

# MISP AND DECAYING OF INDICATORS

AN INDICATOR SCORING METHOD AND ONGOING IMPLE-

TEAM CIRCL

[INFO@CIRCL.LU](mailto:INFO@CIRCL.LU)

APRIL 15, 2024



**MISP**  
Threat Sharing

# EXPIRING IOCs: WHY AND HOW?

- **Sharing information** about threats **is crucial**
- Organisations are sharing more and more

Contribution by **unique organisation** (Orgc.name) on MISPPriv:

Date	Unique Org
2013	17
2014	43
2015	82
2016	105
2017	118
2018	125
2019-10	135

```
1 {  
2   "distribution": [1, 2, 3]  
3 }
```

- 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
      - Conflicting interests such as operational security, attribution,... (depends on the user)
- Can be partially solved with *Taxonomies*

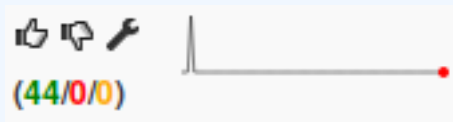
- Various users and organisations can share data via MISP, multiple parties can be involved
  - ▶ **Trust, data quality** and **time-to-live** issues
  - ▶ Each user/organisation has **different use-cases** and interests
    - Conflicting interests such as operational security, attribution,... (depends on the user)
- Can be partially solved with *Taxonomies*
- Attributes can be shared in large quantities (more than 7.3 million on MISPPRIV)
  - ▶ Partial info about their **freshness** (*Sightings*)
  - ▶ Partial info about their **validity** (last update)
- Can be partially solved with our *Decaying model*

# REQUIREMENTS TO ENJOY THE DECAYING FEATURE IN MISP

- Starting from **MISP 2.4.116**, the decaying feature is available
- Don't forget to update the decay models and enable the ones you want
- The decaying feature has no impact on the information in MISp, it's just an overlay to be used in the user-interface and API
- Decay strongly relies on *Taxonomies* and *Sightings*, don't forget to review their configuration

*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**



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
- Users might have other contextual needs

→ Achieved thanks to *Taxonomies*



# TAXONOMIES - REFRESHER (1)

## Taxonomies

« previous 1 2 next »

Id ↑	Namespace	Description	Version	Enabled	Required	Active Tags	Actions
181	workflow	Workflow support language is a common language to support intelligence analysts to perform their analysis on data and information.	9	Yes	<input type="checkbox"/>	27 / 26 (enable all)	- 🔍 🗑️
180	vocabulaire-des-probabilites-estimatives	Ce vocabulaire attribue des valeurs en pourcentage à certains énoncés de probabilité	2	Yes	<input type="checkbox"/>	5 / 5	- 🔍 🗑️
179	threats-to-dns	An overview of some of the known attacks related to DNS as described by Torabi, S., Boukhlouta, A., Assi, C., & Debbabi, M. (2018) in Detecting Internet Abuse by Analyzing Passive DNS Traffic: A Survey of Implemented Systems. IEEE Communications Surveys & Tutorials, 1–1. doi:10.1109/comst.2018.2849614	1	No	<input type="checkbox"/>	0 / 18	+ 🔍 🗑️
178	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.	2	Yes	<input type="checkbox"/>	11 / 11	- 🔍 🗑️

- Tagging is a simple way to attach a classification to an *Event* or an *Attribute*
- Classification must be globally used to be efficient

# TAXONOMIES - REFRESHER (2)

## ADMIRALTY-SCALE Taxonomy Library

<b>Id</b>	127
<b>Namespace</b>	admiralty-scale
<b>Description</b>	The Admiralty Scale or Ranking (also called the NATO System) is used to rank the reliability of a source and the credibility of an information. Reference based on FM 2-22.3 (FM 34-52) HUMAN INTELLIGENCE COLLECTOR OPERATIONS and NATO documents.
<b>Version</b>	4
<b>Enabled</b>	Yes (disable)

