. The extends_uuid is described as a Universally Unique IDentifier (UUID) [RFC4122] with the UUID of the extended event.

extends_uuid is represented as a JSON string. extends_uuid **SHOULD** be present.

2.2.2. Event Objects

2.2.2.1. Org

An Org object is composed of an uuid, name and id.

The uuid represents the Universally Unique IDentifier (UUID) [RFC4122] of the organisation. The organisation UUID is globally assigned to an organisation and **SHALL** be kept overtime.

The name is a readable description of the organisation and **SHOULD** be present. The id is a human-readable identifier generated by the instance and used as reference in the event. A human-readable identifier **MUST** be represented as an unsigned integer.

uuid, name and id are represented as a JSON string. uuid, name and id **MUST** be present.

2.2.2.1.1. Sample Org Object

```
"Org": {
     "id": "2",
     "name": "CIRCL",
     "uuid": "55f6ea5e-2c60-40e5-964f-47a8950d210f"
    }
```

2.2.2.2. Orgc

An Orgc object is composed of an uuid, name and id.

The uuid **MUST** be preserved for any updates or transfer of the same event. UUID version 4 is **RECOMMENDED** when assigning it to a new event. The organisation UUID is globally assigned to an organisation and **SHALL** be kept overtime.

The name is a readable description of the organisation and **SHOULD** be present. The id is a human-readable identifier generated by the instance and used as reference in the event. A human-readable identifier **MUST** be represented as an unsigned integer.

uuid, name and id are represented as a JSON string. uuid, name and id **MUST** be present.

2.3. Attribute

Attributes are used to describe the indicators and contextual data of an event. The main information contained in an attribute is made

up of a category-type-value triplet, where the category and type
give meaning and context to the value. Through the various category-
type combinations a wide range of information can be conveyed.

A MISP document **MUST** at least includes category-type-value triplet
described in section "Attribute Attributes".

2.3.1. Sample Attribute Object

```
"Attribute": {
            "id": "346056",
            "type": "comment",
            "category": "Other",
            "to_ids": false,
            "uuid": "57f4f6d9-cd20-458b-84fd-109ec0a83869",
            "event_id": "3357",
            "distribution": "5",
            "timestamp": "1475679332",
            "comment": "",
            "sharing_group_id": "0",
            "deleted": false,
            "value": "Hello world",
            "SharingGroup": [],
            "ShadowAttribute": [],
            "RelatedAttribute": [],
            "first_seen": "2019-06-02T22:14:28.711954+00:00",
            "last_seen": null
          }
```

2.3.2. Attribute Attributes

2.3.2.1. uuid

uuid represents the Universally Unique IDentifier (UUID) [RFC4122]
of the event. The uuid **MUST** be preserved for any updates or transfer
of the same event. UUID version 4 is **RECOMMENDED** when assigning it
to a new event.

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

2.3.2.2. id

id represents the human-readable identifier associated to the event
for a specific MISP instance. A human-readable identifier **MUST** be
represented as an unsigned integer.

id is represented as a JSON string. id **SHALL** be present.

2.3.2.3. type

type represents the means through which an attribute tries to describe the intent of the attribute creator, using a list of pre-defined attribute types.

type is represented as a JSON string. type **MUST** be present and it **MUST** be a valid selection for the chosen category. The list of valid category-type combinations is as follows:

Antivirus detection link, comment, text, hex, attachment, other, anonymised

Artifacts dropped md5, sha1, sha224, sha256, sha384, sha512, sha512/224, sha512/256, sha3-224, sha3-256, sha3-384, sha3-512, ssdeep, imphash, telfhash, impfuzzy, authentihash, vhash, cdhash, filename, filename|md5, filename|sha1, filename|sha224, filename| sha256, filename|sha384, filename|sha512, filename|sha512/224, filename|sha512/256, filename|sha3-224, filename|sha3-256, filename|sha3-384, filename|sha3-512, filename|authentihash, filename|vhash, filename|ssdeep, filename|tlsh, filename|imphash, filename|impfuzzy, filename|pehash, regkey, regkey|value, pattern-in-file, pattern-in-memory, filename-pattern, pdb, stix2-pattern, yara, sigma, attachment, malware-sample, named pipe, mutex, process-state, windows-scheduled-task, windows-service-name, windows-service-displayname, comment, text, hex, x509-fingerprint-sha1, x509-fingerprint-md5, x509-fingerprint-sha256, other, cookie, gene, kusto-query, mime-type, anonymised, pgp-public-key, pgp-private-key

Attribution threat-actor, campaign-name, campaign-id, whois-registrant-phone, whois-registrant-email, whois-registrant-name, whois-registrant-org, whois-registrar, whois-creation-date, comment, text, x509-fingerprint-sha1, x509-fingerprint-md5, x509-fingerprint-sha256, other, dns-soa-email, anonymised, email

External analysis md5, sha1, sha256, sha3-224, sha3-256, sha3-384, sha3-512, filename, filename|md5, filename|sha1, filename|sha256, filename|sha3-224, filename|sha3-256, filename|sha3-384, filename|sha3-512, ip-src, ip-dst, ip-dst|port, ip-src|port, mac-address, mac-eui-64, hostname, domain, domain|ip, url, user-agent, regkey, regkey|value, AS, snort, bro, zeek, pattern-in-file, pattern-in-traffic, pattern-in-memory, filename-pattern, vulnerability, cpe, weakness, attachment, malware-sample, link, comment, text, x509-fingerprint-sha1, x509-fingerprint-md5, x509-fingerprint-sha256, ja3-fingerprint-md5, jarm-fingerprint, hassh-

md5, hasshserver-md5, github-repository, other, cortex, anonymised, community-id

Financial fraud btc, dash, xmr, iban, bic, bank-account-nr, aba-rtn, bin, cc-number, prtn, phone-number, comment, text, other, hex, anonymised

Internal reference text, link, comment, other, hex, anonymised, git-commit-id

Network activity ip-src, ip-dst, ip-dst|port, ip-src|port, port, hostname, domain, domain|ip, mac-address, mac-eui-64, email, email-dst, email-src, eppn, url, uri, user-agent, http-method, AS, snort, pattern-in-file, filename-pattern, stix2-pattern, pattern-in-traffic, attachment, comment, text, x509-fingerprint-md5, x509-fingerprint-sha1, x509-fingerprint-sha256, ja3-fingerprint-md5, jarm-fingerprint, hassh-md5, hasshserver-md5, other, hex, cookie, hostname|port, bro, zeek, anonymised, community-id, email-subject, favicon-mmh3, dkim, dkim-signature, ssh-fingerprint

Other comment, text, other, size-in-bytes, counter, datetime, cpe, port, float, hex, phone-number, boolean, anonymised, pgp-public-key, pgp-private-key

Payload delivery md5, sha1, sha224, sha256, sha384, sha512, sha512/224, sha512/256, sha3-224, sha3-256, sha3-384, sha3-512, ssdeep, imphash, telfhash, impfuzzy, authentihash, vhash, pehash, tlsh, cdhash, filename, filename|md5, filename|sha1, filename|sha224, filename|sha256, filename|sha384, filename|sha512, filename|sha512/224, filename|sha512/256, filename|sha3-224, filename|sha3-256, filename|sha3-384, filename|sha3-512, filename|authentihash, filename|vhash, filename|ssdeep, filename|tlsh, filename|imphash, filename|impfuzzy, filename|pehash, mac-address, mac-eui-64, ip-src, ip-dst, ip-dst|port, ip-src|port, hostname, domain, email, email-src, email-dst, email-subject, email-attachment, email-body, url, user-agent, AS, pattern-in-file, pattern-in-traffic, filename-pattern, stix2-pattern, yara, sigma, mime-type, attachment, malware-sample, link, malware-type, comment, text, hex, vulnerability, cpe, weakness, x509-fingerprint-sha1, x509-fingerprint-md5, x509-fingerprint-sha256, ja3-fingerprint-md5, jarm-fingerprint, hassh-md5, hasshserver-md5, other, hostname|port, email-dst-display-name, email-src-display-name, email-header, email-reply-to, email-x-mailer, email-mime-boundary, email-thread-index, email-message-id, azure-application-id, mobile-application-id, chrome-extension-id, whois-registrant-email, anonymised

