MISP Standard

The collaborative intelligence standard powering intelligence and information exchange, sharing and modeling.

Alexandre Dulaunoy

http://www.misp-standard.org/
Twitter: @*MISPProject*

University of Lorraine

MISP Standard

- Following the grow of organisations relying on MISP, the **JSON format used by MISP are standardised under the misp-standard.org umbrella**
- The goal is to provide a flexible set of standards to support information exchange and data modeling in the following field:
  - Cybersecurity intelligence
  - Threat intelligence
  - Financial fraud
  - Vulnerability information
  - Border control information
  - Digital Forensic and Incident Response
  - and intelligence at large

Standard - MISP core format

This standard describes the **MISP core format** used to exchange indicators and threat information between MISP instances. The **JSON format includes the overall structure along with the semantics associated for each respective key**. The format is described to support other implementations, aiming to reuse the format and ensuring the interoperability with the existing MISP software and other Threat Intelligence Platforms.

MISP object template format

This standard describes the **MISP object** template format which describes a simple JSON format to represent the various templates used to construct MISP objects. A **public directory of common MISP object templates and relationships** is available and relies on the MISP object reference format.

MISP galaxy format

This standard describes the **MISP galaxy format which describes a simple JSON format to represent galaxies and clusters** that can be attached to MISP events or attributes. A public directory of MISP galaxies is available and relies on the MISP galaxy format. MISP galaxies are used to attach additional information structures such as MISP events or attributes. **MISP galaxy is a public repository of known malware, threats actors and various other collections of data that can be used to mark, classify or label data in threat information sharing**.

SightingDB format

This standard describes the format used by SightingDB to give automated context to a given Attribute by **counting occurrences and tracking times of observability**. SightingDB was designed to provide to MISP and other tools an interoperable, scalable and fast way to store and retrieve attributes sightings.

Internet-Draft - IETF for MISP formats and MISP standard

- If you want to contribute to our IETF Internet-Draft for the MISP standard, misp-rfc[1] is the repository where to contribute.
- **Update only the markdown file**, the XML and ASCII for the IETF I-D are automatically generated.
- If a major release or updates happen in the format, we will publish the I-D to the IETF[2].
- The process is always MISP implementation $\rightarrow$ IETF I-D updates.
- Then published standards in misp-standard.org.

---

[1] https://github.com/MISP/misp-rfc

[2] https://datatracker.ietf.org/doc/search/?name=misp&activedrafts=on&rfcs=on