# **MISP AND DECAYING OF INDICATORS**

AN INDICATOR SCORING METHOD AND ONGOING IMPLE-

**TEAM CIRCL** 

INFO@CIRCL.LU

AUGUST 5, 2022



မှု MISP and Decaying of Indicators



2022

MISP and Decaying of Indicators

**EXPIRING IOCS: WHY AND HOW?** 

# **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



MISP and Decaying of Indicators

Indicators - Problem Statement

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	
	17	
2014	43	- [[
2015	82	distribution": [1, 2, 3]
2016	105	2
2017	118	
2018	125	
2019-10	135	

## **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)
- $\rightarrow$  Can be partially solved with Taxonomies

MISP and Decaying of Indicators

└─Indicators - Problem Statement

 Various users and organisations can share data via MISP, multiple parties can be involved
 + Trust, data quality and time-to-live iscoss
 + Each use/organisation har different use-cases and interests
 Conficting interests uch as operational security, attribution,...

-> Can be partially solved with Toxonomies

## **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)
- $\rightarrow$  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)
  - $\rightarrow$  Can be partially solved with our Decaying model

MISP and Decaying of Indicators

LINDICATORS - Problem Statement

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)
- $\rightarrow$  Can be partially solved with Taxonomies

Attributes can be shared in large quantities (more than 7.3 million on MTSPPRTV)

- Partial info about their freshness (Sighting)
- Partial info about their validity (last update)
- $\rightarrow$  Can be partially solved with our Decaying model

# REQUIREMENTS TO ENJOY THE DECAYING FEATURE IN MISP

MISP and Decaying of Indicators

Requirements to enjoy the decaying feature in MISP 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
  oner year way
- 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 Toxonomies and Sightings, don't forget to review their configuration

- 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 - 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

i⊕ i⊋ ≯ (44/<mark>0</mark>/0) MISP and Decaying of Indicators

└─*Sightings* - Refresher



# 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
  - $\rightarrow$  Achieved thanks to Taxonomies

MISP and Decaying of Indicators

Organisations opt-in - setting a level of confidence DRGANISATIONS OPT-IN - SETTING A LEVEL OF CONFIDENCE

MLSP is a peer-to-peer system, information passes through multiple instances. **e** Producers can add context (such as tags from Taxonomics, Goloxies) about their asserted confidence or the reliability of the data

Consumers can have different levels of trust in the producers and/or analysts themselves

s might have other contextual needs

# **TAXONOMIES - REFRESHER (1)**

<pre>Taxc</pre>	aus 1 2 next -						
ld †	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		27 / 26 (enable all)	- @ 🕯
180	vocabulaire-des-probabilites-estimatives	Ce vocabulaire attribue des valeurs en pourcentage à certains énoncés de probabilité	2	Yes		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. & Doebbabi, M. (2016) in Detecting Internet Abuse by Analyzing Passive DNS Traffic: A Survey of Implemented Systems. IEEE Communications Surveys & Tutorials, 1–1. doi:10.1108/comst2018.2849614	1	No		0/18	+@
178	targeted-threat-index	The Targeled 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 taik."RATAstrophe: Monitoring a Malware Menagerie" along with Katie Kleemola and Greg Wiseman.	2	Yes		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

MISP and Decaying of Indicators

└─Taxonomies - Refresher (1)

Tak	ceamles						
	And and a second se	Rectant.	-	-	-	100.00	-
٠	against the second s	Notice again large process and a cost of the second strategy as a state of addition of the second strategy of the					
	1001000	A constant classes of inclusion dataset where the DM as incursion from 1. Incoments, et. Ann. J., and annual A. (2014) - based spreamer description of the strength of the DM and the property of the strength of the DM and the property of the strength of the DM and the property of the strength of the DM and the property of the strength of the DM and the property of the strength of the DM and the property of the strength of the DM and the property of the strength of the DM and the property of the strength of the DM and the property of the property of the strength of the DM and the property of the property of the property of the strength of the DM and the property of the property of the property of the strength of the property o					••
	hepter limit in the	The Pagel of The Education and the analysis of the Control of the comparison of the Control of the Control of the Control of the education of the Control of the Control of the Control of the education of the Control of the Control of the Control of the impact of the Control of the Control of the Control of the education of the Control of the Control of the Control of the Control of the Control of the Control of the Control of the Control of the Control of the					