- previous   next -

<input type="checkbox"/> Tag	Expanded	Numerical value	Events	Attributes	Tags	Action
<input type="checkbox"/> admiralty-scale:information-credibility="1"	Information Credibility: Confirmed by other sources	100	6	0	admiralty-scale:information-credibility="1"	⏪ ⏩ -
<input type="checkbox"/> admiralty-scale:information-credibility="2"	Information Credibility: Probably true	75	21	1	admiralty-scale:information-credibility="2"	⏪ ⏩ -
<input type="checkbox"/> admiralty-scale:information-credibility="3"	Information Credibility: Possibly true	50	16	5	admiralty-scale:information-credibility="3"	⏪ ⏩ -
<input type="checkbox"/> admiralty-scale:information-credibility="4"	Information Credibility: Doubtful	25	2	0	admiralty-scale:information-credibility="4"	⏪ ⏩ -
<input type="checkbox"/> admiralty-scale:information-credibility="5"	Information Credibility: Improbable	0	1	0	admiralty-scale:information-credibility="5"	⏪ ⏩ -
<input type="checkbox"/> admiralty-scale:information-credibility="6"	Information Credibility: Truth cannot be judged	50	9	2	admiralty-scale:information-credibility="6"	⏪ ⏩ -
<input type="checkbox"/> admiralty-scale:source-reliability="a"	Source Reliability: Completely reliable	100	1	0	admiralty-scale:source-reliability="a"	⏪ ⏩ -
<input type="checkbox"/> admiralty-scale:source-reliability="b"	Source Reliability: Usually reliable	75	21	76	admiralty-scale:source-reliability="b"	⏪ ⏩ -
<input type="checkbox"/> admiralty-scale:source-reliability="c"	Source Reliability: Fairly reliable	50	9	8	admiralty-scale:source-reliability="c"	⏪ ⏩ -
<input type="checkbox"/> admiralty-scale:source-reliability="d"	Source Reliability: Not usually reliable	25	2	0	admiralty-scale:source-reliability="d"	⏪ ⏩ -
<input type="checkbox"/> admiralty-scale:source-reliability="e"	Source Reliability: Unreliable	0	0	0	admiralty-scale:source-reliability="e"	⏪ ⏩ -
<input type="checkbox"/> admiralty-scale:source-reliability="f"	Source Reliability: Reliability cannot be judged	50	10	7	admiralty-scale:source-reliability="f"	⏪ ⏩ -
<input type="checkbox"/> admiralty-scale:source-reliability="g"	Source Reliability: Deliberately deceptive	0	N/A	N/A		+

→ Cherry-pick allowed Tags

- Some taxonomies have `numerical_value`
  - Can be used to prioritise *Attributes*

Description	Value
Completely reliable	100
Usually reliable	75
Fairly reliable	50
Not usually reliable	25
Unreliable	0
Reliability cannot be judged	50 ?
Deliberately deceptive	0 ?

Description	Value
Confirmed by other sources	100
Probably true	75
Possibly true	50
Doubtful	25
Improbable	0
Truth cannot be judged	50 ?

$$\text{score}(\text{Attribute}) = \text{base\_score}(\text{Attribute}, \text{Model}) \bullet \text{decay}(\text{Model}, \text{time})$$

Where,

- $\text{score} \in [0, +\infty$
- $\text{base\_score} \in [0, 100]$
- $\text{decay}$  is a function defined by model's parameters controlling decay speed
- $\text{Attribute}$  Contains *Attribute's* values and metadata (*Taxonomies, Galaxies, ...*)
- $\text{Model}$  Contains the *Model's* configuration

# CURRENT IMPLEMENTATION IN MISP

# IMPLEMENTATION IN MISP: Event/view

The screenshot displays the MISP interface for viewing an event. At the top, there are navigation tabs: Photos, Galaxy, Event graph, Correlation graph, ATTACK matrix, Attributes, and Discussion. Below this, a search bar contains the text "45: Decay...". A "Galaxies" section is visible with a search icon and a plus sign. Below that, there are navigation buttons: "previous", "next", and "view all".

