MISP AND DECAYING OF INDICATORS

AN INDICATOR SCORING METHOD AND ONGOING IMPLE-

TEAM CIRCL

INFO@CIRCL.LU

SEPTEMBER 16, 2022



MISP and Decaying of Indicators

10



2022-09-16 __ ⋜

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	- E
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 Expiring IOCs: Why and How? -60

-Indicators - Problem Statement

- Various users and organisations can share data via MISP, Trust, data quality and time-to-live issues
 Each user/organisation has different use-cases and interest Conflicting interests such as operational security, attribution

9

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

-Indicators - 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
 construct water
- 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

- 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)

Тахо	nomies						
« previo	ous 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., Boukhtouta, A., Assi, C., & Debbabi, M. (2019) in Detecting Internet Abuse by Analyzing Passive DNS Traffic: A Survey of Implemented Systems. IEEE Communications Surveys & Tubriats, 1–1. doi:10.1108/comst2018.2849614	1	No		0/18	+01
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 Kate Kolemola and Greg Wiseman.	2	Yes		11/11	- 0 🕯

- 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	ceamies						
	Services 1	Narran .	-	-	-	100.00	-
٠	with the second s	Notice applied by application of the paper is a polytopic to the polytopic of the polytopic					1
•	1007101	A consistent classes af in frames about the IAM is interacting from 1. Interfaced, et., Ann. 2. or Section, N. (2018). Section for the effective interaction framework from 1. Anno 2. or Section 2. Anno 2. A					•
	Super-Tradinsis	The Tagging Treat Area is a realistic analysis aread tool with generic and comparison to the comparison of the treatment of the treatment and the treatment of the treatment of the treatment of the treatment of the treatment of the treatment of the treatment of the treatment of the treatment of the treatment of the treatment of the treatment of the treatment of the treatment of the treatment of the treatment of the treatment of					•

Classification must be globally used to be efficient

TAXONOMIES - REFRESHER (2)

ADMIRALTY-SCALE Taxonomy Library

		· ·					
	127						
lamespace	admiralty-scale						
lescription		or Ranking (also called the NATO System) is used to rank the r	reliability of a sou	irce and th	e credibility o	of an information. Reference based on FM 2-22.3	(FM 34-5
		NCE COLLECTOR OPERATIONS and NATO documents.					
ersion	4						
nabled	Yes (disable)						
« previous next »							
						Filter	
Tag		Expanded	Numerical value	Events	Attributes	Tags	Actio
admiralty-scale:info	rmation-credibility="1"	Information Credibility: Confirmed by other sources	100	6	0	admiralty-scale:Information-credibility="1"	< 2-
admiralty-scale:info	rmation-credibility="2"	Information Credibility: Probably true	75	21	1	admiralty-scale:information-credibility="2"	< 2-
admiralty-scale:info	rmation-credibility="3"	Information Credibility: Possibly true	50	16	5	admiralty-scale:information-credibility="3"	< ຊ-
admiralty-scale:info	rmation-credibility="4"	Information Credibility: Doubtful	25	2	0	admiralty-scale:information-credibility="4"	< ຊ-
admiralty-scale:info	rmation-credibility="5"	Information Credibility: Improbable	0	1	0	admiralty-scale:Information-credibility="5"	< ສ-
admiralty-scale:info	rmation-credibility="6"	Information Credibility: Truth cannot be judged	50	9	2	admiralty-scale:information-credibility="6"	< ສ-
admiralty-scale:sou	rce-reliability="a"	Source Reliability: Completely reliable	100	1	0	admiraity-scale:source-reliability="a"	g -
admiralty-scale:sou	rce-reliability="b"	Source Reliability: Usually reliable	75	21	76	admiraity-scale:source-reliability="b"	2 -
admiralty-scale:sou	rce-reliability="c"	Source Reliability: Fairly reliable	50	9	8	admiralty-scale:source-reliability="c"	2 -
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	admiraity-scale:source-reliability="e"	g-
admiralty-scale:sou							
admiralty-scale:sou admiralty-scale:sou	rce-reliability="f"	Source Reliability: Reliability cannot be judged	50	10	7	admiralty-scale:source-reliability="f"	g -

\rightarrow Cherry-pick allowed *Tags*

MISP and Decaying of Indicators Lexpiring IOCs: Why and How?

