

MISP AND DECAYING OF INDICATORS

AN INDICATOR SCORING METHOD AND ONGOING IMPL-

TEAM CIRCL

INFO@CIRCL.LU

JULY 8, 2024



2024-07-08

MISP and Decaying of Indicators

MISP AND DECAYING OF INDICATORS

AN INDICATOR SCORING METHOD AND ONGOING IMPL-

TEAM CIRCL

INFO@CIRCL.LU

JULY 8, 2024



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 }
```

2024-07-08

MISP and Decaying of Indicators
└ Expiring IOCs: Why and How?

└ Indicators - Problem Statement

- **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

```
{  
  "distribution": [1, 2, 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*

2024-07-08

MISP and Decaying of Indicators

- └ Expiring IOCs: Why and How?

- └ Indicators - Problem Statement

- 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*

MISP and Decaying of Indicators

- └ Expiring IOC: Why and How?

- └ Indicators - Problem Statement

- 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

2024-07-08

MISP and Decaying of Indicators

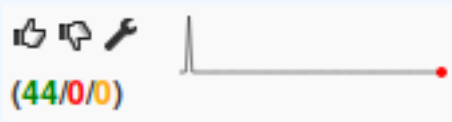
└ Expiring IOCs: Why and How?

└ 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**



2024-07-08

MISP and Decaying of Indicators

└ Expiring IOCs: Why and How?

└ *Sightings* - Refresher

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*

- **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

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-estimates	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

2024-07-08

MISP and Decaying of Indicators
└ Expiring IOCs: Why and How?

└ Taxonomies - Refresher (1)

■ 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

Id	127
Namespace	admiralty-scale
Description	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.
Version	4
Enabled	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

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

2024-07-08

MISP and Decaying of Indicators
└ Expiring IOCs: Why and How?

└ Taxonomies - Refresher (3)

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

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 ?
Deliberately deceptive	0 ?		

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

Where,

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

2024-07-08

MISP and Decaying of Indicators

└ Expiring IOCs: Why and How?

└ Scoring Indicators: Our solution

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

Where,

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

CURRENT IMPLEMENTATION IN MISP

IMPLEMENTATION IN MISP: Event/view

The screenshot shows the MISP Event/view interface. At the top, there are navigation tabs: "Photos", "Galaxy", "Event graph", "Correlation graph", "ATTACK matrix", "Attributes", and "Discussion". Below these is a "Galaxies" search box and navigation buttons for "previous" and "next". The main content area features a table of events with columns for "Date", "Org", "Category", "Type", "Value", "Tags", "Galaxies", "Comment", "Correlate", "Related Events", "Feed hits", "IDS", "Distribution", "Sightings", "Activity", "Score", and "Actions". A "Decay score" toggle button is visible in the top navigation bar. The table lists several events, each with a "NIDS Simple Decaying ..." model 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	adm_rality_scale:source-reliability="A" x retention:expired x				1 2 2 2 Show S1.1 S1.2 11 more...			Inherit	(5/0)		NIDS Simple Decaying ... 54.6 Model 5 52.69	
2019-08-13		Network activity	ip-src	9.9.9.9	adm_rality_scale:source-reliability="C" x misp:confidence-level="completely-confident" x Ipnumber x				1 3 1 9 Show S1.1 28 Show 6 more...			Inherit	(4/1)		NIDS Simple Decaying ... 37.43 Model 5 0	
2019-08-13		Network activity	ip-src	7.7.7.7	adm_rality_scale:information-credibility="4" x retention:20 x				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

2024-07-08

MISP and Decaying of Indicators

- └ Current implementation in MISP

- └ Implementation in MISP: Event/view

This is a smaller version of the screenshot shown in the main content area, illustrating the MISP Event/view interface with the 'Decay score' toggle button.

/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  [...]
```

2024-07-08

MISP and Decaying of Indicators

└ Current implementation in MISP

└ Implementation in MISP: API result