The main content area shows a table of events. The table has columns for Date, Org, Category, Type, Value, Tags, Galaxies, Comment, Correlate, Related Events, Feed hits, IDS, Distribution, Sightings, Activity, Score, and Actions. The "Decay score" toggle is active, and the "Filtering tool (1)" is also active. The table lists several events, each with a "Decay score" value and a "Model 5" score.

Date	Org	Category	Type	Value	Tags	Galaxies	Comment	Correlate	Related Events	Feed hits	IDS	Distribution	Sightings	Activity	Score	Actions
2019-09-12		Network activity	ip-src	5.5.5.5								Inherit	(0/0)		NIDS Simple Decaying ... 65.26 Model 5 79.88	
2019-08-13		Network activity	ip-src	8.8.8.8	admiralty-scale:source-reliability="A" retention:expired				1 2 2 2 Show 11 more...	S1.1 S1.2		Inherit	(5/0)		NIDS Simple Decaying ... 54.6 Model 5 52.69	
2019-08-13		Network activity	ip-src	9.9.9.9	admiralty-scale:source-reliability="C" misp:confidence-level="completely-confident" Ipnumber				1 3 1 9 Show 6 more...	S1.1		Inherit	(4/1)		NIDS Simple Decaying ... 37.43 Model 5 0	
2019-08-13		Network activity	ip-src	7.7.7.7	admiralty-scale:information-credibility="4" retention:2U				41			Inherit	(3/0)		NIDS Simple Decaying ... 37.41 Model 5 0	
2019-07-18		Network activity	ip-src	6.6.6.6					41			Inherit	(0/0)		NIDS Simple Decaying ... 23.31 Model 5 0	

## ■ Decay score toggle button

- ▶ Shows Score for each Models associated to the Attribute type

# IMPLEMENTATION IN MISP: API RESULT

/attributes/restSearch

```
1 "Attribute": [  
2   {  
3     "category": "Network activity",  
4     "type": "ip-src",  
5     "to_ids": true,  
6     "timestamp": "1565703507",  
7     [...]  
8     "value": "8.8.8.8",  
9     "decay_score": [  
10      {  
11        "score": 54.475223849544456,  
12        "decayed": false,  
13        "DecayingModel": {  
14          "id": "85",  
15          "name": "NIDS Simple Decaying Model"  
16        }  
17      }  
18    ],  
19  [...]
```

- **Automatic scoring** based on default values
- **User-friendly UI** to manually set *Model* configuration (lifetime, decay, etc.)
- **Simulation** tool
- Interaction through the **API**
- Opportunity to create your **own** formula or algorithm



# DECAYING MODELS IN DEPTH

# SCORING INDICATORS: base\_score (1)

$$\text{score}(\text{Attribute}) = \text{base\_score}(\text{Attribute}, \text{Model}) \bullet \text{decay}(\text{Model}, \text{time})$$

When scoring indicators<sup>1</sup>, multiple parameters<sup>2</sup> can be taken into account. The **base score** is calculated with the following in mind:

- Data reliability, credibility, analyst skills, custom prioritisation tags (economical-impact), etc.
- Trust in the source

$$\text{base\_score} = \omega_{tg} \cdot \text{tags} + \omega_{sc} \cdot \text{source\_confidence}$$

Where,

$$\omega_{sc} + \omega_{tg} = 1$$

---

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

<sup>2</sup>at a variable extent as required

## SCORING INDICATORS: base\_score (2)

Current implementation ignores source\_confidence:

→  $base\_score = tags$

Tag	Computation			Result
	Eff. Ratio		numerical_value	
admiralty-scale:source-reliability="Completely reliable"	0.50	*	100.00	50.00
phishing:psychological-acceptability="high"	0.50	*	75.00	37.50
				<b>87.50</b>

