$_{\underset{\ensuremath{\Theta}}{\infty}}$ MISP and Decaying of Indicators

2024-07

MISP AND DECAYING OF INDICATORS AN INDICATOR SCORING METHOD AND ONGOING IMPLE-



MISP AND DECAYING OF INDICATORS

AN INDICATOR SCORING METHOD AND ONGOING IMPLE-

TEAM CIRCL

INFO@CIRCL.LU

JULY 8, 2024



2024-07-08 __ ⊠

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 2024-07-08 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	
	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 ω Expiring IOCs: Why and How? 2024-07

-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

Õ

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 ω Expiring IOCs: Why and How? 2024-07

-Indicators - Problem Statement

- Trust, data quality and time-to-live issues
 Each user/organisation has different use-cases and interest
- Conflicting interests such as operational security, attribution,

- ► Partial info about their freshness (Sighting
- Partial info about their validity (last update)

REQUIREMENTS TO ENJOY THE DECAYING FEATURE IN MISP

MISP and Decaying of Indicators Expiring IOCs: Why and How? Requirements to enjoy th

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

> ng ng 🌶 (44/<mark>0</mark>/0)

MISP and Decaying of Indicators ω Expiring IOCs: Why and How? 2024-07

-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 Expiring IOCs: Why and How?

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

MISP is a peer-to-peer system, information passes through multiple instances. **B Producers can add context** (such as tags from Toxonomics, 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

TAXONOMIES - REFRESHER (1)

Taxo	onomies						
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. (2019) in Detecting Internet Abuse by Analyzing Passive DNS Traffic: A Survey of Implemented Systems. IEEE Communications Surveys & Tutorials, 1–1. doi:10.1109/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 makware to a victim's computer. The TIT metric was first introduced at SecTor 2013 by Sen Hardray as and to the taik "RABarboyte: kontroling a Malware Menagerie" along with Katle 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 80 Expiring IOCs: Why and How? 2024-07

-Taxonomies - Refresher (1)

24	ceanies						
	Notes and Names of Street of Streeto	Rection 1	***	-	-	10.00	-
٠	age of the second se	Notice agent improving the service improve integrate the specific of games and other to and all the many time and well information		*			
	making transition strates.	Constraints while income providing a press much in press in					
•	President and	A constant class of inclusion dataset in the A an analysis in Table 1. Eventues, et. An J. Schwartz, K. (2018). Standard strands from the integration for the A and th					•••
0	hepter/institute	The Traphel Trans Join 1 and 1 is straping or word theory were presented on sensing the sector characteristic action in the Sector Sector Sector Sector presented to the Sector Sector Sector Sector Sector Sector Sector Interpret Proceedings of the Sector Sector Sector Sector Sector Interpret Proceedings of the Sector Sect		1			

Classification must be globally used to be efficient

TAXONOMIES - REFRESHER (2)

ADMIRALTY-SCALE Taxonomy Library

đ	127						
amespace	admiralty-scale						
lescription	The Admiralty Scale	or Ranking (also called the NATO System) is used to rank the	reliability of a sou	rce and th	e credibility	of an information. Reference based on FM 2-22.3 (M 34-5
	HUMAN INTELLIGE	NCE COLLECTOR OPERATIONS and NATO documents.					
rersion	4 Mag (displate)						
Inabled	res (disable)						
« previous next »							
						Filter	
- T -		Freedad	Numerical	Franks	Antolioutere	Tran	Anting
Tag		Expanded	value	Events	Attributes	lags	ACTION
		Information Conditionity Conditioned by although a second	400		•	a desta da la foto esta de la della	a-
admirally-scale.infor	mation-credibility= 1	information Credibility: Continned by other sources	100	0	0	admiranty-scales/mormation-credibility= 1	10-
admiralty-scale:infor	mation-credibility="2"	Information Credibility: Probably true	75	21	1	admiralty-scale:Information-credibility="2"	g -
admiralty-scale:infor	mation-credibility="3"	Information Credibility: Possibly true	50	16	5	admiralty-scale:information-credibility="3"	ຊ-
admiralty-scale:infor	mation-credibility="4"	Information Credibility: Doubtful	25	2	0	admiralty-scale:Information-credibility="4"	ຊ-
admiralty-scale:infor	mation-credibility="5"	Information Credibility: Improbable	0	1	0	admiralty-scale:Information-credibility="5"	ຊ-
admiralty-scale:infor	mation-credibility="6"	Information Credibility: Truth cannot be judged	50	9	2	admiralty-scale:Information-credibility="6"	g-
admiralty-scale:sour	ce-reliability="a"	Source Reliability: Completely reliable	100	1	0	admiralty-scale:source-reliability="a"	e -
admiralty-scale:sour	ce-reliability="b"	Source Reliability: Usually reliable	75	21	76	admiralty-scale:source-reliability="b"	<i>c</i> -
admiralty-scale:sour	ce-reliability="c"	Source Reliability: Fairly reliable	50	9	8	admiralty-scale:source-reliability="c"	g -
admiralty-scale:sour	ce-reliability="d"	Source Reliability: Not usually reliable	25	2	0	admiralty-scale:source-reliability="d"	c -
admiralty-scale:sour	ce-reliability="e"	Source Reliability: Unreliable	0	0	0	admiralty-scale:source-reliability="e"	ø-
admiralty-scale:sour	ce-reliability="f"	Source Reliability: Reliability cannot be judged	50	10	7	admiralty-scale:source-reliability="f"	ø-
	as selicibility for	Source Reliability: Deliberatly decentive	0	NI/A	NI/A		