Payload installation md5, sha1, sha224, sha256, sha384, sha512, sha512/224, sha512/256, sha3-224, sha3-256, sha3-384, sha3-512, ssdeep, imphash, telfhash, impfuzzy, authentihash, vhash, pehash, tlsh, cdhash, filename, filename|md5, filename|sha1, filename|sha224, filename|sha256, filename|sha384, filename|sha512, filename|sha512/224, filename|sha512/256, filename|sha3-224, filename|sha3-256, filename|sha3-384, filename|sha3-512,

filename|authentihash, filename|vhash, filename|ssdeep, filename|
tlsh, filename|imphash, filename|impfuzzy, filename|pehash,
pattern-in-file, pattern-in-traffic, pattern-in-memory, filename-
pattern, stix2-pattern, yara, sigma, vulnerability, cpe,
weakness, attachment, malware-sample, malware-type, comment,
text, hex, x509-fingerprint-sha1, x509-fingerprint-md5, x509-
fingerprint-sha256, azure-application-id, azure-application-id,
mobile-application-id, chrome-extension-id, other, mime-type,
anonymised

Payload type comment, text, other, anonymised

Persistence mechanism filename, regkey, regkey|value, comment,
text, other, hex, anonymised

Person first-name, middle-name, last-name, full-name, date-of-
birth, place-of-birth, gender, passport-number, passport-country,
passport-expiration, redress-number, nationality, visa-number,
issue-date-of-the-visa, primary-residence, country-of-residence,
special-service-request, frequent-flyer-number, travel-details,
payment-details, place-port-of-original-embarkation, place-port-
of-clearance, place-port-of-onward-foreign-destination,
passenger-name-record-locator-number, comment, text, other,
phone-number, identity-card-number, anonymised, email, pgp-
public-key, pgp-private-key

Social network github-username, github-repository, github-
organisation, jabber-id, twitter-id, email, email-src, email-dst,
eppn, comment, text, other, whois-registrant-email, anonymised,
pgp-public-key, pgp-private-key

Support Tool link, text, attachment, comment, other, hex,
anonymised

Targeting data target-user, target-email, target-machine, target-
org, target-location, target-external, comment, anonymised

Attributes are based on the usage within their different
communities. Attributes can be extended on a regular basis and this
reference document is updated accordingly.

2.3.2.4. category

category represents the intent of what the attribute is describing
as selected by the attribute creator, using a list of pre-defined
attribute categories.

category is represented as a JSON string. category **MUST** be present
and it **MUST** be a valid selection for the chosen type. The list of
valid category-type combinations is mentioned above.

2.3.2.5. to_ids

to_ids represents whether the attribute is meant to be actionable.
Actionable defined attributes that can be used in automated

processes as a pattern for detection in Local or Network Intrusion
Detection System, log analysis tools or even filtering mechanisms.

to_ids is represented as a JSON boolean. to_ids **MUST** be present.

2.3.2.6. event_id

event_id represents a human-readable identifier referencing the
Event object that the attribute belongs to. A human-readable
identifier **MUST** be represented as an unsigned integer.

The event_id **SHOULD** be updated when the event is imported to reflect
the newly created event's id on the instance.

event_id is represented as a JSON string. event_id **MUST** be present.

2.3.2.7. distribution

distribution represents the basic distribution rules of the
attribute. The system must adhere to the distribution setting for
access control and for dissemination of the attribute.

distribution is represented by a JSON string. distribution **MUST** be
present and be one of the following options:

0 Your Organisation Only
1 This Community Only
2 Connected Communities
3 All Communities
4 Sharing Group
5 Inherit Event

2.3.2.8. timestamp

timestamp represents a reference time when the attribute was created
or last modified. timestamp is expressed in seconds (decimal) since
1st of January 1970 (Unix timestamp). The time zone **MUST** be UTC.

timestamp is represented as a JSON string. timestamp **MUST** be
present.

2.3.2.9. comment

comment is a contextual comment field.

comment is represented by a JSON string. comment **MAY** be present.

2.3.2.10. sharing_group_id

sharing_group_id represents a human-readable identifier referencing a Sharing Group object that defines the distribution of the attribute, if distribution level "4" is set. A human-readable identifier **MUST** be represented as an unsigned integer.

sharing_group_id is represented by a JSON string and **SHOULD** be present. If a distribution level other than "4" is chosen the sharing_group_id **MUST** be set to "0".

2.3.2.11. deleted

deleted represents a setting that allows attributes to be revoked. Revoked attributes are not actionable and exist merely to inform other instances of a revocation.

deleted is represented by a JSON boolean. deleted **MUST** be present.

2.3.2.12. data

data contains the base64 encoded contents of an attachment or a malware sample. For malware samples, the sample **MUST** be encrypted using a password protected zip archive, with the password being "infected".

data is represented by a JSON string in base64 encoding. data **MUST** be set for attributes of type malware-sample and attachment.

2.3.2.13. RelatedAttribute

RelatedAttribute is an array of attributes correlating with the current attribute. Each element in the array represents an JSON object which contains an Attribute dictionnary with the external attributes who correlate. Each Attribute **MUST** include the id, org_id, info and a value. Only the correlations found on the local instance are shown in RelatedAttribute.

RelatedAttribute **MAY** be present.

2.3.2.14. ShadowAttribute

ShadowAttribute is an array of shadow attributes that serve as proposals by third parties to alter the containing attribute. The structure of a ShadowAttribute is similar to that of an Attribute, which can be accepted or discarded by the event creator. If accepted, the original attribute containing the shadow attribute is removed and the shadow attribute is converted into an attribute.

Each shadow attribute that references an attribute **MUST** contain the containing attribute's ID in the old_id field and the event's ID in the event_id field.

2.3.2.15. value

value represents the payload of an attribute. The format of the value is dependent on the type of the attribute.

value is represented by a JSON string. value **MUST** be present.

2.3.2.16. first_seen

first_seen represents a reference time when the attribute was first seen. first_seen is expressed as an ISO 8601 datetime up to the micro-second with time zone support.

first_seen is represented as a JSON string. first_seen **MAY** be present.

2.3.2.17. last_seen

last_seen represents a reference time when the attribute was last seen. last_seen is expressed as an ISO 8601 datetime up to the micro-second with time zone support.

last_seen is represented as a JSON string. last_seen **MAY** be present.

2.4. ShadowAttribute

ShadowAttributes are 3rd party created attributes that either propose to add new information to an event or modify existing information. They are not meant to be actionable until the event creator accepts them - at which point they will be converted into attributes or modify an existing attribute.

They are similar in structure to Attributes but additionally carry a reference to the creator of the ShadowAttribute as well as a revocation flag.

