

MISP AND DECAYING OF INDICATORS

PRIMER FOR INDICATOR SCORING IN MISP

TEAM CIRCL

INFO@CIRCL.LU

AUGUST 5, 2022



2022-08-05

MISP and Decaying of Indicators

MISP AND DECAYING OF INDICATORS

PRIMER FOR INDICATOR SCORING IN MISP

TEAM CIRCL

INFO@CIRCL.LU

AUGUST 5, 2022



- Present the components used in MISP to expire IOCs
- Present the current state of Indicators life-cycle management in MISP

└ Outline of the presentation

- Present the components used in MISP to expire IOCs
- Present the current state of Indicators life-cycle management in MISP

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 }
```

2022-08-05

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

└ Indicators lifecycle - 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 **relevance** issues
 - ▶ Each user/organisation have **different use-cases** and interests
 - Conflicting interests: Operational security VS attribution
- Can be partially solved with *Taxonomies*

- Various users and organisations can share data via MISP, multiple parties can be involved
 - ▶ **Trust, data quality** and **relevance** issues
 - ▶ Each user/organisation have **different use-cases** and interests
 - Conflicting interests: Operational security VS attribution
- Can be partially solved with *Taxonomies*
- Attributes can be shared in large quantities (more than 12M on MISPPRIV - Sept. 2020)
 - ▶ Partial info about their **freshness** (*Sightings*)
 - ▶ Partial info about their **validity** (*last_seen*)
- Can be partially solved with our *Data model*

MISP's *Decaying model* combines the two

MISP and Decaying of Indicators

- └ Expiring IOCs: Why and How?

- └ Indicators lifecycle - Problem Statement

- Various users and organisations can share data via MISP, multiple parties can be involved
 - ▶ **Trust, data quality** and **relevance** issues
 - ▶ Each user/organisation have **different use-cases** and interests
 - Conflicting interests: Operational security VS attribution
 - Can be partially solved with *Taxonomies*
 - Attributes can be shared in large quantities (more than 12M on MISPPRIV - Sept. 2020)
 - ▶ Partial info about their **freshness** (*Sightings*)
 - ▶ Partial info about their **validity** (*last_seen*)
 - Can be partially solved with our *Data model*
- MISP's Decaying model combines the two

REQUIREMENTS TO ENJOY THE DECAYING FEATURE IN MISP

- Starting from **MISP 2.4.116**, the decaying feature is available
- **Update** decay models and **enable** some
- MISP Decaying strongly relies on *Taxonomies* and *Sightings*, don't forget to review their configuration

Note: The decaying feature has no impact on the information stored in MISP, it's just an **overlay** to be used in the user-interface and API

MISP and Decaying of Indicators

└ Expiring IOCs: Why and How?

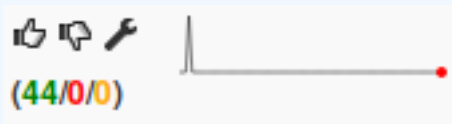
└ Requirements to enjoy the decaying feature in MISP

- Starting from **MISP 2.4.116**, the decaying feature is available
- **Update** decay models and **enable** some
- MISP Decaying strongly relies on *Taxonomies* and *Sightings*, don't forget to review their configuration

Note: The decaying feature has no impact on the information stored in MISP, it's just an **overlay** to be used in the user-interface and API

Sightings add a **temporal context** to indicators.

- *Sightings* can be used to represent that you saw the IoC
- **Usecase:** Continuous feedback loop MISP ↔ IDS



Sightings add a **temporal context** to indicators.

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

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., Boukhtouta, 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	- 🔍 🗑️

- *Taxonomies* are a simple way to attach a classification to an *Event* or an *Attribute*
- Classification must be globally used to be efficient (or agreed on beforehand)



- Taxonomies are a simple way to attach a classification to an Event or an Attribute
- Classification must be globally used to be efficient (or agreed on beforehand)

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

2022-08-05

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

└ Taxonomies - Refresher (2)

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 a `numerical_value`
- Allows concepts to be used in an mathematical expression
 - Can be used to prioritise IoCs

admiralty-scale taxonomy¹

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