\rightarrow Cherry-pick allowed *Tags*

MISP and Decaying of Indicators

└─Taxonomies - Refresher (2)

ADMIRA.	LTY-SCALE T	exception Library					
	10						
No. of Concession, Name	10000						
Internet						star Internation, Robert	
Boles .							
Topological Contraction of Contracti							
- × 0		Separate	-	-	-	*	
			-9				
		menator Leating Income					
		Mondan Taskella, Kantalan					
		mouth radialy for south page				-	
		Accessive Concess where	-9				-
		Some finding (peak where					-
		Recta Science (Series Science)	-				1.000
	Townson and the second s	NAME AND ADDRESS OF A DATA OF A DATA				10000	
		Southeasts (seals					
() and the							

2024

TAXONOMIES - REFRESHER (3)

MISP and Decaying of Indicators -08 -Expiring IOCs: Why and How? 2024-07

-Taxonomies - Refresher (3)

Description	Value	Description	Valu
Completely reliable	100	Confirmed by other sources	100
Isually reliable	75	Probably true	75
lairly reliable	50	Possibly true	50
tot usually reliable	25	Doubtful	25
Inteliable	0	Improbable	0
teliability cannot be judged	507	Truth cannot be judged	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 ?	Truth cannot be judged	50 ?
Deliberatly deceptive	0?		

SCORING INDICATORS: OUR SOLUTION

MISP and Decaying of Indicators ω Expiring IOCs: Why and How? 2024-07

-Scoring Indicators: Our solution

- score $\in [0, +\infty)$
- base score c lo pop decay is a function defined by model's param
- Attribute Contains Attribute's va
- Model Contains the Model's configuration

Score(Attribute) = base score(Attribute, Model) • decay(Model, time)

Where.

- **score** \in [0, + ∞
- **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

MISP and Decaying of Indicators

CURRENT IMPLEMENTATION IN MISP

CURRENT IMPLEMENTATION IN MISP

IMPLEMENTATION IN MISP: Event/view

= Pixots = Galaxy 🗙 45: Decayi	+Event graph +Cor	rrelation gra	ph +ATT&CK matrix -Attributes -Discussion										
Galaxies	view all												
+ E E 2	Category Type	Delete Value	d 🛃 Decay score 🕜 Context 🚏 Rélated Tags Tags	Filtering too Galaxies	(1) Comment	Correlate	Related Fee Events hits	d IDS	Distribution	Sightings	Activity	Enter value to search Score	Q X Actions
2019-09-12	Network activity ip-se	c 5.5.5.5	©÷ ≜+	⊗ + ≗ +		8			Inherit	ić Q ≱ (0\0/0)		NIDS Simple Decaying 65.26 Model 5 79.88	• • •
2019-08-13	Network activity ip-sr	c 8.8.8.8	Image: Source-reliability="a" x Image: Source-reliability="a x Image: So	8 + 2 +		×	1222 S1:1 Show S1:2 11 more	8	Inherit	心 ゆ チ (500)	LLL.	NIDS Simple Decaying 54.6 Model 5 52.69	• • •
2019-08-13	Network activity lip-sr	c 9.9.9.9 A	admiratly-scale:source-reliabilitys"c" x misp:confidence-level="completely-confident" x tip:amber x	() + () + () + () + () + () + () + () +		×	1 3 19 S1:1 28 Show 6 more	8	Inherit	むや <i>ト</i> (4/10)	MJL	NIDS Simple Decaying 37.43 Model 5 0	• • •
2019-08-13	Network activity ip-sr	c 7.7.7.7	Ø admiratly-scale information-credibility="4" x Ø retention:2d x Ø + ▲+	8 + ± +		8	41	8	Inherit	かや <i>ド</i> (300)		NIDS Simple Decaying 37.41 Model 5 0	.
2019-07-18	Network activity ip-sr	c 6.6.6.6	⊗ + ≜ +	⊗ + ≗ +		8	41	8	Inherit	i⇔ i⊃ ≯ (0\0/0)		NIDS Simple Decaying 23.31 Model 5 0	