Classification must be globally used to be efficient

# TAXONOMIES - REFRESHER (2)

#### ADMIRALTY-SCALE Taxonomy Library

	127							
amespace	admiralty-scale							
escription		or Ranking (also called the NATO System) is used to ran	k the reliability of a sou	urce and th	ne credibility	of an information. Reference based on FM 2	-22.3 (FI	M 34-52
		NCE COLLECTOR OPERATIONS and NATO documents						
ersion nabled	4 Yes (disable)							
« previous next »								
						Filter		
Тад		Expanded	Numerical value	Events	Attributes	Tags		Action
admiralty-scale:info	rmation-credibility="1"	Information Credibility: Confirmed by other sources	100	6	0	admiralty-scale:information-credibility=	<u> </u>	<b>c</b> -
admiralty-scale:info	rmation-credibility="2"	Information Credibility: Probably true	75	21	1	admiralty-scale:Information-credibility=	"2" <b>&lt;</b>	<b>g</b> -
admiralty-scale:info	rmation-credibility="3"	Information Credibility: Possibly true	50	16	5	admiralty-scale:information-credibility=	"3" <b>&lt;</b>	<b>g</b> -
admiralty-scale:info	rmation-credibility="4"	Information Credibility: Doubtful	25	2	0	admiralty-scale:information-credibility=	"4" <	<b>g</b> -
admiralty-scale:info	rmation-credibility="5"	Information Credibility: Improbable	0	1	0	admiralty-scale:Information-credibility:	"5" <	g -
admiralty-scale:info	rmation-credibility="6"	Information Credibility: Truth cannot be judged	50	9	2	admiralty-scale:information-credibility=	<sup>6</sup> <	ø-
admiralty-scale:sou	rce-reliability="a"	Source Reliability: Completely reliable	100	1	0	admiralty-scale:source-reliability="a"	<	<b>с</b> -
admiralty-scale:sou	rce-reliability="b"	Source Reliability: Usually reliable	75	21	76	admiralty-scale:source-reliability="b"	<	<b>с-</b>
admiralty-scale:sou	rce-reliability="c"	Source Reliability: Fairly reliable	50	9	8	admiralty-scale:source-reliability="c"	<	ຊ-
admiralty-scale:sou	rce-reliability="d"	Source Reliability: Not usually reliable	25	2	0	admiralty-scale:source-reliability="d"	<	ຊ-
	rce-reliability="e"	Source Reliability: Unreliable	0	0	0	admiralty-scale:source-reliability="e"	<	<b>e</b> -
admiralty-scale:sou								
admiralty-scale:sou admiralty-scale:sou		Source Reliability: Reliability cannot be judged	50	10	7	admiralty-scale:source-reliability="f"	<	<b>с</b> -

#### $\rightarrow$ Cherry-pick allowed *Tags*

└─Taxonomies - Refresher (2)

ADMIRAL	TY-SCALE 1	axonomy Library					
	10						
And and a second second							
Board of Concession, Name							
						_	
0 🐜 👘		beener .	London House	-	****	*	
			-9				
						*****	

# TAXONOMIES - REFRESHER (3)

MISP and Decaying of Indicators

└─Taxonomies - Refresher (3)

TAXONOMIES - REFRESHER	
TAXONOMIES - KERKESHER	

Some taxonomies have numerical\_value  $\rightarrow$  Can be used to prioritise Attributes

Description	Value	Description	Value
	100	Confirmed by other sources	100
Isually reliable	75	Probably true	75
airly reliable	50	Possibly true	50
tot usually reliable	25	Doubtful	25
Inveliable	0	Improbable	0
teliability cannot be judged	507	Truth cannot be judited	507
eliberatly deceptive	07		-

#### Some taxonomies have numerical\_value

 $\rightarrow$  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 <b>?</b>	Truth cannot be judged	50 ?
Deliberatly deceptive	0?		