¹<https://github.com/MISP/misp-taxonomies/blob/master/admiralty-scale/machinetag.json>

- Some taxonomies have a `numerical_value`
- Allows concepts to be used in an mathematical expression
 - Can be used to prioritise IOCs

admiralty-scale taxonomy¹

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		

¹<https://github.com/MISP/misp-taxonomies/blob/master/admiralty-scale/machinetag.json>

admiralty-scale taxonomy²

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 ?

→ Users can override tag numerical_value

²<https://github.com/MISP/misp-taxonomies/blob/master/admiralty-scale/machinetag.json>

admiralty-scale taxonomy ²		admiralty-scale taxonomy ²	
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 ?		

→ Users can override tag numerical_value

²<https://github.com/MISP/misp-taxonomies/blob/master/admiralty-scale/machinetag.json>

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

■ $\text{base_score}(\text{Attribute}, \text{Model})$

- ▶ Initial score of the *Attribute* only considering the context (*Attribute's type, Tags*)

■ $\text{decay}(\text{Model}, \text{time})$

- ▶ Function composed of the **lifetime** and **decay speed**
- ▶ Decreases the base_score over time

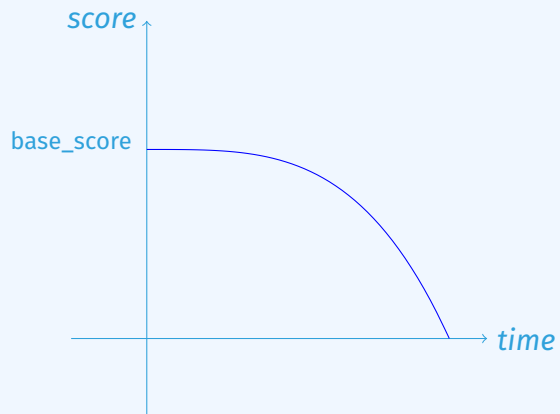
└ Expiring IOCs: Why and How?

└ Scoring Indicators: Our solution

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

- $\text{base_score}(\text{Attribute}, \text{Model})$
 - ▶ Initial score of the *Attribute* only considering the context (*Attribute's type, Tags*)
- $\text{decay}(\text{Model}, \text{time})$
 - ▶ Function composed of the **lifetime** and **decay speed**
 - ▶ Decreases the base_score over time

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



- └ Expiring IOCs: Why and How?

- └ Scoring Indicators: Our solution

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



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", "next", and "view all". The main content area features a toolbar with "Scope toggle", "Deleted", "Decay score", "Context", "Related Tags", and "Filtering tool (1)". A search bar is also present. The table below lists events with 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" column shows values like 65.26, 54.6, 37.43, 37.41, and 23.31. A "Decay score toggle button" is visible in the top right of the table area.

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-svc	5.5.5.5									Inherit		NIDS Simple Decaying ... 65.26 Model 5 79.88	
2019-08-13		Network activity	ip-svc	8.8.8.8	adm:admiralty-scale:source-reliability="A" x retention:expired x				1 2 2 2 Show S1.1 11 S1.2 more...				Inherit		NIDS Simple Decaying ... 54.6 Model 5 52.69	
2019-08-13		Network activity	ip-svc	9.9.9.9	adm:admiralty-scale:source-reliability="C" x misp:confidence-level="completely-confident" x ip:remember x				1 3 1 9 Show S1.1 28 S1.1 more...				Inherit		NIDS Simple Decaying ... 37.43 Model 5 0	
2019-08-13		Network activity	ip-svc	7.7.7.7	adm:admiralty-scale:information-credibility="4" x retention:20 x				41				Inherit		NIDS Simple Decaying ... 37.41 Model 5 0	
2019-07-18		Network activity	ip-svc	6.6.6.6					41				Inherit		NIDS Simple Decaying ... 23.31 Model 5 0	

■ Decay score toggle button

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

2022-08-05

MISP and Decaying of Indicators

- └ Current implementation in MISP

- └ Implementation in MISP: Event/view

The thumbnail shows a similar view to the main screenshot, but with a "Decay score toggle button" highlighted in blue. Below the button, a tooltip reads: "Shows Score for each Models associated to the Attribute type".

/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  [...]
```

2022-08-05

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: Objectives

- 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

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

Models are an instantiation of the formula with configurable parameters:

- Parameters: `lifetime`, `decay_rate`, `threshold`
- `base_score` computation
- `default base_score`
- associate *Attribute* types
- formula
- creator organisation

└ Current implementation in MISP

└ Implementation in MISP: Models definition

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

Models are an instantiation of the formula with configurable parameters:

- Parameters: `lifetime`, `decay_rate`, `threshold`
- `base_score` computation
- `default base_score`
- associate *Attribute* types
- formula
- creator organisation