09-16

2022

└─Taxonomies - Refresher (2)

	LTY-SCALE 1	acceanty Library					
Annual I						fan informalien, federerier inner	
	a part of the second						
- *		Spender .	territor and	-	****	~	
			-0				
		Mondae (webs), Kindy See					
						And the second second	
		months faulting fail and to page					

TAXONOMIES - REFRESHER (3)

MISP and Decaying of Indicators

└─Taxonomies - Refresher (3)

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	507	Truth cannot be judied	507
Deliberative decention	0.7		

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 ?	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(streams) = base_score(streams, must) + decay(must, time

Where,

- $\blacksquare \ \texttt{score} \in [0,+\infty]$
- base_score ∈ [0,100]
- decay is a function defined by model's parameter controlling decay speed
- Attribute Contains Attribute's values and metadata
- Model Contains the Model's configuration

Score(Attribute) = base_score(Attribute, Model) • decay(Model, time)

Where,

- **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

2022-09-16 ┌─ ⊠

MISP and Decaying of Indicators

CURRENT IMPLEMENTATION IN MISP

CURRENT IMPLEMENTATION IN MISP

IMPLEMENTATION IN MISP: Event/view

3	laxies + 💵														
« pr	evíous I	next »	view all												
+	E I	e > Org	Category		Teles	ted 🛃 Decay score 🕢 Context 🖓 Related Tags	Filtering to Galaxies	Correlate	Related Fee	sd IDS	Distribution	Sightings	Activity	Enter value to search	Q X
									Events hit	5					
2	019-09-12		Network activity	ip-src	5.5.5.5	C + 2 +	⊗ + ≗ +	×			Inherit	6 Q /		NIDS Simple Decaying 65.26 Model 5 79.88	•••
2	019-08-13		Network activity	lp-src	8.8.8.8 A	Image: Source-reliability="a" x Image: Source-reliability="a" x <t< td=""><td>3+ ≗+</td><td>×</td><td>1222 S1: Show S1: 11 more</td><td></td><td>Inherit</td><td>心 ゆ ア (5/0/0)</td><td>LLL.</td><td>NIDS Simple Decaying 54.6 Model 5 52.69</td><td>• • •</td></t<>	3 + ≗ +	×	1222 S1: Show S1: 11 more		Inherit	心 ゆ ア (5/0/0)	LLL.	NIDS Simple Decaying 54.6 Model 5 52.69	• • •
) 2	019-08-13		Network activity	ip-src	9.9.9.9 A	edmirally-scale:source-reliability="c" x misp:confidence-level="completely-confident" tip:amber x © +	⊗ +≜+ ×	×		1 @	Inherit	らな メ (4/10)	MI_I	NIDS Simple Decaying 37.43 Model 5 0	• • •
) 2	019-08-13		Network activity	ip-src	7.7.7.7	Image: Second	8 + よ+	×	41	8	Inherit	かな メ (3000)		NIDS Simple Decaying 37.41 Model 5 0	• • •
							⊗ + ≜ +		41		Inherit	691		model 0	

Decay score toggle button

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

Implementation in MISP: Event/view

2										
	•••				-					
					-	- 22			-	-
			- 08/8		1913			217		••
			2000	- 1497	- 30			27		
		-	1	141.4				-	And C.	
			Seren		-		-			-
								227		

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

29

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

و

6

2022

Implementation in MISP: API result



IMPLEMENTATION IN MISP: PLAYING WITH MODELS

MISP and Decaying of Indicators

2022

└─Implementation 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

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 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

 $base_score = \omega_{tg} \cdot tags + \omega_{sc} \cdot source_confidence$

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,

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

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

Scoring Indicators: base_score (2)

Current implentation ignores source confidence:

\rightarrow base_score = tags

	Comp			
Tag	Eff. Ratio		numerical_value	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 -Decaying Models in Depth Ś

-Scoring Indicators: base_score (2)

SCORING INDICATORS: base_score (2)
Current implentation ignores source_confidence:

→ base_score	– tags							
	Comp	Computation						
54	an. Raio		namerical value	Plenalt				
adminally scale secure reliability: "Completely reliable"	6.90		300.80	10.00				
phisting psychological-acceptabilitys/high*	6.50		75.00	07.50				
		-						

ە

SCORING INDICATORS: DECAY SPEED (1)

MISP and Decaying of Indicators

└─Scoring Indicators: decay speed (1)

SCORING INDICATORS: DECAY SPEED (1)

core(minute) = base_score(minute, main) + decay(main, main)

- The decay is calculated usin
- The lifetime of the indicator
 May yary 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 score
- 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

SCORING INDICATORS: PUTTING IT ALL TOGHETHER

MISP and Decaying of Indicators

2022

Scoring Indicators: putting it all toghether

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

 $[1^{2}$ some = hose, some $(1 - (\frac{1}{2})^{\frac{1}{2}})$

- edefined: Parameters:lifetime, decay_rate, threshold base_score default base score
- formula
 associate Attribute types

creator organisation

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

IMPLEMENTATION IN MISP: MODELS TYPES

MISP and Decaying of Indicators

2022

Implementation in MISP: Models Types

IMPLEMENTATION IN MISP: MODELS TYPES

Multiple model types are available **Default Models:** Models created and shared by the community. Available from misp-decaying-models repository0. **→** → Not ofdiable