→ The base\_score can be use to prioritize attribute based on their attached context and source

$$\text{score}(\text{Attribute}) = \text{base\_score}(\text{Attribute}, \text{Model}) \bullet \text{decay}(\text{Model}, \text{time})$$

The decay is calculated using:

- The lifetime of the indicator
  - ▶ May vary depending on the indicator type
  - ▶ short for an IP, long for an hash
- The decay rate, or speed at which an attribute loses score over time
- The time elapsed since the latest update or sighting

→ decay rate is **re-initialized upon sighting** addition, or said differently, the score is reset to its base score as new *sightings* are applied.

$$score = base\_score \cdot \left( 1 - \left( \frac{t}{\tau} \right)^{\frac{1}{\delta}} \right)$$

- $\tau$  = lifetime
- $\delta$  = decay speed

$$\rightarrow score = base\_score \cdot \left(1 - \left(\frac{t}{\tau}\right)^{\frac{1}{\delta}}\right)$$

*Models* are an instantiation of the formula where elements can be defined:

- Parameters: *lifetime*, *decay\_rate*, *threshold*
- *base\_score*
- *default base\_score*
- *formula*
- associate *Attribute* types
- creator organisation

Multiple model types are available

- **Default Models:** Models created and shared by the community. Available from `misp-decaying-models` repository<sup>3</sup>.
  - ▶ → Not editable
- **Organisation Models:** Models created by a user belonging to an organisation
  - ▶ These models can be hidden or shared to other organisation
  - ▶ → Editable









---

<sup>3</sup><https://github.com/MISP/misp-decaying-models.git>

# IMPLEMENTATION IN MISP: INDEX

## Decaying Models

« previous   next »

All Models		My Models		Shared Models		Default Models				
ID	Organization	Usable to everyone	Name	Description	Parameters { }	Formula	# Assigned Types	Version	Enabled	Actions
29	1	✓	Phishing model	Simple model to rapidly decay phishing website.	<pre>{   "lifetime": 3,   "decay_speed": 2.3,   "threshold": 30,   "default_base_score": 80,   "base_score_config": {     "estimative-language": 0.5,     "phishing": 0.5   } }</pre>	Polynomial	9	1	✓	   
85	1	✗	NIDS Simple Decaying Model MISP	Simple decaying model for Network Intrusion Detection System (NIDS).	<pre>{   "lifetime": 120,   "decay_speed": 2,   "threshold": 30,   "default_base_score": 80,   "base_score_config": {     "estimative-language": 0.25,     "priority-level": 0.25,     "retention": 0.25,     "targeted-threat-index": 0.125,     "false-positive": 0.125   } }</pre>	Polynomial	13	1	✓	   

Page 1 of 1, showing 2 records out of 2 total, starting on record 1, ending on 2

« previous   next »

View, update, add, create, delete, enable, export, import



# IMPLEMENTATION IN MISP: FINE TUNING TOOL

**Decaying Of Indicator Fine Tuning Tool**

Attribute Type | Category | Model ID

Attribute Type	Category	Model ID
aba-rtn	Financial fraud	
authen@hash	Payload delivery	
bank-account-iv	Financial fraud	
bc	Financial fraud	
bin	Financial fraud	
bro	Network activity	10-11
bc	Financial fraud	11
cc-number	Financial fraud	
cd@hash	Payload delivery	
community-id	Network activity	
domain	Network activity	
domain@ip	Network activity	10-94
email-attachment	Payload delivery	
email-@ip	Network activity	11
email-@ic	Payload delivery	
headers	Payload delivery	
headers/authen@hash	Payload delivery	
headers/@fuzzy	Payload delivery	
headers/@ip@hash	Payload delivery	
headers/@ip@id	Payload delivery	12
headers/@ip@hash	Payload delivery	13
headers/@ip@h1	Payload delivery	13

Polynomial

Graph showing Score (0-100) vs Days (0.0-3.0). The score starts at 100 and decays exponentially towards a cutoff threshold of 30.