## SCORING INDICATORS: OUR SOLUTION

MISP and Decaying of Indicators

└─Scoring Indicators: Our solution

SCORING INDICATORS: OUR SOLUTION

ore(minimum) = base\_score(minimum, mont) • decay(mont, mont

Where,

- $\blacksquare \ score \in [0,+\infty$
- base\_score ∈ [0, 100]
   decay is a function defined by model's parameter
  - decay is a function defined by model's paramete controlling decay speed
- Attribute Contains Attribute's values and metadat
- Model Contains the Model's configuration

Score(Attribute) = base\_score(Attribute, Model) • decay(Model, time)

Where,

- $\blacksquare$  score  $\in$  [0,  $+\infty$
- **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

2022

MISP and Decaying of Indicators

CURRENT IMPLEMENTATION IN

# CURRENT IMPLEMENTATION IN MISP

# IMPLEMENTATION IN MISP: Event/view

	alaxie															
« p	previous	nexto	view all													
•	+ =		Scope tog			ed 🗠 Decay score 🛛 Context 🧐 Related Tag:									Enter value to search	Q ×
9	Date 1	Org	Category	Туре	Value	Tags	Galaxies	Comment	Correlate	Related Fee Events hits		Distribution	Sightings	Activity	Score	Actions
3	2019-09	-12	Network activity	ip-src	5.5.5.5	G + ± +	<b>3</b> + <b>2</b> +		8			Inherit	ić © ∦ (000)		NIDS Simple Decaying 65.26 Model 5 79.88	• • •
	2019-08	-13	Network activity	ip-src	8.8.8.8	Image: Contract of the state of the sta	<b>(3 + 2 +</b>	1	×	1222 S1: Show S1: 11 more		Inherit	i⇔ © ≯ (5/0/0)	LLL.	NIDS Simple Decaying 54.6 Model 5 52.69	• • •
	2019-08	-13	Network activity	ip-src	9.9.9.9 A	Image: admirally-scale:source-reliability::"c" x         Image: admirally-scale:source-reliability: admirally-	(8 + 🛓 +		×	1 3 19 S1: 28 Show 6 more	8	Inherit	心 心 产 (4/10)	ML.I	NIDS Simple Decaying 37.43 Model 5 0	• 1 2
)	2019-08	-13	Network activity	ip-src	7.7.7.7	admiralty-scale:information-credibility="4" x       retention:2d x       () +	<b>8</b> + <b>±</b> +	l	8	41	8	Inherit	たやチ (31010)		NIDS Simple Decaying 37.41 Model 5 0	• • •
3	2019-07	-18	Network activity	ip-src	6.6.6.6	(ð÷]≛÷	🕃 + 불 +	1		41	ø	Inherit	69≯ (0000)		NIDS Simple Decaying 23.31	

Decay score toggle button

Shows Score for each *Models* associated to the *Attribute* type

MISP and Decaying of Indicators

Implementation in MISP: Event/view

-									
				-	1.00		-	-	-
	inter state of		1919	1919		-	217		 •••
			Sector Sector	12/19			227		•••
		17							
			Second Second				-		

Decay score toggle button
 Shows Score for each Model's associated to the Attribute type

## **IMPLEMENTATION IN MISP: API RESULT**

#### /attributes/restSearch

10

11

12

13

14

```
"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"
```

MISP and Decaying of Indicators 05 -Current implementation in MISP

8

2022

-Implementation in MISP: API result



### IMPLEMENTATION IN MISP: PLAYING WITH MODELS

MISP and Decaying of Indicators

2022-

LImplementation in MISP: Playing with Models

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

#### 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

MISP and Decaying of Indicators

**DECAYING MODELS IN DEPTH** 

# **DECAYING MODELS IN DEPTH**

# Scoring Indicators: base\_score (1)

SCOTe(Attribute) = base\_score(Attribute, Model) • decay(Model, 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

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

Where,

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

MISP and Decaying of Indicators

2022

└─Scoring Indicators: base\_score (1)

SCORING INDICATORS: base\_score (1)

ore(minute) = base\_score(minute, most) + decay(mint, most)

When scoring indicators', multiple parameters' 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

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

mere,

<sup>1</sup>Paper available: https://arxiv.org/pdf/1803.11052 <sup>3</sup>at a variable extent as required

<sup>&</sup>lt;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 implentation ignores source\_confidence:

#### $\rightarrow$ base\_score = tags

	Comp			
Tag	Eff. Ratio	numerical_valu		Result
admiralty-scale:source-reliability="Completely reliable"	0.50	*	100.00	50.00
phishing:psychological-acceptability="high"	0.50	*	75.00	37.50
				87.50

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

MISP and Decaying of Indicators

└─Scoring Indicators: base\_score (2)

SCORING INDICATORS: Dase_score (2)
Current implentation ignores source_confidence:
a base and a base

	Comp	-		
54	an. Paste		namerical, salar	Resalt
administly scale savata reliability:"Campiblely reliable"	6.90		300.80	90.80
phishing psychological-acceptability-"high"	6.50		75.00	07.50
		-		12.00

The base\_score can be use to prioritize attribute based or heir attached context and source

# SCORING INDICATORS: DECAY SPEED (1)

MISP and Decaying of Indicators

└─Scoring Indicators: decay speed (1)

SCORING INDICATORS: DECAY SPEED (1)

core(strainer) = base\_score(strainer, model) • decay(model, time)

- The decay is calculated usin
- The lifetime of the indicator
  May your depending on the indic
- 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 sco over time
- The time elapsed since the latest update or sighting

 $\texttt{score}(\texttt{Attribute}) = \texttt{base}\_\texttt{score}(\texttt{Attribute, Model}) \bullet \texttt{decay}(\texttt{Model, time})$ 

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

3

#### SCORING INDICATORS: PUTTING IT ALL TOGHETHER

MISP and Decaying of Indicators

2022

Scoring Indicators: putting it all toghether

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

 $score = base\_score \cdot \left(1 - \left(\frac{t}{\tau}\right)^{\frac{1}{2}}\right)$ 

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

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

•  $\tau = \text{lifetime}$ •  $\delta = \text{decay speed}$ 

#### **IMPLEMENTATION IN MISP: MODELS DEFINITION**

MISP and Decaying of Indicators

2022-

Implementation in MISP: Models definition

 $f^{*}$  are an instanciation of the formula where elements can denote

- B Parameters:lifetime, decay\_rate, threshold base\_score default base score
- formula
   associate Attribute types

creator organisation

 $ightarrow score = base\_score \cdot \left(1 - \left(\frac{t}{\tau}\right)^{\frac{1}{\delta}}\right)$ Models are an instanciation of the formula where elements can be defined:

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

MISP and Decaying of Indicators

2022

└─Implementation in MISP: Models Types

Aultiple model types are available ■ Default Models: Models created and shared by the community. Available from misp-decaying-models repository5. ► a Not offable

- 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

Multiple model types are available

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

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

## IMPLEMENTATION IN MISP: INDEX

#### **Decaying Models**

« previous next »

D	Organization	Usable to everyone	Name	Description	Parameters { }	Formula	# Assigned Types	Version	Enabled	Actions
29	1	~	Phishing model	Simple model to rapidly decay photning website.	{     "iffetime": 3,     "idecay, speed": 2.3,     "threshold": 30,     "default_base_score": 80,     "base_score_config": {         language": 0.5,         "phishing": 0.5     }     } }	Polynomial	9	1	~	<b>■ &amp; ê</b> ¢ <b>H</b>
85	1	×	NDS Simple Decaying Model	Single decaying model for Network Intrusion Detection System (NIDS).	{     "lifetime": 120,     "decay, speed": 2,     "threshold": 30,     "default, base, score, score, so,     "base, score, score, so,     "base, score, score, so,     "priority-tevel": 0.25,     "frietention": 0.25,     "targeted-threat- indect": 0.125,     "talse-positive": 0.125     } }	Polynomial	13	1	~	<b>■</b> & ⊘ <b>■</b>
age 1 of « previo		rds out of 2 total,	, starting on record 1, ending on 2							

MISP and Decaying of Indicator

2022

└─Implementation in MISP: Index

Design of the second se		Name of Street o		-
				-
	NAMES OF TAXABLE		1000	
		And a second sec		
			•	