- Organisation Models: Models created by a user belonging to
- 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 repository³.
 - $\blacktriangleright \rightarrow Not \ editable$
- Organisation Models: Models created by a user belonging to an organisation
 - These models can be hidden or shared to other organisation
 - $\blacktriangleright \rightarrow Editable$

³https://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 phishing website.	{ "ilfetime": 3, "idecay_speed": 2.3, "threshold": 30, "default_base_score": 80, "base_score_config": { language": 0.5, "phishing": 0.5, } }	Polynomial	9	1	~	■ △
35	1	×	NIDS Simple Decaying Model	Simple decaying model for Network Intrusion Detection System (NDS).	{ "lifetime": 120, "decay_speed": 2, "threshold": 30, "default base score": 80, "base, score": 80, "base, score": 80, "base, score": 025, "priority-level": 0.25, "targeted-threat- index": 0.125, "tailse-positive": 0.125 } } }	Polynomial Ø	13	1	~	⊞ & ⊘ ∥
-		rds out of 2 total, s	starting on record 1, ending on 2							
« previo	us next »									

MISP and Decaying of Indicators

09-16

2022

└─Implementation in MISP: Index

Tantan Index	Cartan Cartan	 frame (***	A DECK	-
	and have been seen of				

IMPLEMENTATION IN MISP: FINE TUNING TOOL

		aying Of Indicator F	·ine	running roor																	
del	Sho	w All Types 🔋 Show MISP Objects	Searc	h Attribute Type	5			Polynor	nial		т ө										
	8	Attribute Type		Category	Model ID	1	1	100	1												
OF S		aba m		Financial traud				50	ł												
		authenthush		Payload delivery				80													
		bank-account-nr		Financial fraud				70	1												
		bic		Financial fraud				60		_											
		bin		Financial fraud				50 40													
		bro		Network activity	10 11			30					-								
		btc		Financial Insud	11		1	20													
		ec-number		Financial Insud				30													
		odhash		Payload delivery				0.0			o ois io is						15 20 25				
	0	community-id		Network activity							0.8	10		Days		2.0	2.5		8.0		
	8	domain		Network activity			L t	Life	ime 3		-8			days	Facil	e aher ölfetime		10	leys and 71	ours.	
	8	domainijo		Network activity	10.84			Decay speed 2.5								: halved after (1) 0 de		lay and 6 hours	
	8	enal-atachment		Poyload delivery				Cutoff threshold 30				E .									
		enal-dg		Network activity	н				ant base see	_		illate this me									
		email-src		Payload delivery			1.5	() Adj	INT DANK NO	170 E	e sin	un na na	SI .								
		Service	-	Payload delivery				Phishing	model		Sin	nple model 6	o rapidly d	ocay 🍏	C tak						
		Sexarrejauthenthash		Payload delivery				0 AL	All available models 0 My models * Default models												
		tienanejinpluzzy		Payload delivery									Paramet								
		tiesanejinphash		Payload delivery					Model	Org				Decay		Default					
		Network/md5		Payload delivery	13			10	Phishing	ю	Description	Formula Polynomial	Lifetime		Threshold 30	basescore 80	Basescore config		is Types	Enabled	
																	estrative- 0.				Load mod

Create, modify, visualise, perform mapping

MISP and Decaying of Indicators

09-16

2022

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 -Decaying Models in Depth

10

6

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 RestSearch⁶ Ratio Value × 75.00 "includeDecayScore": 1, "includeFullModel": 0. × 50.00 0 "score": 30, × 100.00 0 "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
```

09-16

2022

Implementation in MISP: API query body



ttributes/restSearch	
<pre>'includeDecayScore': 1, 'includeFullModel': 0, 'excludeDecayed': 0, 'decayinModel': [85].</pre>	
"modelOverrides": ["threshold": 30	
"score": 30,	

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

Q

2022-09-

└─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 /DecavingModels Formular
- Extend the Base class as defined in DecayingModelBas
- Extend the Base class as defined in DecayIngModeLBase
 Implement the two mandatory functions computeScore
- and isDecayed using your own formula/algorithm 4. Create a Model and set the formula field to \$filename
- Jse cases: Add support for more feature (expiration taxonomy
- B Add support for more reature (expiration taxonomy)
 B 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

ى

6

2022

└─Creating a new decay algorithm (2)

REATING A NEW DECAY ALGURITHM (2) phy dise_enses "Base_phy"; ass Polynomial extends OccayingNodellass public cosst DECEMPTOR - "The Gescription of your new decaying algurith";

public runction computescore(smose), sattribute, spake_sco selapsed_time) { // algorithm returning a numerical score }

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

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

Q

2022-09

Decaying Models 2.0

DECAYING MODELS 2.

Improved support of 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 neighboring surgest
- 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 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