Decay score toggle button

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

MISP and Decaying of Indicators

Implementation in MISP: Event/view

-										
68.9										
										12
			-	-		-	100	-		-
	interaction of	1919	12/10		-	227			**	•
	-	 OTHER DESIGNATION.	12/2		-	12.0				•
		Construction of the local distribution of th								
		(*************************************								
	No. of the local division of the local divis				-					
		Common La Ca				-				

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

29

2024

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

ω

2024

Implementation in MISP: API result



IMPLEMENTATION IN MISP: PLAYING WITH MODELS

MISP and Decaying of Indicators

2024-

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

MISP and Decaying of Indicators

DECAYING MODELS IN DEPTH

DECAYING MODELS IN DEPTH

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

base score = $\omega_{ta} \cdot tags + \omega_{sc} \cdot source_confidence$

Where,

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

MISP and Decaying of Indicators ω Decaying Models in Depth 2024-07

-Scoring Indicators: base_score (1)

account. The base score is calculated with the following in mine Data reliability, credibility, analyst skills, custon prioritisation tags (economical-impact), etc. Trust in the source

 $base_score = \omega_{bo} \cdot togs + \omega_{ac} \cdot source_confidence$

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

	Compu	on			
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

-Scoring Indicators: base_score (2)

|--|

urrent implentation ignores source_confidence:

→ base_score = togs

	_		
742	105		Persalt
	Plate	namerical, sala	
administry scale secare reliability: "Completely reliable"	6.90	300.80	90.80
phishing psychological-acceptability/"high"	6.50	75.00	07.50
			87.80

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

2024-

SCORING INDICATORS: DECAY SPEED (1)

MISP and Decaying of Indicators ω Decaying Models in Depth 2024-07

-Scoring Indicators: decay speed (1)

- The lifetime of the indicator

- The time elapsed since the latest update or sightin

Score(Attribute) = base score(Attribute, Model) • decay(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

2024-

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 ∞ 2024-07-0 Decaying Models in Depth

-Implementation in MISP: Models definition

Parameters: lifetime, decay rate, threshold base_score default base score associate Attribute type creator organisatio

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

ω

6

2024-

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 repository?. **b** whot offable

- 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

21

IMPLEMENTATION IN MISP: INDEX

Decaying Models

« previous next »

1 • Plaking model Single model to rapidly decay plaking widets.	ID	Organization	Usable to everyone	Name	Description	Parameters { }	Formula	# Assigned Types	Version	Enabled	Actions
1 X NDDS Simple Decaying Model www Simple decaying model for Network transion Detection System (NDDS)	29	1	~	Phishing model	Simple model to rapidly decay phishing website.	{ "iffetime": 3, "idecay, speed": 2.3, "threshold": 30, "default_base_score": 80, "base_score_config": { language": 0-5, "phishing": 0.5, } }	Polynomial Ø	9	1	~	■ △ 🚔 ♂ ॥
Page 1 of 1, showing 2 records out of 2 total, starting on record 1, ending on 2	85	1	×	NUDS Simple Decaying Model	Simple decaying model for Network Intrusion Detection System (NDS).	{ "lifetime": 120, "ideay: speed": 2, "threshold": 30, "default, bas, score', s0, "base, score, config": { "restimative- restimative- language": 0.25, "retention": 0.25, "taste-positive": 0.125, "false-positive": 0.125, } } }	Polynomial	13	1	*	₩ & ৫ ₩
a possibility and a	Page 1 of 1	showing 2 reco	rds out of 2 total, st	arting on record 1, ending on 2							
w heatened to be a second of the second of t	« previou	s next »									

MISP and Decaying of Indicators

2024

└─Implementation in MISP: Index

E	Tariate	-	and the second	-	hanse (***	1100	-	
			-	ling inspired in land in an link (see 1999)					