Parameters:

- Lifetime: 3 days
- Decay speed: 2.3
- Cutoff threshold: 30
- Expire after (lifetime): 1 days and 7 hours
- Score halved after (Half-life): 0 day and 6 hours

Adjust base score | Simulate this model

Phishing model | Simple model to rapidly decay | Rate

Parameters									
ID	Model Name	Org ID	Description	Formula	Lifetime	Decay speed	Threshold	Default basescore	Basescore config
29	Phishing model	1	Simple model to rapidly decay phishing website	Polynomial	3	2.3	30	80	estimate-language phishing 0.5

Create, modify, visualise, perform mapping

# IMPLEMENTATION IN MISP: base\_score TOOL

Search Taxonomy  x 3 not having numerical value

Default basescore 80

Taxonomies	Weight
<b>admiralty-scale</b>	
source-reliability	<input type="range" value="31"/> 31
information-credibility	<input type="range" value="30"/> 30
<b>priority-level</b>	
priority-level	<input type="range" value="53"/> 53
<b>retention</b>	
retention	<input type="range" value="0"/> 0
<b>estimative-language</b>	
likelihood-probability	<input type="range" value="0"/> 0
confidence-in-analytic-judgment	<input type="range" value="0"/> 0
<b>misp</b>	
confidence-level	<input type="range" value="0"/> 0
threat-level	<input type="range" value="0"/> 0
automation-level	<input type="range" value="0"/> 0
<b>phishing</b>	
state	<input type="range" value="0"/> 0
psychological-acceptability	<input type="range" value="0"/> 0
<b>Excluded</b>	

admiralty-scale:information-credibility (26%)

priority-level (26%)

admiralty-scale:source-reliability (27%)

Placeholder for "Organisation source confidence"

### Example [↗](#)

Attribute	Tags	Base score
Tag your attribute	<span style="background-color: black; color: white; padding: 2px;">+</span>	
Attribute 1	<span style="background-color: #28a745; color: white; padding: 2px;">admiralty-scale:information-credibility="3"</span>	0.0 <a href="#">?</a>
Attribute 2	<span style="background-color: #28a745; color: white; padding: 2px;">priority-level:baseline-minor</span> <span style="background-color: #28a745; color: white; padding: 2px;">admiralty-scale:source-reliability="d"</span> <span style="background-color: #28a745; color: white; padding: 2px;">admiralty-scale:information-credibility="2"</span>	38.2 <a href="#">?</a>
Attribute 3	<span style="background-color: #dc3545; color: white; padding: 2px;">priority-level:severe</span> <span style="background-color: #28a745; color: white; padding: 2px;">admiralty-scale:information-credibility="2"</span>	84.6 <a href="#">?</a>

### Computation steps

Tag	Computation		Result
	Eff. Ratio	Value	
<span style="background-color: #007bff; color: white; padding: 2px;">priority-level:baseline-minor</span>	0.46	* 25.00	11.62
<span style="background-color: #28a745; color: white; padding: 2px;">admiralty-scale:source-reliability="d"</span>	0.27	* 25.00	6.80

# IMPLEMENTATION IN MISP: SIMULATION TOOL

NIDS Simple Decaying Model

RestSearch [Specific ID](#)

**Attribute RestSearch®**

```
{
  "includeDecayScore": 1,
  "includeFullModel": 0,
  "score": 30,
  "includeDecayed": 0,
  "decayingModel": [8],
  "tag_id": 1,
  "tags": ["estimative-language"], "priority-levels": "interior", "timestamp": "2019-09-13"
}
```

[Search](#)

**Base score** Base score configuration not set. But default value sets.

Tag	Computation	ERT	Ratio	Value	Result
<code>resp.confidence-level="usually-confident"</code>	0	X	75.00	0	
<code>resp.confidence-level="fairly-confident"</code>	0	X	50.00	0	
<code>generally-scale:source-reliability="x"</code>	0	X	100.00	0	
<code>retention:expired</code>	0	X	NaN	0	
<code>base_score</code>					88.00