2.4.1. Sample Attribute Object

```
"ShadowAttribute":  {
                    "id": "8",
                    "type": "ip-src",
                    "category": "Network activity",
                    "to_ids": false,
                    "uuid": "57d475f1-da78-4569-89de-1458c0a83869",
                    "event_uuid": "57d475e6-41c4-41ca-b450-145ec0a838
                    "event_id": "9",
                    "old_id": "319",
                    "comment": "",
                    "org_id": "1",
                    "proposal_to_delete": false,
                    "value": "5.5.5.5",
                    "deleted": false,
                    "Org": {
                        "id": "1",
                        "name": "MISP",
                        "uuid": "568cce5a-0c80-412b-8fdf-1ffac0a83869
                    },
                    "first_seen": "2019-06-02T22:14:28.711954+00:00",
                    "last_seen": null
                }
```

2.4.2. ShadowAttribute Attributes

2.4.2.1. uuid

uuid represents the Universally Unique IDentifier (UUID) [RFC4122]
of the event. The uuid **MUST** be preserved for any updates or transfer
of the same event. UUID version 4 is **RECOMMENDED** when assigning it
to a new event.

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

2.4.2.2. id

id represents the human-readable identifier associated to the event
for a specific MISP instance. human-readable identifier **MUST** be
represented as an unsigned integer. id is represented as a JSON
string. id **SHALL** be present.

2.4.2.3. type

type represents the means through which an attribute tries to
describe the intent of the attribute creator, using a list of pre-
defined attribute types.

type is represented as a JSON string. type **MUST** be present and it
MUST be a valid selection for the chosen category. The list of valid
category-type combinations is as follows:

Antivirus detection link, comment, text, hex, attachment, other,
  anonymised
Artifacts dropped md5, sha1, sha224, sha256, sha384, sha512,
  sha512/224, sha512/256, sha3-224, sha3-256, sha3-384, sha3-512,
  ssdeep, imphash, telfhash, impfuzzy, authentihash, vhash, cdhash,
  filename, filename|md5, filename|sha1, filename|sha224, filename|
  sha256, filename|sha384, filename|sha512, filename|sha512/224,
  filename|sha512/256, filename|sha3-224, filename|sha3-256,
  filename|sha3-384, filename|sha3-512, filename|authentihash,
  filename|vhash, filename|ssdeep, filename|tlsh, filename|imphash,
  filename|impfuzzy, filename|pehash, regkey, regkey|value,
  pattern-in-file, pattern-in-memory, filename-pattern, pdb, stix2-
  pattern, yara, sigma, attachment, malware-sample, named pipe,
  mutex, process-state, windows-scheduled-task, windows-service-
  name, windows-service-displayname, comment, text, hex, x509-
  fingerprint-sha1, x509-fingerprint-md5, x509-fingerprint-sha256,
  other, cookie, gene, kusto-query, mime-type, anonymised, pgp-
  public-key, pgp-private-key
Attribution threat-actor, campaign-name, campaign-id, whois-
  registrant-phone, whois-registrant-email, whois-registrant-name,
  whois-registrant-org, whois-registrar, whois-creation-date,
  comment, text, x509-fingerprint-sha1, x509-fingerprint-md5, x509-
  fingerprint-sha256, other, dns-soa-email, anonymised, email
External analysis md5, sha1, sha256, sha3-224, sha3-256, sha3-384,
  sha3-512, filename, filename|md5, filename|sha1, filename|sha256,
  filename|sha3-224, filename|sha3-256, filename|sha3-384,
  filename|sha3-512, ip-src, ip-dst, ip-dst|port, ip-src|port, mac-
  address, mac-eui-64, hostname, domain, domain|ip, url, user-
  agent, regkey, regkey|value, AS, snort, bro, zeek, pattern-in-
  file, pattern-in-traffic, pattern-in-memory, filename-pattern,
  vulnerability, cpe, weakness, attachment, malware-sample, link,
  comment, text, x509-fingerprint-sha1, x509-fingerprint-md5, x509-
  fingerprint-sha256, ja3-fingerprint-md5, jarm-fingerprint, hassh-
  md5, hasshserver-md5, github-repository, other, cortex,
  anonymised, community-id
Financial fraud btc, dash, xmr, iban, bic, bank-account-nr, aba-
  rtn, bin, cc-number, prtn, phone-number, comment, text, other,
  hex, anonymised
Internal reference text, link, comment, other, hex, anonymised,
  git-commit-id
Network activity ip-src, ip-dst, ip-dst|port, ip-src|port, port,
  hostname, domain, domain|ip, mac-address, mac-eui-64, email,
  email-dst, email-src, eppn, url, uri, user-agent, http-method,
  AS, snort, pattern-in-file, filename-pattern, stix2-pattern,
  pattern-in-traffic, attachment, comment, text, x509-fingerprint-

md5, x509-fingerprint-sha1, x509-fingerprint-sha256, ja3-fingerprint-md5, jarm-fingerprint, hassh-md5, hasshserver-md5, other, hex, cookie, hostname|port, bro, zeek, anonymised, community-id, email-subject, favicon-mmh3, dkim, dkim-signature, ssh-fingerprint

Other comment, text, other, size-in-bytes, counter, datetime, cpe, port, float, hex, phone-number, boolean, anonymised, pgp-public-key, pgp-private-key

Payload delivery md5, sha1, sha224, sha256, sha384, sha512, sha512/224, sha512/256, sha3-224, sha3-256, sha3-384, sha3-512, ssdeep, imphash, telfhash, impfuzzy, authentihash, vhash, pehash, tlsh, cdhash, filename, filename|md5, filename|sha1, filename|sha224, filename|sha256, filename|sha384, filename|sha512, filename|sha512/224, filename|sha512/256, filename|sha3-224, filename|sha3-256, filename|sha3-384, filename|sha3-512, filename|authentihash, filename|vhash, filename|ssdeep, filename|tlsh, filename|imphash, filename|impfuzzy, filename|pehash, mac-address, mac-eui-64, ip-src, ip-dst, ip-dst|port, ip-src|port, hostname, domain, email, email-src, email-dst, email-subject, email-attachment, email-body, url, user-agent, AS, pattern-in-file, pattern-in-traffic, filename-pattern, stix2-pattern, yara, sigma, mime-type, attachment, malware-sample, link, malware-type, comment, text, hex, vulnerability, cpe, weakness, x509-fingerprint-sha1, x509-fingerprint-md5, x509-fingerprint-sha256, ja3-fingerprint-md5, jarm-fingerprint, hassh-md5, hasshserver-md5, other, hostname|port, email-dst-display-name, email-src-display-name, email-header, email-reply-to, email-x-mailer, email-mime-boundary, email-thread-index, email-message-id, azure-application-id, mobile-application-id, chrome-extension-id, whois-registrant-email, anonymised

Payload installation md5, sha1, sha224, sha256, sha384, sha512, sha512/224, sha512/256, sha3-224, sha3-256, sha3-384, sha3-512, ssdeep, imphash, telfhash, impfuzzy, authentihash, vhash, pehash, tlsh, cdhash, filename, filename|md5, filename|sha1, filename|sha224, filename|sha256, filename|sha384, filename|sha512, filename|sha512/224, filename|sha512/256, filename|sha3-224, filename|sha3-256, filename|sha3-384, filename|sha3-512, filename|authentihash, filename|vhash, filename|ssdeep, filename|tlsh, filename|imphash, filename|impfuzzy, filename|pehash, pattern-in-file, pattern-in-traffic, pattern-in-memory, filename-pattern, stix2-pattern, yara, sigma, vulnerability, cpe, weakness, attachment, malware-sample, malware-type, comment, text, hex, x509-fingerprint-sha1, x509-fingerprint-md5, x509-fingerprint-sha256, azure-application-id, azure-application-id, mobile-application-id, chrome-extension-id, other, mime-type, anonymised

Payload type comment, text, other, anonymised

Persistence mechanism filename, regkey, regkey|value, comment, text, other, hex, anonymised

Person first-name, middle-name, last-name, full-name, date-of-
birth, place-of-birth, gender, passport-number, passport-country,
passport-expiration, redress-number, nationality, visa-number,
issue-date-of-the-visa, primary-residence, country-of-residence,
special-service-request, frequent-flyer-number, travel-details,
payment-details, place-port-of-original-embarkation, place-port-
of-clearance, place-port-of-onward-foreign-destination,
passenger-name-record-locator-number, comment, text, other,
phone-number, identity-card-number, anonymised, email, pgp-
public-key, pgp-private-key

Social network github-username, github-repository, github-
organisation, jabber-id, twitter-id, email, email-src, email-dst,
eppn, comment, text, other, whois-registrant-email, anonymised,
pgp-public-key, pgp-private-key

Support Tool link, text, attachment, comment, other, hex,
anonymised

Targeting data target-user, target-email, target-machine, target-
org, target-location, target-external, comment, anonymised

Attributes are based on the usage within their different
communities. Attributes can be extended on a regular basis and this
reference document is updated accordingly.

