

MISP AND DECAYING OF INDICATORS

AN INDICATOR SCORING METHOD AND ONGOING IMPLE-

TEAM CIRCL

INFO@CIRCL.LU

SEPTEMBER 13, 2022



2022-09-13

MISP and Decaying of Indicators

MISP AND DECAYING OF INDICATORS

AN INDICATOR SCORING METHOD AND ONGOING IMPLE-

TEAM CIRCL

INFO@CIRCL.LU

SEPTEMBER 13, 2022



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 }
```

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*

2022-09-13

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

- 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

2022-09-13

MISP and Decaying of Indicators

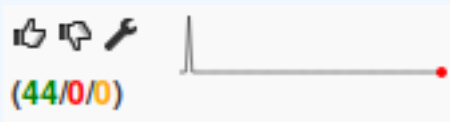
└ Expiring IOCs: Why and How?

└ 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**



2022-09-13

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*

2022-09-13

MISP and Decaying of Indicators

└ Expiring IOCs: Why and How?

└ 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
- 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-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., Boukhouta, 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

2022-09-13

MISP and Decaying of Indicators

Expiring IOC: Why and How?

Taxonomies - Refresher (1)

Taxonomies						
Id	Namespace	Description	Version	Enabled	Required	Active Tags
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., Boukhouta, 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

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 »

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

2022-09-13

MISP and Decaying of Indicators

└ Expiring IOCs: Why and How?

└ Taxonomies - Refresher (2)

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)											
Author	N/A													

No	Expanded	Numerical value	Events	Attributes	Tags	Action			
1	admiralty-scale:information-credibility="1"	Information Credibility: Confirmed by other sources	100	6	0	admiralty-scale:information-credibility="1"	⏏	⚙	-
2	admiralty-scale:information-credibility="2"	Information Credibility: Probably true	75	21	1	admiralty-scale:information-credibility="2"	⏏	⚙	-
3	admiralty-scale:information-credibility="3"	Information Credibility: Possibly true	50	16	5	admiralty-scale:information-credibility="3"	⏏	⚙	-
4	admiralty-scale:information-credibility="4"	Information Credibility: Doubtful	25	2	0	admiralty-scale:information-credibility="4"	⏏	⚙	-
5	admiralty-scale:information-credibility="5"	Information Credibility: Improbable	0	1	0	admiralty-scale:information-credibility="5"	⏏	⚙	-
6	admiralty-scale:information-credibility="6"	Information Credibility: Truth cannot be judged	50	9	2	admiralty-scale:information-credibility="6"	⏏	⚙	-
7	admiralty-scale:source-reliability="a"	Source Reliability: Completely reliable	100	1	0	admiralty-scale:source-reliability="a"	⏏	⚙	-
8	admiralty-scale:source-reliability="b"	Source Reliability: Usually reliable	75	21	76	admiralty-scale:source-reliability="b"	⏏	⚙	-
9	admiralty-scale:source-reliability="c"	Source Reliability: Fairly reliable	50	9	8	admiralty-scale:source-reliability="c"	⏏	⚙	-
10	admiralty-scale:source-reliability="d"	Source Reliability: Not usually reliable	25	2	0	admiralty-scale:source-reliability="d"	⏏	⚙	-
11	admiralty-scale:source-reliability="e"	Source Reliability: Unreliable	0	0	0	admiralty-scale:source-reliability="e"	⏏	⚙	-
12	admiralty-scale:source-reliability="f"	Source Reliability: Reliability cannot be judged	50	10	7	admiralty-scale:source-reliability="f"	⏏	⚙	-
13	admiralty-scale:source-reliability="g"	Source Reliability: Deliberately deceptive	0	N/A	N/A				+

→ Cherry-pick allowed Tags

→ 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 ?

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

- $\text{score} \in [0, +\infty]$
- $\text{base_score} \in [0, 100]$
- 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 tabs for 'Plots', 'Galaxy', 'Event graph', 'Correlation graph', 'ATTACK matrix', 'Attributes', and 'Discussion'. Below these is a 'Galaxies' search bar. The main table displays a list 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. The 'Decay score' toggle button is visible in the top right of the table. The table contains several rows of events, each with a 'NIDS Simple Decaying ...' model and a 'Model 5' score.

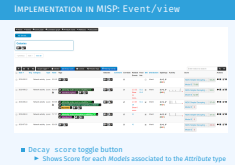
Date	Org	Category	Type	Value	Tags	Galaxies	Comment	Correlate	Related Events	Feed hits	IDS Distribution	Sightings	Activity	Score	Actions
2019-09-12		Network activity	ip-src	5.5.5.5										65.26	
2019-08-13		Network activity	ip-src	8.8.8.8										54.6	
2019-08-13		Network activity	ip-src	9.9.9.9										37.43	
2019-08-13		Network activity	ip-src	7.7.7.7										37.41	
2019-07-18		Network activity	ip-src	6.6.6.6										23.31	

- Decay score toggle button
 - Shows Score for each Models associated to the Attribute type

2022-09-13

MISP and Decaying of Indicators
└ Current implementation in MISP

└ Implementation in MISP: Event/view



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    [...]
```