Sighting: Wed Sep 4 12:18:09 2019 | Current score: 54.60

Date	Score
Aug 4	88.00
Aug 11	~75
Aug 18	~55
Aug 25	~75
Aug 31	~55
Sep 7	~75
Sep 14	~55
Sep 21	~45
Sep 28	~55
Oct 5	~45
Oct 12	~35
Oct 19	~25
Oct 26	~15
Nov 2	~10
Nov 9	~5
Nov 16	~2
Nov 23	~1
Nov 30	~0.5
Dec 7	~0.2
Dec 14	~0.1
Dec 21	~0.05
Dec 28	~0.02
Jan 4 2020	0

← previous | next →

ID	Event #	Date	Org	Category	Type	Value	Tags	Event Tags	Galaxies	Comment	IDS	Sightings	Score
36758	45	2019-08-13	ORIGNAME	Network activity	ip-sic	7.7.7.7	<code>generally-scale:information-credibility="x"</code> <code>retention:2d</code>	<code>resp.confidence-level="usually-confident"</code> <code>resp.confidence-level="fairly-confident"</code>			✓		NIDS Simple Decaying ... 37.41
36757	45	2019-08-13	ORIGNAME	Network activity	ip-sic	8.8.8.8	<code>generally-scale:source-reliability="x"</code> <code>retention:expired</code>	<code>resp.confidence-level="usually-confident"</code> <code>resp.confidence-level="fairly-confident"</code>			✓		NIDS Simple Decaying ... 54.6

Page 1 of 1, showing 2 records out of 2 total, starting on record 1, ending on 2

← previous | next →

Simulate Attributes with different Models

/attributes/restSearch

```
1 {  
2   "includeDecayScore": 1,  
3   "includeFullModel": 0,  
4   "excludeDecayed": 0,  
5   "decayingModel": [85],  
6   "modelOverrides": {  
7     "threshold": 30  
8   }  
9   "score": 30,  
10 }  
11
```

# CREATING A NEW DECAY ALGORITHM (1)

The current architecture allows users to create their **own** formulae.

1. Create a new file `$filename` in `app/Model/DecayingModelsFormulas/`
2. Extend the Base class as defined in `DecayingModelBase`
3. Implement the two mandatory functions `computeScore` and `isDecayed` using your own formula/algorithm
4. Create a Model and set the formula field to `$filename`

Use cases:

- Add support for **more feature** (expiration taxonomy)
- **Query external services** then influence the score
- Completely **different approach** (i.e streaming algorithm)
- ...

## CREATING A NEW DECAY ALGORITHM (2)

```
1 <?php
2 include_once 'Base.php';
3
4 class Polynomial extends DecayingModelBase
5 {
6     public const DESCRIPTION = 'The description of your new
7     decaying algorithm';
8
9     public function computeScore($model, $attribute, $base_score,
10     $elapsed_time)
11     {
12         // algorithm returning a numerical score
13     }
14
15     public function isDecayed($model, $attribute, $score)
16     {
17         // algorithm returning a boolean stating
18         // if the attribute is expired or not
19     }
20 }
```

# DECAYING MODELS 2.0

- Improved support of *Sightings*
  - ▶ False positive *Sightings* should somehow reduce the score
  - ▶ Expiration *Sightings* should mark the attribute as decayed
- Potential *Model* improvements
  - ▶ Instead of resetting the score to `base_score` once a *Sighting* is set, the score should be increased additively (based on a defined coefficient); thus **prioritizing surges** rather than infrequent *Sightings*
  - ▶ Take into account related *Tags* or *Correlations* when computing score
- Increase *Taxonomy* coverage
  - ▶ Users should be able to manually override the `numerical_value` of *Tags*
- For specific type, take into account data from other services
  - ▶ Could fetch data from *BGP ranking*, *Virus Total*, *Passive X* for IP/domain/... and adapt the score