2.4.2.4. category

category represents the intent of what the attribute is describing
as selected by the attribute creator, using a list of pre-defined
attribute categories.

category is represented as a JSON string. category **MUST** be present
and it **MUST** be a valid selection for the chosen type. The list of
valid category-type combinations is mentioned above.

2.4.2.5. to_ids

to_ids represents whether the Attribute to be created if the
ShadowAttribute is accepted is meant to be actionable. Actionable
defined attributes that can be used in automated processes as a
pattern for detection in Local or Network Intrusion Detection
System, log analysis tools or even filtering mechanisms.

to_ids is represented as a JSON boolean. to_ids **MUST** be present.

2.4.2.6. event_id

event_id represents a human-readable identifier referencing the
Event object that the ShadowAttribute belongs to.

The event_id **SHOULD** be updated when the event is imported to reflect
the newly created event's id on the instance.

event_id is represented as a JSON string. event_id **MUST** be present.

2.4.2.7. old_id

old_id represents a human-readable identifier referencing the Attribute object that the ShadowAttribute belongs to. A ShadowAttribute can this way target an existing Attribute, implying that it is a proposal to modify an existing Attribute, or alternatively it can be a proposal to create a new Attribute for the containing Event.

The old_id **SHOULD** be updated when the event is imported to reflect the newly created Attribute's id on the instance. Alternatively, if the ShadowAttribute proposes the creation of a new Attribute, it should be set to 0.

old_id is represented as a JSON string. old_id **MUST** be present.

2.4.2.8. timestamp

timestamp represents a reference time when the attribute was created or last modified. timestamp is expressed in seconds (decimal) since 1st of January 1970 (Unix timestamp). The time zone **MUST** be UTC.

timestamp is represented as a JSON string. timestamp **MUST** be present.

2.4.2.9. comment

comment is a contextual comment field.

comment is represented by a JSON string. comment **MAY** be present.

2.4.2.10. org_id

org_id represents a human-readable identifier referencing the proposal creator's Organisation object. A human-readable identifier **MUST** be represented as an unsigned integer.

Whilst attributes can only be created by the event creator organisation, shadow attributes can be created by third parties. org_id tracks the creator organisation.

org_id is represented by a JSON string and **MUST** be present.

2.4.2.11. proposal_to_delete

proposal_to_delete is a boolean flag that sets whether the shadow attribute proposes to alter an attribute, or whether it proposes to remove it completely.

Accepting a shadow attribute with this flag set will remove the
target attribute.

proposal_to_delete is a JSON boolean and it **MUST** be present. If
proposal_to_delete is set to true, old_id **MUST NOT** be 0.

2.4.2.12. deleted

deleted represents a setting that allows shadow attributes to be
revoked. Revoked shadow attributes only serve to inform other
instances that the shadow attribute is no longer active.

deleted is represented by a JSON boolean. deleted **SHOULD** be present.

2.4.2.13. data

data contains the base64 encoded contents of an attachment or a
malware sample. For malware samples, the sample **MUST** be encrypted
using a password protected zip archive, with the password being
"infected".

data is represented by a JSON string in base64 encoding. data **MUST**
be set for shadow attributes of type malware-sample and attachment.

2.4.2.14. first_seen

first_seen represents a reference time when the attribute was first
seen. first_seen as an ISO 8601 datetime up to the micro-second with
time zone support.

first_seen is represented as a JSON string. first_seen **MAY** be
present.

2.4.2.15. last_seen

last_seen represents a reference time when the attribute was last
seen. last_seen as an ISO 8601 datetime up to the micro-second with
time zone support.

last_seen is represented as a JSON string. last_seen **MAY** be present.

2.4.2.16. value

value represents the payload of an attribute. The format of the
value is dependent on the type of the attribute.

value is represented by a JSON string. value **MUST** be present.

2.4.3. ShadowAttribute Objects

2.4.3.1. Org

An Org object is composed of an uuid, name and id.

The uuid represents the Universally Unique IDentifier (UUID)
[RFC4122] of the organization. The organization UUID is globally
assigned to an organization and **SHALL** be kept overtime.

The name is a readable description of the organization and **SHOULD** be
present. The id is a human-readable identifier generated by the
instance and used as reference in the event. A human-readable
identifier **MUST** be represented as an unsigned integer.

uuid, name and id are represented as a JSON string. uuid, name and
id **MUST** be present.

2.4.3.1.1. Sample Org Object

```
"Org": {
      "id": "2",
      "name": "CIRCL",
      "uuid": "55f6ea5e-2c60-40e5-964f-47a8950d210f"
     }
```

2.5. Object

Objects serve as a contextual bond between a list of attributes
within an event. Their main purpose is to describe more complex
structures than can be described by a single attribute Each object
is created using an Object Template and carries the meta-data of the
template used for its creation within. Objects belong to a meta-
category and are defined by a name.

The schema used is described by the template_uuid and
template_version fields.

A MISP document containing an Object **MUST** contain a name, a meta-
category, a description, a template_uuid and a template_version as
described in the "Object Attributes" section.

2.5.1. Sample Object

```
"Object": {
   "id": "588",
   "name": "file",
   "meta-category": "file",
   "description": "File object describing a file with meta-information",
   "template_uuid": "688c46fb-5edb-40a3-8273-1af7923e2215",
   "template_version": "3",
   "event_id": "56",
   "uuid": "398b0094-0384-4c48-9bf0-22b3dff9c4d3",
   "timestamp": "1505747965",
   "distribution": "5",
   "sharing_group_id": "0",
   "comment": "",
   "deleted": false,
   "ObjectReference": [],
   "Attribute": [
     {
                 "id": "7822",
                 "type": "filename",
                 "category": "Payload delivery",
                 "to_ids": true,
                 "uuid": "59bfe3fb-bde0-4dfe-b5b1-2b10a07724d1",
                 "event_id": "56",
                 "distribution": "0",
                 "timestamp": "1505747963",
                 "comment": "",
                 "sharing_group_id": "0",
                 "deleted": false,
                 "disable_correlation": false,
                 "object_id": "588",
                 "object_relation": "filename",
                 "value": "StarCraft.exe",
                 "ShadowAttribute": [],
                 "first_seen": null,
                 "last_seen": null
     },
     "first_seen": "2019-06-02T22:14:28.711954+00:00",
     "last_seen": null
   ]
}
```

2.5.2. Object Attributes

2.5.2.1. uuid

uuid represents the Universally Unique IDentifier (UUID) [RFC4122]
of the object. The uuid **MUST** be preserved for any updates or

transfer of the same object. UUID version 4 is **RECOMMENDED** when
assigning it to a new object.

2.5.2.2. id

id represents the human-readable identifier associated to the object
for a specific MISP instance. A human-readable identifier **MUST** be
represented as an unsigned integer.

id is represented as a JSON string. id **SHALL** be present.