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

#### IMPLEMENTATION IN MISP: FINE TUNING TOOL

	Dec	aying Of Indicator F	ine	runing roor																	
del	0 Sho	w All Types 🔋 Show MISP Objects	Searc	h Attribute Type	<b>1</b>			Polynor	тазі		т 0										
		Attribute Type		Category	Model ID	1	1	100	1												
dels		aba m	-	Financial traud		_		50	4												
		authenthush		Payload delivery				80													
		bank-account-nr		Financial tread				70													
		bic		Financial tread				50			$\checkmark$										
		bin		Financial traud				g 50 40				<									
		bro		Network activity	10 11			20					-								
		bic		Financial Insud	11		1	20													
	0	cc-number	-	Financial Insud				10	-												
	0	othash	-	Payload delivery				•			0.5	1.0		1.5		2.0	2.5				
	0	community-id	-	Network activity							0.5	10		Days		2.0	2.5				
	8	domain		Network activity			L I	Lifes	time 3		-8			- days	Expir	e aher ölfetime	1	10	us and 7 h	ours	
	8	domainijo	-	Network activity	10 84		1	Decay	speed 2	13					Scon	r halved after (f	Half-Me)	0.0	ty and 6 ho	202	
	8	enal-atachment	-	Payload delivery			1.	Current th	meshold 3	0											
	8	enal-óz		Network activity	н		1.2		test base sco	_	1 Landard	alate this mos	-								
		email.src	*	Payload delivery			13	(JAG)		e											
		fiename	*	Payload delivery				Phishing	g model		Sir	nple model 6	o rapidly d	юсау 📩	C Edit						
		Benamejauthenthash	-	Payload delivery				0 AI	available n	iodels	0 Mymode	is @ Defa	ult models								
		tienanejinpluzzy		Payload delivery									Paramete								
		tiesanejinphash		Payload delivery					Nodel	Org				Decay		Default					
		tiename(md5	-	Payload delivery	13			D	Nore	ю		Formala	Lifetime				Basescore config		s Types		_
		Senarrelpehash	1.0	Payload delivery	13			8 29	Phishing		Simple model to	Polynomial	3	2.3	30	80	estimative- 0		9	×	Load mod

Create, modify, visualise, perform mapping

MISP and Decaying of Indicators

Implementation in MISP: Fine tuning tool



### IMPLEMENTATION IN MISP: base\_score TOOL

	ity-level (45%)	
# directly scale		
socrea estability   information-credibility   printry-level   printry-level   printry-level   information-credibility   information-level   infor		
information-credulity   printly-loadie   printly-loadie   printly-loadie   researce   res		
printy leads * * * * * * * * * * * * * * * * * * *		
prodrydered 53   versense 54   versense 55   versense 55 <td></td> <td></td>		
restatus   resta		
execution       0         execution 4 analysis (a)       0         conditioned probability       0         conditioned readinguing       0         conditioned readinguing       0         conditioned readinguing       0         conditioned readinguing       0         conditioned reading       0         conditioned reading       0         conditioned reading       0         prochological acceptability       0         conditioned reading       0		
advandave drog unge *   insellindove drog unge drog under difference   insellindove drog under difference   ins		
indentood producting •   indentood prod		
conditiones evaluation (udgrand)   rendences evaluation (udgrand)   rendences evaluation   rendences evaluation   rendences   rendences <td></td> <td></td>		
automation-level - 0		
condenses severil     intreat-level     intreat-level </td <td></td> <td></td>		
trade-week     automation-sevel     automation-sevel     automation-sevel     automation-sevel     automation-sevel     prochological-acceptability     brochological-acceptability     brochological-acceptability <td></td> <td></td>		
automation-level		
Attribute     Taps       table     Tapsor       psychological accorptability •     Tapsor       Cardinated =     Tapsor       Attribute     Tapsor       Attribute     Tapsor       Cardinated =     Tapsor       Cardinated =     Tapsor       Tapsor     Tapsor       Attribute     Interaction encodenting states and en		
state •     0     Tage       psychological acceptability •     0     attribute     attribute       State •     0     attribute     attribute       Attribute 2     state transport and states states informations and states states informations and states states informations and states attribute     attribute 1       Attribute 2     informations and states attributes at		
tatar •		Base
prychologicał acceptability • • • • • • • • • • • • • • • • • • •	soc	score
Exhibited *     Attributed 2     At		
Introduction constraining     Introduction constraining       Attribute 3     infortigenetic activity       Computation steps     Computation       Tag     Eff.       Ratio     Ratio		0.0 €
Computation steps Tag Eff. Ratio Vi	e	38.2 €
Tag Eff. Ratio Va		84.6 €
Tag Ert. Patio Va		
arr. Ratio Va		
		Result
priority-level:baseline-minor 0.46 * 2	Value * 25.00 11.62	11.62
admirally-scale:source-reliability="d" 0.27 * 2	* 25.00 6.80	3.80