IMPLEMENTATION IN MISP: FINE TUNING TOOL

	10 Sho	w All Types B Show MISP Objects Sea	ch Attribute Type	3		Polynor	nial		T 😡										
		Attribute Type	Category	Model ID	1	100	,												
lets		aba m 🕨	Financial traud		1	50	1												
		authenthash 🕨	Payload delivery			80													
		bank-account-or	Financial Insud			70		<											
		bic 🏓	Financial Insul		1	. 60	1	~											
		ba P	Financial based			§ 50			-	~									
		bro 🏓	Network activity	10.11			1				-								
		bic 🏓	Financial haud	n		20													
		co-number	Financial haud			10													
	0	cdhash 🏓	Payload delivery					L.,									٩.		
	0	community-id	Network activity						0.5	10		Days		2.0	2.5		8.0		
	8	domain 🏴	Network activity			Life	ime 3		-8			days	Expin	e alter ölletime	9		i days and	7 hours	
	8	domainijo 🍽	Network activity	10.84		Decay	speed 2	3					Score	halved after ()	Half-We)	-) day and 6	hours	
	8	enal-atachment	Payload delivery			th Tron	reshold 3	n											
	8	email-dst 🕨	Network activity	ш					La start	2									
	8	email-sco 🍽	Payload delivery																
		tiesane 🕨	Payload delivery		P	hishing	model		Sim	ple model 6	o rapidly d	ocay 🍏	C tak						
		tienamejauthenthash	Payload delivery			0 A17	wailable m	odels	O My model	is @ Deta	uit models								
	•	tienamejimpluzzy	Payload delivery								Paramete	en .							
		Nesarajimphaah	Payload delivery				Model	Org				Decay		Default			1		
		tienamejno5	Payload delivery	13			rearee		Unscription	Pormula.	Literine	speed	inreshold	onsescore	Dasescore con	g Sett	ngo Type	n unabled	A000
		Reconstruction back	Designed defenses	12		5 25	Phishing	1	Simple model to	Polynomial	3	23	30	80	estrative-	35	,	~	Lo
			Payona centrely												language				

Create, modify, visualise, perform mapping

MISP and Decaying of Indicators

2024

Implementation in MISP: Fine tuning tool



IMPLEMENTATION IN MISP: base_score TOOL

Search Taxonomy	×	3 not having numerical value		admirally-scale information-credibility (20%)	pr	iority-leve	H (46%)	
Default basescore 80								
Taxonomies	Weight							
admiralty-scale -								
source-reliability -		31						
information-credibility -	Ξ.	30						
priority-level *								
priority-level -		53		adminalty-scale source-reliability (27%)				
retention *								
retention -	1	0						
estimative-language -								
likelihood-probability -		0						
confidence-in-analytic-judgment -	ā	0						
misp -								
confidence-level -	ā	0						
threat-level -	8	0		Placeholder for 'Organisation	n source confidence`			
automation-level -	1	0	Example	ø				
phishing +								Base
state -	8	0	Tag your	Tags				score
psychological-acceptability -	E	0	attribute	-				
Excluded *	_		Attribute 1	admiralty-scale:information-credibility="5"		_		0.0 😧
			Attribute 2	priority-level:baseline-minor admiralty-sca admiralty-scale:information-credibility="2"	ale:source-reliability	=""		38.2 😧
			Attribute 3	priority-level:severe admiralty-scale:inform	mation-credibility="2			84.6 😧
			Computa	ation steps				
					Comp	utation		
			Tag		Eff. Ratio Value		Value	Result
			priority-lev	rel:baseline-minor	0.46	*	25.00	11.62
			admiralty-	scale:source-reliability="d"	0.27		25.00	6.80

MISP and Decaying of Indicators

2024

└─Implementation in MISP: base_score tool



IMPLEMENTATION IN MISP: SIMULATION TOOL

MISP and Decaying of Indicators

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 "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

2024-07-08 -

IMPLEMENTATION IN MISP: API QUERY BODY

/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
```

MISP and Decaying of Indicators

2024-

Implementation in MISP: API query body

IMPLEMENTATION IN MISP: API QUERY BODY

"incl	deDecayScor	ets sur-		
"incl	defullModel	1: e.		
"excl	deDecayed*:	e, 1		
*decar	in#Model":	[85].		
"mode	Overrides":			
	threshold":	30		
"scor	*: 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 ω Decaying Models in Depth 2024-07-

-Creating a new decay algorithm (1)

The current architecture allows users to create their on

- Add support for more feature (expiration taxonomy
- Completely different approach (i.e streaming algorithm) .

27

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

2024

└─Creating a new decay algorithm (2)

CREATING A NEW DECAY ALGORITHM (2)

```
And a set of the set o
```

28

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 ω Decaying Models in Depth 2024-07

Decaying Models 2.0

Improved support of Sightings

- Potential Model improvements

- Increase Toxonomy coverage