2.5.2.3. name

name represents the human-readable name of the object describing the
intent of the object package.

name is represented as a JSON string. name **MUST** be present.

2.5.2.4. meta-category

meta-category represents the sub-category of objects that the given
object belongs to. meta-categories are not tied to a fixed list of
options but can be created on the fly.

meta-category is represented as a JSON string. meta-category **MUST** be
present.

2.5.2.5. description

description is a human-readable description of the given object
type, as derived from the template used for creation.

description is represented as a JSON string. description **SHALL** be
present.

2.5.2.6. template_uuid

template_uuid represents the Universally Unique IDentifier (UUID)
[RFC4122] of the template used to create the object. The uuid **MUST**
be preserved to preserve the object's association with the correct
template used for creation. UUID version 4 is **RECOMMENDED** when
assigning it to a new object.

template_uuid is represented as a JSON string. template_uuid **MUST** be
present.

2.5.2.7. template_version

template_version represents a numeric incrementing version of the
template used to create the object. It is used to associate the

object to the correct version of the template and together with the template_uuid forms an association to the correct template type and version.

template_version is represented as a JSON string. template_version **MUST** be present.

2.5.2.8. event_id

event_id represents the human-readable identifier of the event that the object belongs to on a specific MISP instance. A human-readable identifier **MUST** be represented as an unsigned integer.

event_id is represented as a JSON string. event_id **SHALL** be present.

2.5.2.9. timestamp

timestamp represents a reference time when the object was created or last modified. timestamp is expressed in seconds (decimal) since 1st of January 1970 (Unix timestamp). The time zone **MUST** be UTC.

timestamp is represented as a JSON string. timestamp **MUST** be present.

2.5.2.10. distribution

distribution represents the basic distribution rules of the object. The system must adhere to the distribution setting for access control and for dissemination of the object.

distribution is represented by a JSON string. distribution **MUST** be present and be one of the following options:

0 Your Organisation Only
1 This Community Only
2 Connected Communities
3 All Communities
4 Sharing Group

2.5.2.11. sharing_group_id

sharing_group_id represents a human-readable identifier referencing a Sharing Group object that defines the distribution of the object, if distribution level "4" is set. A human-readable identifier **MUST** be represented as an unsigned integer.

sharing_group_id is represented by a JSON string and **SHOULD** be present. If a distribution level other than "4" is chosen the sharing_group_id **MUST** be set to "0".

2.5.2.12. comment

comment is a contextual comment field.

comment is represented by a JSON string. comment **MAY** be present.

2.5.2.13. deleted

deleted represents a setting that allows objects to be revoked. Revoked objects are not actionable and exist merely to inform other instances of a revocation.

deleted is represented by a JSON boolean. deleted **MUST** be present.

2.5.2.14. Attribute

Attribute is an array of attributes that describe the object with data.

Each attribute in an object **MUST** contain the parent event's ID in the event_id field and the parent object's ID in the object_id field.

2.5.2.15. first_seen

first_seen represents a reference time when the object was first seen. first_seen as an ISO 8601 datetime up to the micro-second with time zone support.

first_seen is represented as a JSON string. first_seen **MAY** be present.

2.5.2.16. last_seen

last_seen represents a reference time when the object was last seen. last_seen as an ISO 8601 datetime up to the micro-second with time zone support.

last_seen is represented as a JSON string. last_seen **MAY** be present.

2.6. Object References

Object References serve as a logical link between an Object and another referenced Object or Attribute. The relationship is categorised by an enumerated value from a fixed vocabulary.

The relationship_type is recommended to be taken from the MISP object relationship list [[MISP-R]] is **RECOMMENDED** to ensure a coherent naming of the tags

All Object References **MUST** contain an object_uuid, a referenced_uuid
and a relationship type.

2.6.1. Sample ObjectReference object

```
"ObjectReference": {
                   "id": "195",
                   "uuid": "59c21a2c-c0ac-4083-93b3-363da07724d1",
                   "timestamp": "1505892908",
                   "object_id": "591",
                   "event_id": "113",
                   "referenced_id": "590",
                   "referenced_type": "1",
                   "relationship_type": "derived-from",
                   "comment": "",
                   "deleted": false,
                   "object_uuid": "59c1134d-8a40-4c14-ad94-0f7ba07724d1
                   "referenced_uuid": "59c1133c-9adc-4d06-a34b-0f7ca077
                   }
```

2.6.2. ObjectReference Attributes

2.6.2.1. uuid

uuid represents the Universally Unique IDentifier (UUID) [RFC4122]
of the object reference. The uuid **MUST** be preserved for any updates
or transfer of the same object reference. UUID version 4 is
RECOMMENDED when assigning it to a new object reference.

2.6.2.2. id

id represents the human-readable identifier associated to the object
reference for a specific MISP instance.

id is represented as a JSON string. id **SHALL** be present.

2.6.2.3. timestamp

timestamp represents a reference time when the object was created or
last modified. timestamp is expressed in seconds (decimal) since 1st
of January 1970 (Unix timestamp). The time zone **MUST** be UTC.

timestamp is represented as a JSON string. timestamp **MUST** be
present.

2.6.2.4. object_id

object_id represents the human-readable identifier of the object
that the object reference belongs to on a specific MISP instance. A

human-readable identifier **MUST** be represented as an unsigned integer.

object_id is represented as a JSON string. object_id **SHALL** be present.

2.6.2.5. event_id

event_id represents the human-readable identifier of the event that the object reference belongs to on a specific MISP instance. A human-readable identifier **MUST** be represented as an unsigned integer.

event_id is represented as a JSON string. event_id **SHALL** be present.

2.6.2.6. referenced_id

referenced_id represents the human-readable identifier of the object or attribute that the parent object of the object reference points to on a specific MISP instance.

referenced_id is represented as a JSON string. referenced_id **MAY** be present.

2.6.2.7. referenced_type

referenced_type represents the numeric value describing what the object reference points to, "0" representing an attribute and "1" representing an object

referenced_type is represented as a JSON string. referenced_type **MAY** be present.

2.6.2.8. relationship_type

relationship_type represents the human-readable context of the relationship between an object and another object or attribute as described by the object_reference.

relationship_type is represented as a JSON string. relationship_type **MUST** be present.

2.6.2.9. comment

comment is a contextual comment field.

comment is represented by a JSON string. comment **MAY** be present.

2.6.2.10. deleted

deleted represents a setting that allows object references to be revoked. Revoked object references are not actionable and exist merely to inform other instances of a revocation.

deleted is represented by a JSON boolean. deleted **MUST** be present.

2.6.2.11. object_uuid

object_uuid represents the Universally Unique IDentifier (UUID) [RFC4122] of the object that the given object reference belongs to. The object_uuid **MUST** be preserved to preserve the object reference's association with the object.

2.6.2.12. referenced_uuid

referenced_uuid represents the Universally Unique IDentifier (UUID) [RFC4122] of the object or attribute that is being referenced by the object reference. The referenced_uuid **MUST** be preserved to preserve the object reference's association with the object or attribute.

2.7. EventReport

EventReport are used to complement an event with one or more report in Markdown format. The EventReport contains unstructured information which can be linked to Attributes, Objects, Tags or Galaxy with an extension to the Markdown marking language.

2.7.1. id

id represents the human-readable identifier associated to the EventReport for a specific MISP instance. A human-readable identifier **MUST** be represented as an unsigned integer.

id is represented as a JSON string. id **SHALL** be present.

2.7.2. UUID

uuid represents the Universally Unique IDentifier (UUID) [RFC4122] of the EventReport. The uuid **MUST** be preserved for any updates or transfer of the same EventReport. UUID version 4 is **RECOMMENDED** when assigning it to a new EventReport.