MISP and Decaying of Indicators

- Current implementation in MISP

- Implementation in MISP: API result

2022-09-13

```
/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

2022-09-13

MISP and Decaying of Indicators

└ 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

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 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

MISP and Decaying of Indicators

└ Decaying Models in Depth

└ Scoring Indicators: base_score (1)

SCORING INDICATORS: base_score (1)

```
score(attribute) = base_score(attribute, model) * decay(model, 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

SCORING INDICATORS: base_score (2)

Current implentation ignores source_confidence:

→ $\text{base_score} = \text{tags}$

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

MISP and Decaying of Indicators

└ Decaying Models in Depth

└ Scoring Indicators: base_score (2)

Current implementation ignores source_confidence:

→ $\text{base_score} = \text{tags}$

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

SCORING INDICATORS: PUTTING IT ALL TOGETHER

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

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

- τ = lifetime
- δ = decay speed

MISP and Decaying of Indicators

└ Decaying Models in Depth

└ Scoring Indicators: putting it all together

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

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

- τ = lifetime
- δ = decay speed

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

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>

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.	{ "lifetime": 3, "decay_speed": 2.3, "threshold": 30, "default_base_score": 80, "base_score_config": { "estimative-language": 0.5, "phishing": 0.5 } }	Polynomial	9	1	✓	   
85	1	✗	NIDS Simple Decaying Model MISP	Simple decaying model for Network Intrusion Detection System (NIDS).	{ "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 } }	Polynomial	13	1	✓	   

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

« previous next »

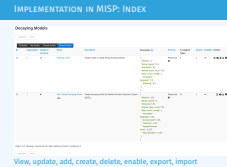
View, update, add, create, delete, enable, export, import

2022-09-13

MISP and Decaying of Indicators

Decaying Models in Depth

Implementation in MISP: Index



IMPLEMENTATION IN MISP: base_score TOOL

Search Taxonomy 3 not having numerical value

Default basescore 80

Taxonomies

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	

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

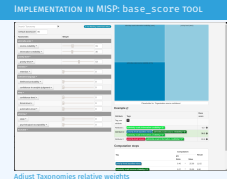
Tag	Eff. Ratio	Value	Result
priority-level:baseline-minor	0.46	25.00	11.62
admiralty-scale:source-reliability="d"	0.27	25.00	6.80

2022-09-13

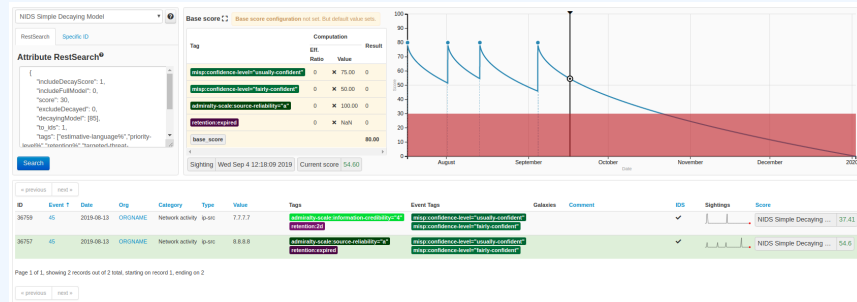
MISP and Decaying of Indicators

Decaying Models in Depth

Implementation in MISP: base_score tool



IMPLEMENTATION IN MISP: SIMULATION TOOL



Simulate *Attributes* with different *Models*

2022-09-13

MISP and Decaying of Indicators

└ Decaying Models in Depth

└ Implementation in MISP: simulation tool



/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
```

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

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 }
```

MISP and Decaying of Indicators

└─Decaying Models in Depth

└─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 }
```

- 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

2022-09-13

MISP and Decaying of Indicators

└─ Decaying Models in Depth

└─ 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