```
/attributes/restSearch  
"Attribute": [  
  {  
    "category": "Network activity",  
    "type": "ip-src",  
    "to_ids": true,  
    "timestamp": "1565703507",  
    [...]  
    "value": "8.8.8.8",  
    "decay_score": [  
      {  
        "score": 54.475223849544456,  
        "decayed": false,  
        "DecayingModel": {  
          "id": "85",  
          "name": "NIDS Simple Decaying Model"  
        }  
      }  
    ],  
    [...]  
  }  
]
```

- **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

└─ Current implementation in MISP

└─ Implementation in MISP: Playing with Models

- **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

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

When scoring indicators¹, multiple parameters² 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,

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

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

²at a variable extent as required

- 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,

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

¹Paper available: <https://arxiv.org/pdf/1803.11052>
²at a variable extent as required

SCORING INDICATORS: base_score (2)

Current implentation 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
				87.50

→ The base_score can be use to prioritize attribute based on their attached context and source

2024-07-08

MISP and Decaying of Indicators

└ Decaying Models in Depth

└ Scoring Indicators: base_score (2)

Current implentation 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
				87.50

→ 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

- 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.

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

- τ = lifetime
- δ = decay speed

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

- τ = lifetime
- δ = 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` repository³.
 - ▶ → Not editable
- **Organisation Models:** Models created by a user belonging to an organisation
 - ▶ These models can be hidden or shared to other organisation
 - ▶ → Editable

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

Multiple model types are available

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

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

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.nr	Financial fraud	
bc	Financial fraud	
bn	Financial fraud	
brn	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-att	Network activity	11
email-enc	Payload delivery	
headers	Payload delivery	
headers/authen@hash	Payload delivery	
headers@puzzry	Payload delivery	
headers@p@hash	Payload delivery	
headers@r@f	Payload delivery	12
headers@p@hash	Payload delivery	13
headers@h@L	Payload delivery	13

Polynomial

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

Adjust base score | Simulate this model

Phishing model | Simple model to rapidly decay | Edit

Parameters													
Model ID	Name	Org ID	Description	Formula	Lifetime	Decay speed	Threshold	Default basescore	Basescore config	Settings	# Types	Enabled	Action
29	Phishing model	1	Simple model to rapidly decay phishing website	Polynomial	3	2.3	30	80	estimate-language phishing	0.5	9	✓	Edit model

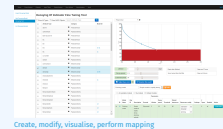
Create, modify, visualise, perform mapping

2024-07-08

MISP and Decaying of Indicators

└ Decaying Models in Depth

└ Implementation in MISP: Fine tuning tool



Create, modify, visualise, perform mapping

Search Taxonomy

Default basescore 80

3 not having numerical value

Taxonomies Weight

admiralty-scale

source-reliability

information-credibility

priority-level

priority-level

retention

retention

estimative-language

likelihood-probability

confidence-in-analytic-judgment

misp

confidence-level

threat-level

automation-level

phishing

state

psychological-acceptability

Excluded

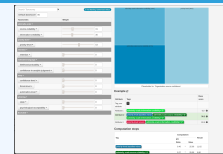
Placeholder for "Organisation source confidence"

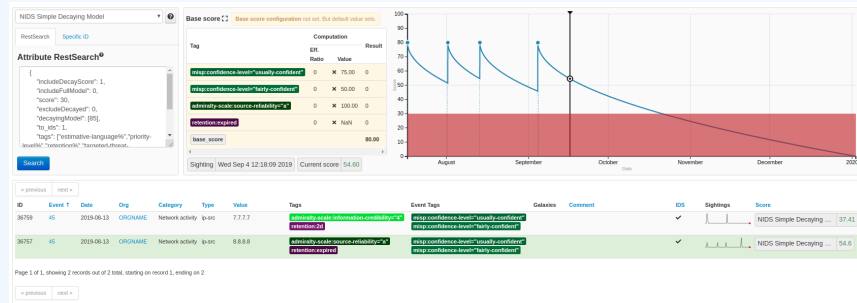
Example [🔗](#)

Attribute	Tags	Base score
Tag your attribute	+	
Attribute 1	admiralty-scale-information-credibility="5"	0.0 ?
Attribute 2	priority-level-baseline-minor admiralty-scale-source-reliability="d" admiralty-scale-information-credibility="2"	38.2 ?
Attribute 3	priority-level-severe admiralty-scale-information-credibility="2"	84.6 ?

Computation steps

Tag	Computation		Result
	Eff. Ratio	Value	
priority-level-baseline-minor	0.46	* 25.00	11.62
admiralty-scale-source-reliability="d"	0.27	* 25.00	6.80





Simulate Attributes with different Models



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
```

2024-07-08

MISP and Decaying of Indicators

└─ Decaying Models in Depth

└─ Implementation in MISP: API query body

/attributes/restSearch

```
"includeDecayScore": 1,  
"includeFullModel": 0,  
"excludeDecayed": 0,  
"decayingModel": [85],  
"modelOverrides": {  
  "threshold": 30  
}  
"score": 30,
```

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)
- ...

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 }
```

```
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 }
```

- 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

- 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