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

2.7.3. event_id

event_id represents the human-readable identifier associating the
EventReport to an event on a specific MISP instance. A human-
readable identifier **MUST** be represented as an unsigned integer.

event_id is represented as a JSON string. event_id **MUST** be present.

2.7.4. name

name represents the information field of the EventReport. name is a
free-text value to provide a human-readable summary of the report.
name **SHOULD** NOT be bigger than 256 characters and **SHOULD** NOT include
new-lines.

name is represented as a JSON string. name **MUST** be present.

2.7.5. content

content includes the raw EventReport in Markdown format with or
without the specific MISP Markdown markup extension.

The markdown extension for MISP is composed with a symbol as prefix
then between square bracket the scope (attribute, object, tag or
galaxymatrix) followed by the UUID in parenthesis.

content is represented as a JSON string. content **MUST** be present.

2.7.6. distribution

distribution represents the basic distribution rules of the
EventReport. The system must adhere to the distribution setting for
access control and for dissemination of the EventReport.

distribution is represented by a JSON string. distribution **MUST** be
present and be one of the following options:

0 Your Organisation Only
1 This Community Only
2 Connected Communities
3 All Communities
4 Sharing Group
5 Inherit Event

2.7.7. sharing_group_id

sharing_group_id represents the local id to the MISP local instance
of the Sharing Group associated for the distribution.

sharing_group_id is represented by a JSON string. sharing_group_id
MUST be present and set to "0" if not used.

2.7.8. timestamp

timestamp represents a reference time when the EventReport was
created or last modified. timestamp is expressed in seconds
(decimal) since 1st of January 1970 (Unix timestamp). The time zone
MUST be UTC.

timestamp is represented as a JSON string. timestamp **MUST** be
present.

2.7.9. deleted

deleted represents a setting that allows EventReport to be revoked.
Revoked EventReport are not actionable and exist merely to inform
other instances of a revocation.

deleted is represented by a JSON boolean. deleted **MUST** be present.

2.8. Tag

A tag is a simple method to classify an event with a simple string.
The tag name can be freely chosen. The tag name can be also chosen
from a fixed machine-tag vocabulary called MISP
taxonomies[[MISP-T]]. When an event is distributed outside an
organisation, the use of MISP taxonomies[[MISP-T]] is **RECOMMENDED** to
ensure a coherent naming of the tags. A tag is represented as a JSON
array where each element describes each tag associated. A tag array
SHALL be at event level or attribute level. A tag element is
described with a name, id, colour and exportable flag.

exportable represents a setting if the tag is kept local or
exportable to other MISP instances. exportable is represented by a
JSON boolean. id is a human-readable identifier that references the
tag on the local instance. colour represents an RGB value of the
tag.

name **MUST** be present. colour, id and exportable **SHALL** be present.

2.8.1. Sample Tag

```
"Tag": [{
        "exportable": true,
        "colour": "#ffffff",
        "name": "tlp:white",
        "id": "2" }]
```

2.9. Sighting

A sighting is an ascertainment which describes whether an attribute has been seen under a given set of conditions. The sighting can include the organisation who sighted the attribute or can be anonymised. Sighting is composed of a JSON array in which each element describes one singular instance of a sighting. A sighting element is a JSON object composed of the following values:

type **MUST** be present. type describes the type of a sighting. MISP allows 3 default types:

Sighting type	Description
0	denotes an attribute which has been seen
1	denotes an attribute which has been seen and confirmed as false-positive
2	denotes an attribute which will be expired at the time of the sighting

Table 1

uuid **MUST** be present. uuid references the uuid of the sighted attribute.

date_sighting **MUST** be present. date_sighting is expressed in seconds (decimal) elapsed since 1st of January 1970 (Unix timestamp). date_sighting represents when the referenced attribute, designated by its uuid, is sighted.

source **MAY** be present. source is represented as a JSON string and represents the human-readable version of the sighting source, which can be a given piece of software (e.g. SIEM), device or a specific analytical process.

id, event_id and attribute_id are represented as a JSON string and **MAY** be present.

id represents the human-readable identifier of the sighting reference which belongs to a specific MISP instance. event_id represents the human-readable identifier of the event referenced by the sighting and belongs to a specific MISP instance. attribute_id represents the human-readable identifier of the attribute referenced by the sighting and belongs to a specific MISP instance.

org_id **MAY** be present along the JSON object describing the organisation. If the org_id is not present, the sighting is considered as anonymised.

org_id represents the human-readable identifier of the organisation
which did the sighting and belongs to a specific MISP instance.

A human-readable identifier **MUST** be considered as an unsigned
integer.

2.9.1. Sample Sighting

```
"Sighting": [
                {
                                "id": "13599",
                                "attribute_id": "1201615",
                                "event_id": "10164",
                                "org_id": "2",
                                "date_sighting": "1517581400",
                                "uuid": "5a747459-41b4-4826-9b29-42dd950
                                "source": "M2M-CIRCL",
                                "type": "0",
                                "Organisation": {
                                        "id": "2",
                                        "uuid": "55f6ea5e-2c60-40e5-964f
                                        "name": "CIRCL"
                                }
                },
                {
                                "id": "13601",
                                "attribute_id": "1201615",
                                "event_id": "10164",
                                "org_id": "2",
                                "date_sighting": "1517581401",
                                "uuid": "5a74745a-a190-4d04-b719-4916950
                                "source": "M2M-CIRCL",
                                "type": "0",
                                "Organisation": {
                                        "id": "2",
                                        "uuid": "55f6ea5e-2c60-40e5-964f
                                        "name": "CIRCL"
                                }
                }
        ]
```

2.10. Galaxy

A galaxy is a simple method to express a large object called cluster
that can be attached to MISP events. A cluster can be composed of
one or more elements. Elements are expressed as key-values.

2.10.1. Sample Galaxy

```
"Galaxy": [ {
        "id": "18",
        "uuid": "698774c7-8022-42c4-917f-8d6e4f06ada3",
        "name": "Threat Actor",
        "type": "threat-actor",
        "description": "Threat actors are characteristics of maliciou
                        (or adversaries) representing a cyber attack t
                        including presumed intent and historically obs
            "version": "1",
      "GalaxyCluster": [
        {
            "id": "1699",
            "uuid": "7cdff317-a673-4474-84ec-4f1754947823",
            "type": "threat-actor",
            "value": "Anunak",
            "tag_name": "misp-galaxy:threat-actor=\"Anunak\"",
            "description": "Groups targeting financial organizations
                or people with significant financial assets.",
            "galaxy_id": "18",
            "source": "MISP Project",
            "authors": [
                "Alexandre Dulaunoy",
                "Florian Roth",
                "Thomas Schreck",
                "Timo Steffens",
                "Various"
            ],
            "tag_id": "111",
                "meta": {
                    "synonyms": [
                        "Carbanak",
                        "Carbon Spider"
                    ],
                    "country": [
                        "RU"
                    ],
                    "motive": [
                        "Cybercrime"
                    ]
                }
            }
        ]
    }
]
```

