

MISP and Decaying of Indicators

An indicator scoring method and ongoing imple-

info@circl.lu

December 29, 2018

Team CIRCL



MISP
Threat Sharing

- Various users and organisations can share data via MISP, multiple parties can be involved
 - ▶ Trust, data quality and time-to-live issues
 - ▶ Each user/organisation has different use-cases and interests
- Attributes can be shared in large quantities (more than 1.3 million on MISPPRIV)
 - ▶ Partial info about their validity (sightings)
 - ▶ Partial info about their freshness (last update)
 - ▶ Various conflicting interests such as operational security, attribution, source reliability evaluation...

Sightings add temporal context to indicators. A user, script or an IDS can extend the information related to indicators by reporting back to MISP that an indicator has been seen, or that an indicator can be considered as a false-positive

- Sightings give more credibility/visibility to indicators
- This information can be used to **prioritise and decay indicators**

ORGANISATIONS OPT-IN - SETTING A LEVEL OF CONFIDENCE

MISP is a peer-to-peer system, information passes through multiple instances.

- Producers can add context (such as tags from taxonomies, galaxies) about their asserted confidence or the reliability of the data
- Consumers can have different levels of trust in the producers and/or analysts themselves

Description	Value	Description	Value
Completely reliable	100	Confirmed by other sources	100
Usually reliable	75	Probably true	75
Fairly reliable	50	Possibly true	50
Not usually reliable	25	Doubtful	25
Unreliable	0	Improbable	0
Reliability cannot be judged	50	Truth cannot be judged	50
Deliberatly deceptive	0		

When scoring indicators¹, multiple parameters² can be taken into account. The **base score** is calculated with the following in mind:

- The reliability in the producer
- The trust in the data as signaled by the producer

$$base_score = weight_{tg} \cdot tags + \omega_{sc} \cdot source_confidence$$

¹Paper available: <https://arxiv.org/pdf/1803.11052>

²at a variable extent as required

The weighted score is calculated using:

- The lifetime of the indicator (e.g. IP address vs hash value of a file)
 - ▶ The lifespan of the indicator (short for an IP - long for an hash): τ
 - ▶ The decay rate \rightarrow Speed at which an attribute loses value: δ
 - ▶ Weighed score is reset to its base score as new sightings are received

$$score = base_score \cdot \left(1 - \left(\frac{t}{\tau_a} \right)^{\frac{1}{\delta_a}} \right)$$

ONGOING IMPLEMENTATION IN MISP

Setting thresholds and retrieving the information should be simple and straightforward for the user:

- Automatic scoring based on default values
- User-friendly UI to manually set lifetime parameters
- Interaction through the API