Two types of model are available

- **Default Models:** Created and shared by the community.
Coming from `misp-decaying-models` repository³.
→ Not editable
- **Organisation Models:** Created by a user on MISP
 - ▶ Can be hidden or shared to other organisation
 - Editable

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

└─ Current implementation in MISP

└─ Implementation in MISP: Models Types

- Two types of model are available
- **Default Models:** Created and shared by the community.
Coming from `misp-decaying-models` repository.
→ Not editable
 - **Organisation Models:** Created by a user on MISP
 - ▶ Can be hidden or shared to other organisation
 - Editable

IMPLEMENTATION IN MISP: INDEX

Decaying Models

« previous next »

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 MSP	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 »

Standard CRUD operations: View, update, add, create, delete, enable, export, import

2022-08-05

MISP and Decaying of Indicators
└─ Current implementation in MISP

└─ Implementation in MISP: Index



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	
authn-hash	Payload delivery	
bank-account-iv	Financial fraud	
bc	Financial fraud	
bn	Financial fraud	
br	Network activity	10 11
bc	Financial fraud	11
cc-number	Financial fraud	
cd-hash	Payload delivery	
community-id	Network activity	
domain	Network activity	
domainip	Network activity	10 94
email-attachment	Payload delivery	
email-otp	Network activity	11
email-otp	Payload delivery	
headers	Payload delivery	
headers/authn-hash	Payload delivery	
headers/otp-fuzzy	Payload delivery	
headers/otp-hash	Payload delivery	
headers/otp-id	Payload delivery	12
headers/otp-hash	Payload delivery	13
headers/otp-hl	Payload delivery	13

Polynomial

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

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

Configure models: Create, modify, visualise, perform mapping

2022-08-05

MISP and Decaying of Indicators
└ Current implementation in MISP

└ Implementation in MISP: Fine tuning tool



Configure models: Create, modify, visualise, perform mapping

IMPLEMENTATION IN MISP: base_score TOOL

Search Taxonomy x 3 not having numerical value

Default basescore 80

Taxonomies Weight

admiralty-scale *

source-reliability 31

information-credibility 30

priority-level *

priority-level 53

retention *

retention 0

estimative-language *

likelihood-probability 0

confidence-in-analytic-judgment 0

misp *

confidence-level 0

threat-level 0

automation-level 0

phishing *

state 0

psychological-acceptability 0

Excluded *

Placeholder for "Organisation source confidence"

Example [🔗](#)

Attribute	Tags	Base score
Tag your attribute	<input type="button" value="+"/>	
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

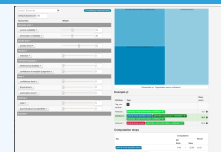
Tag	Computation		Result
	Eff. Ratio	Value	
priority-level:baseline-minor	0.46	* 25.00	11.62
admiralty-scale:source-reliability="d"	0.27	* 25.00	6.80

2022-08-05

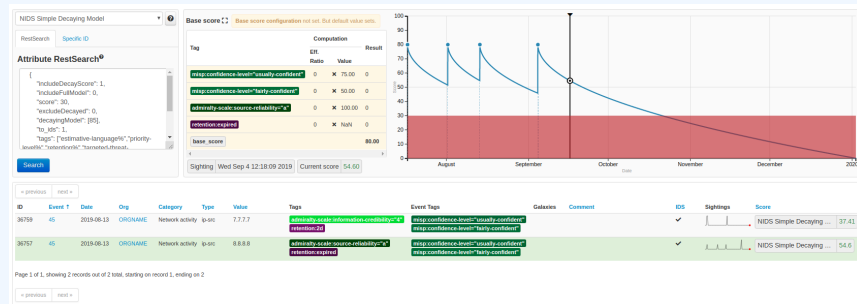
MISP and Decaying of Indicators

└ Current implementation in MISP

└ Implementation in MISP: base_score tool



IMPLEMENTATION IN MISP: SIMULATION TOOL



Simulate decay on *Attributes* with different *Models*

2022-08-05

MISP and Decaying of Indicators

└ Current implementation in MISP

└ Implementation in MISP: simulation tool



Simulate decay on 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
```

2022-08-05

MISP and Decaying of Indicators

└ Current implementation in MISP

└ Implementation in MISP: API query body

/attributes/restSearch

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

```
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 }
```

└ Current implementation in MISP

└ Creating a new decay algorithm

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

2022-08-05

- MISP and Decaying of Indicators
 - └ Current implementation in MISP
 - └ 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*