3. **JSON Schema**

The JSON Schema [JSON-SCHEMA] below defines the structure of the
MISP core format as literally described before. The JSON Schema is
used to validate MISP events at creation time or parsing.

```json
{
  "$schema": "http://json-schema.org/draft-04/schema#",
  "title": "Validator for misp events",
  "id": "https://github.com/MISP/MISP/blob/2.4/format/2.4/schema.json",
  "defs": {
    "org": {
      "type": "object",
      "additionalProperties": false,
      "properties": {
        "id": {
          "type": "string"
        },
        "name": {
          "type": "string"
        },
        "uuid": {
          "type": "string"
        }
      },
      "required": [
        "uuid"
      ]
    },
    "orgc": {
      "type": "object",
      "additionalProperties": false,
      "properties": {
        "id": {
          "type": "string"
        },
        "name": {
          "type": "string"
        },
        "uuid": {
          "type": "string"
        }
      },
      "required": [
        "uuid"
      ]
    },
    "sharing_group": {
      "type": "object",
      "additionalProperties": false,
      "properties": {
        "id": {
          "type": "string"
        },
        "name": {
```

```
      "type": "string"
    },
    "releasability": {
      "type": "string"
    },
    "description": {
      "type": "string"
    },
    "uuid": {
      "type": "string"
    },
    "organisation_uuid": {
      "type": "string"
    },
    "org_id": {
      "type": "string"
    },
    "sync_user_id": {
      "type": "string"
    },
    "active": {
      "type": "boolean"
    },
    "created": {
      "type": "string"
    },
    "modified": {
      "type": "string"
    },
    "local": {
      "type": "boolean"
    },
    "roaming": {
      "type": "boolean"
    },
    "Organisation": {
      "$ref": "#/defs/org"
    },
    "SharingGroupOrg": {
      "type": "array",
      "uniqueItems": true,
      "items": {
        "$ref": "#/defs/sharing_group_org"
      }
    },
    "SharingGroupServer": {
      "type": "array",
      "uniqueItems": true,
      "items": {
```

```json
          "$ref": "#/defs/sharing_group_server"
        }
      },
      "required": [
        "uuid"
      ]
    },
    "required": [
      "uuid"
    ]
  },
  "sharing_group_org": {
    "type": "object",
    "additionalProperties": false,
    "properties": {
      "id": {
        "type": "string"
      },
      "sharing_group_id": {
        "type": "string"
      },
      "org_id": {
        "type": "string"
      },
      "extend": {
        "type": "boolean"
      },
      "Organisation": {
        "$ref": "#/defs/org"
      }
    }
  },
  "sharing_group_server": {
    "type": "object",
    "additionalProperties": false,
    "properties": {
      "id": {
        "type": "string"
      },
      "sharing_group_id": {
        "type": "string"
      },
      "server_id": {
        "type": "string"
      },
      "all_orgs": {
        "type": "boolean"
      },
      "Server": {
```

```
        "$ref": "#/defs/server"
      }
    }
  },
  "server": {
    "type": "object",
    "additionalProperties": false,
    "properties": {
      "id": {
        "type": "string"
      },
      "url": {
        "type": "string"
      },
      "name": {
        "type": "string"
      }
    }
  },
  "object": {
    "type": "object",
    "additionalProperties": false,
    "properties": {
      "uuid": {
        "type": "string"
      },
      "name": {
        "type": "string"
      },
      "event_id": {
        "type": "string"
      },
      "description": {
        "type": "string"
      },
      "template_uuid": {
        "type": "string"
      },
      "template_version": {
        "type": "string"
      },
      "id": {
        "type": "string"
      },
      "meta-category": {
        "type": "string"
      },
      "deleted": {
        "type": "boolean"
```

```json
        },
        "timestamp": {
          "type": "string"
        },
        "first_seen": {
          "type": "string"
        },
        "last_seen": {
          "type": "string"
        },
        "distribution": {
          "type": "string"
        },
        "sharing_group_id": {
          "type": "string"
        },
        "comment": {
          "type": "string"
        },
        "ObjectReference": {
            "type": "array",
            "uniqueItems": true,
            "items": {
              "$ref": "#/defs/objectreference"
            }
        },
        "Attribute": {
          "type": "array",
          "uniqueItems": true,
          "items": {
            "$ref": "#/defs/attribute"
          }
        }
      }
    },
    "sighthing": {
      "type": "object",
      "additionalProperties": false,
      "properties": {
        "id": {
          "type": "string"
        },
        "attribute_id": {
          "type": "string"
        },
        "event_id": {
          "type": "string"
        },
        "source": {
```

```
          "type": "string"
        },
        "type": {
          "type": "string"
        },
        "org_id": {
          "type": "string"
        },
        "date_sighting": {
          "type": "string"
        },
        "uuid": {
          "type": "string"
        },
        "Organisation": {
            "$ref": "#/defs/organisation"
        }
      }
    },
    "organisation": {
      "type": "object",
      "additionalProperties": false,
      "properties": {
        "id": {
          "type": "string"
        },
        "uuid": {
          "type": "string"
        },
        "name": {
          "type": "string"
        }
      }
    },
    "objectreference": {
      "type": "object",
      "additionalProperties": false,
      "properties": {
        "deleted": {
          "type": "boolean"
        },
        "object_id": {
          "type": "string"
        },
        "event_id": {
          "type": "string"
        },
        "timestamp": {
          "type": "string"
```

```
        },
        "id": {
          "type": "string"
        },
        "uuid": {
          "type": "string"
        },
        "type": {
          "type": "string"
        },
        "referenced_id": {
          "type": "string"
        },
        "referenced_uuid": {
          "type": "string"
        },
        "referenced_type": {
          "type": "string"
        },
        "relationship_type": {
          "type": "string"
        },
        "object_uuid": {
          "type": "string"
        },
        "comment": {
          "type": "string"
        },
        "Object": {
          "$ref": "#/defs/object"
        }
      }
    },
    "attribute": {
      "type": "object",
      "additionalProperties": false,
      "properties": {
        "id": {
          "type": "string"
        },
        "old_id": {
          "type": "string"
        },
        "type": {
          "type": "string"
        },
        "category": {
          "type": "string"
        },
```

```
"to_ids": {
  "type": "boolean"
},
"uuid": {
  "type": "string"
},
"event_id": {
  "type": "string"
},
"event_uuid": {
  "type": "string"
},
"proposal_to_delete": {
  "type": "boolean"
},
"validationIssue": {
  "type": "boolean"
},
"Org": {
  "$ref": "#/defs/organisation"
},
"org_id": {
  "type": "string"
},
"distribution": {
  "type": "string"
},
"timestamp": {
  "type": "string"
},
"first_seen": {
  "type": "string"
},
"last_seen": {
  "type": "string"
},
"comment": {
  "type": "string"
},
"sharing_group_id": {
  "type": "string"
},
"deleted": {
  "type": "boolean"
},
"disable_correlation": {
  "type": "boolean"
},
"value": {
```

```
      "type": "string"
    },
    "data": {
      "type": "string"
    },
    "object_relation": {
      "type": ["string", "null"]
    },
    "object_id": {
      "type": "string"
    },
    "SharingGroup": {
      "$ref": "#/defs/sharing_group"
    },
    "ShadowAttribute": {
      "type": "array",
      "uniqueItems": true,
      "items": {
        "$ref": "#/defs/attribute"
      }
    },
    "Sighting": {
        "type": "array",
        "uniqueItems": true,
        "items": {
          "$ref": "#/defs/sighthing"
        }
    },
    "Galaxy": {
      "type": "array",
      "uniqueItems": true,
      "items": {
        "$ref": "#/defs/galaxy"
      }
    },
    "Tag": {
      "uniqueItems": true,
      "type": "array",
      "items": {
        "$ref": "#/defs/tag"
      }
    }
  }
},
"event": {
  "type": "object",
  "additionalProperties": false,
  "properties": {
    "id": {
```

```
      "type": "string"
    },
    "orgc_id": {
      "type": "string"
    },
    "org_id": {
      "type": "string"
    },
    "date": {
      "type": "string"
    },
    "extends_uuid": {
        "type": "string"
    },
    "threat_level_id": {
      "type": "string"
    },
    "info": {
      "type": "string"
    },
    "published": {
      "type": "boolean"
    },
    "uuid": {
      "type": "string"
    },
    "attribute_count": {
      "type": "string"
    },
    "analysis": {
      "type": "string"
    },
    "timestamp": {
      "type": "string"
    },
    "distribution": {
      "type": "string"
    },
    "proposal_email_lock": {
      "type": "boolean"
    },
    "locked": {
      "type": "boolean"
    },
    "publish_timestamp": {
      "type": "string"
    },
    "sharing_group_id": {
      "type": "string"
```

```
    },
    "disable_correlation": {
      "type": "boolean"
    },
    "event_creator_email": {
      "type": "string"
    },
    "Org": {
      "$ref": "#/defs/org"
    },
    "Orgc": {
      "$ref": "#/defs/org"
    },
    "SharingGroup": {
      "$ref": "#/defs/sharing_group"
    },
    "Attribute": {
      "type": "array",
      "uniqueItems": true,
      "items": {
        "$ref": "#/defs/attribute"
      }
    },
    "ShadowAttribute": {
      "type": "array",
      "uniqueItems": true,
      "items": {
        "$ref": "#/defs/attribute"
      }
    },
    "RelatedEvent": {
      "type": "array",
      "uniqueItems": true,
      "items": {
        "type": "object",
        "additionalProperties": false,
        "properties": {
          "Event":{
            "$ref": "#/defs/event"
          }
        }
      }
    },
    "Galaxy": {
      "type": "array",
      "uniqueItems": true,
      "items": {
        "$ref": "#/defs/galaxy"
      }
```

```
      },
      "Object": {
          "type": "array",
          "uniqueItems": true,
          "items": {
              "$ref": "#/defs/object"
          }
      },
      "Tag": {
        "type": "array",
        "uniqueItems": true,
        "items": {
          "$ref": "#/defs/tag"
        }
      }
    }
  },
  "tag": {
    "type": "object",
    "additionalProperties": false,
    "properties": {
      "id": {
        "type": "string"
      },
      "name": {
        "type": "string"
      },
      "colour": {
        "type": "string"
      },
      "exportable": {
        "type": "boolean"
      },
      "hide_tag": {
        "type": "boolean"
      },
      "user_id": {
        "type": "string"
      }
    }
  },
  "galaxy": {
    "type": "object",
    "additionalProperties": false,
    "properties": {
      "id": {
        "type": "string"
      },
      "uuid": {
```

```
        "type": "string"
      },
      "name": {
        "type": "string"
      },
      "type": {
        "type": "string"
      },
      "description": {
        "type": "string"
      },
      "version": {
        "type": "string"
      },
      "icon": {
        "type": "string"
      },
      "namespace": {
        "type": "string"
      },
      "GalaxyCluster": {
        "type": "array",
        "uniqueItems": true,
        "items": {
          "$ref": "#/defs/galaxy_cluster"
        }
      }
    }
  },
  "galaxy_cluster": {
    "type": "object",
    "additionalProperties": false,
    "properties": {
      "id": {
        "type": "string"
      },
      "uuid": {
        "type": "string"
      },
      "type": {
        "type": "string"
      },
      "value": {
        "type": "string"
      },
      "tag_name": {
        "type": "string"
      },
      "description": {
```

```
                  "type": "string"
              },
              "galaxy_id": {
                  "type": "string"
              },
              "version": {
                  "type": "string"
              },
              "source": {
                  "type": "string"
              },
              "authors": {
                  "type": "array",
                  "uniqueItems": true,
                  "items": {
                      "type": "string"
                  }
              },
              "tag_id": {
                  "type": "string"
              },
              "meta": {
                  "type": "object"
              }
          }
      }
  },
  "type": "object",
  "properties": {
      "Event": {
          "$ref": "#/defs/event"
      }
  },
  "required": [
      "Event"
  ]
}
```