MISP and Decaying of Indicators من المنافعة ال

2022

Implementation in MISP: base\_score tool



#### IMPLEMENTATION IN MISP: SIMULATION TOOL

MISP and Decaying of Indicators

2022

Implementation in MISP: simulation tool



 Base score () Base score configuration not set. But default value sets. NIDS Simple Decaying Mode RestSearch Specific ID Computation Result CH. Attribute RestSearch<sup>6</sup> Ratio Value × 75.00 "includeDecayScore": 1, "includeFullModel": 0. × 50.00 0 "score": 30, × 100.00 "decayingModel": [85], 0 × NoN ( "to\_ids": 1, "tags": l'estimative-language%", "prioritybase\_score 80.00 September Sighting Wed Sep 4 12:18:09 2019 Current score 54:60 August October November December Event Teen Galaxies × NIDS Simple Decaying ... 37.41 ORGNAME Network activity (p-sro 8888 admiralty-scales VIDS Simple Decaying ... 54.6 Page 1 of 1, showing 2 records out of 2 total, starting on record 1, ending on 2

Simulate Attributes with different Models

#### IMPLEMENTATION IN MISP: API QUERY BODY

/attributes/restSearch

MISP and Decaying of Indicators

2022

└─Implementation in MISP: API query body

IMPLEMENTATION IN MISP: API QUERY BODY

attributes/restSearch

fintledscopic.er=1:1.
intledsitions.intledsition.
factledscopyed:0,
factledscopyed:0,
factledscopyed:0,
factledscopyed:0,
factledsit:10
f

# 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)

MISP and Decaying of Indicators

2022

 $\Box$  Creating a new decay algorithm (1)

#### CREATING A NEW DECAY ALGORITHM (1)

#### the current architecture allows users to create their **own** formulae.

- Create a new file \$filename in app/Model/DecayingModelsEprmulas
- Extend the Base class as defined in DecayingModelBas
- Implement the two mandatory functions computeScore
- and isDecayed using your own formula/algorithm 4. Create a Model and set the formula field to \$filename
  - 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

10 11 12

13 14

15

2 include\_once 'Base.php';

```
4 class Polynomial extends DecayingModelBase
```

```
public const DESCRIPTION = 'The description of your new
decaying algorithm';
```

public function computeScore(\$model, \$attribute, \$base\_score, \$elapsed\_time)

```
// algorithm returning a numerical score
```

public function isDecayed(\$model, \$attribute, \$score)

// algorithm returning a boolean stating
// if the attribute is expired or not

MISP and Decaying of Indicators

2022

└─Creating a new decay algorithm (2)

REATING A NEW DECAY ALGORITHM (2)
ptp
clude\_ence "Ease-php";
ass. Dobracelal estands DecemberGoldean

```
nihytemetti aasted bezytemettemetteme
bestering optimistic constructions - The decaying optimistic
decaying optimistic constructions(funds), faiththete, faber_scene,
interpretering a numerical scene
j // algebrain networks a numerical scene
profile foretion indecayed(funds), faiththete, faiththete
j algebrain networks a numerical scene
j // influence in separate or skene
// influence in separate or skene
```

# 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

MISP and Decaying of Indicators

Decaying Models 2.0

#### DECAYING MODELS 2.0

#### Improved support of Sightings Solution positive Sightings

- 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 Togs or Correlations when
- computing score Increase Toxonomy coverage
- Users should be able to manually override the numerical\_value of Tops
- For specific type, take into account data from other services
   Could fetch data from BGP ranking, Virus Total, Possive X for IP/domain/... and adapt the score