4. Manifest

MISP events can be shared over an HTTP repository, a file package or
USB key. A manifest file is used to provide an index of MISP events
allowing to only fetch the recently updated files without the need
to parse each json file.

4.1. Format

A manifest file is a simple JSON file named manifest.json in a
directory where the MISP events are located. Each MISP event is a
file located in the same directory with the event uuid as filename
with the json extension.

The manifest format is a JSON object composed of a dictionary where
the field is the uuid of the event.

Each uuid is composed of a JSON object with the following fields
which came from the original event referenced by the same uuid:

   *info (**MUST**)
   *Orgc object (**MUST**)
   *analysis (**SHALL**)
   *timestamp (**MUST**)
   *date (**MUST**)
   *threat_level_id (**SHALL**)

In addition to the fields originating from the event, the following
fields can be added:

   *integrity:sha256 represents the SHA256 value in hexadecimal
    representation of the associated MISP event file to ensure
    integrity of the file. (**SHOULD**)
   *integrity:pgp represents a detached PGP signature [RFC4880] of
    the associated MISP event file to ensure integrity of the file.
    (**SHOULD**)

If a detached PGP signature is used for each MISP event, a detached
PGP signature is a **MUST** to ensure integrity of the manifest file. A
detached PGP signature for a manifest file is a manifest.json.asc
file containing the PGP signature.

4.1.1. Sample Manifest

```json
{
  "57c6ac4c-c60c-4f79-a38f-b666950d210f": {
    "info": "Malspam 2016-08-31 (.wsf in .zip) - campaign: Photo",
    "Orgc": {
      "id": "2",
      "name": "CIRCL",
      "uuid": "55f6ea5e-2c60-40e5-964f-47a8950d210f"
    },
    "analysis": "0",
    "Tag": [
      {
        "colour": "#3d7a00",
        "name": "circl:incident-classification=\"malware\""
      },
      {
        "colour": "#ffffff",
        "name": "tlp:white"
      }
    ],
    "timestamp": "1472638251",
    "date": "2016-08-31",
    "threat_level_id": "3"
  },
  "5720accd-dd28-45f8-80e5-4605950d210f": {
    "info": "Malspam 2016-04-27 - Locky",
    "Orgc": {
      "id": "2",
      "name": "CIRCL"
    },
    "analysis": "2",
    "Tag": [
      {
        "colour": "#ffffff",
        "name": "tlp:white"
      },
      {
        "colour": "#3d7a00",
        "name": "circl:incident-classification=\"malware\""
      },
      {
        "colour": "#2c4f00",
        "name": "malware_classification:malware-category=\"Ransomware\""
      }
    ],
    "timestamp": "1461764231",
    "date": "2016-04-27",
    "threat_level_id": "3"
  }
}
```

5. Implementation

MISP format is implemented by different software including the MISP threat sharing platform and libraries like PyMISP [MISP-P]. Implementations use the format as an export/import mechanism, staging transport format or synchronisation format as used in the MISP core platform. MISP format doesn't impose any restriction on the data representation of the format in data-structure of other implementations.

6. Security Considerations

MISP events might contain sensitive or confidential information. Adequate access control and encryption measures shall be implemented to ensure the confidentiality of the MISP events.

Adversaries might include malicious content in MISP events and attributes. Implementation **MUST** consider the input of malicious inputs beside the standard threat information that might already include malicious intended inputs.

7. Acknowledgements

The authors wish to thank all the MISP community who are supporting the creation of open standards in threat intelligence sharing. A special thank to Nicolas Bareil for the review of the JSON Schema.

8. References

9. 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>.

[RFC4880]   Callas, J., Donnerhacke, L., Finney, H., Shaw, D., and R.
            Thayer, "OpenPGP Message Format", RFC 4880, DOI 10.17487/
            RFC4880, November 2007, <https://www.rfc-editor.org/info/
            rfc4880>.

[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>.

10. 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-R]   Community, M., "MISP Object Relationship Types - common vocabulary of relationships", <https://github.com/MISP/misp-objects/tree/master/relationships>.

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

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