TURNING DATA INTO ACTIONABLE IN-TELLIGENCE

ADVANCED FEATURES IN MISP SUPPORTING YOUR ANA-

CIRCL / TEAM MISP PROJECT



CIISI-IE DUBLIN 2024



Turning data into actionable intelligence

-08



Turning data into actionable intelligence

Labout CIRCL

∞

2024-07

circleu
 The Computer Incident Response Certer Luxembourg (CIRCL)
 is a government-driven instatute designed to provide a
 and incidents. CIRCL is the CERT for the private sector,
 communes and non-governmental entities in Luxembourg
 and is operated by securitymateling is.



The Computer Incident Response Center Luxembourg (CIRCL) is a government-driven initiative designed to provide a systematic response facility to computer security threats and incidents. CIRCL is the CERT for the private sector, communes and non-governmental entities in Luxembourg and is operated by securitymadein.lu g.i.e.

MISP AND CIRCL

Turning data into actionable intelligence

MISP and CIRCL

 CIRCL: in mandated by the Ministry of Economy and acting as the Luxenbourg National CERT frequents sector.
 CIRCL: Leads the development of the Open Source MSP threat intelligence communities, private companies, financial sector, National CERS and LESS globally.
 CIRCL: runs multiple large MSP communities performing active daily threat-intelligence advance.

- CIRCL is mandated by the Ministry of Economy and acting as the Luxembourg National CERT for private sector.
- CIRCL leads the development of the Open Source MISP threat intelligence platform which is used by many military or intelligence communities, private companies, financial sector, National CERTs and LEAs globally.
- CIRCL runs multiple large MISP communities performing active daily threat-intelligence sharing.

∞

THE AIM OF THIS PRESENTATION

Turning data into actionable intelligence

└─The aim of this presentation

- To give some insight into what sort of an evolution of our various communities' have gone through as observed over the past 8 years
- Show the importance of strong contextualisation...
- _and how that can be leveraged when trying to make ou data actionable

- To give some insight into what sort of an evolution of our various communities' have gone through as observed over the past 8 years
- Show the importance of **strong contextualisation**...
- …and how that can be leveraged when trying to make our data actionable

80

DEVELOPMENT BASED ON PRACTICAL USER FEEDBACK

There are many different types of users of an information sharing platform like MISP:

- Malware reversers willing to share indicators of analysis with respective colleagues.
- Security analysts searching, validating and using indicators in operational security.
- Intelligence analysts gathering information about specific adversary groups.
- Law-enforcement relying on indicators to support or bootstrap their DFIR cases.
- Risk analysis teams willing to know about the new threats, likelyhood and occurences.
- **Fraud analysts** willing to share financial indicators to detect financial frauds.

Turning data into actionable intelligence

Development based on practical user feedback

DEVELOPMENT BASED ON PRACTICAL USER FEEDBACI

- There are many different types of users of an information sharing platform like MISP:
- Malware reversers willing to share indicators of analysis with respective colleagues.
- Security analysts searching, validating and using indicators in operational security.
- Intelligence analysis gathering information about specific adversary groups.
- Law-enforcement relying on indicators to support or bootstrop their DER cacer.
- Risk analysis teams willing to know about the new threats
- Fraud analysts willing to share financial indicators to dete financial frauds.

80

Turning data into actionable intelligence

└─The initial scope of MISP

Extract information during the analysis process
 Store and correlate these datapoints
 Share the data with partners
 Procue on technical indicators: IP, domain, hostname, hashe
 fineame, pattern in file //memory/traffic
 Generate protective signatures out of the data: snort,
 suricata, OpenIOC

- **Extract information** during the analysis process
- Store and **correlate** these datapoints
- **Share** the data with partners
- Focus on technical indicators: IP, domain, hostname, hashes, filename, pattern in file/memory/traffic
- Generate protective signatures out of the data: snort, suricata, OpenIOC

80

INITIAL WORKFLOW



Turning data into actionable intelligence

└─Initial workflow



Turning data into actionable intelligence

∞

2024-07

└─Why was it so simplistic?

- This was both a reflection of our maturity as a community
- Capabilities for extracting information
- Capabilities for utilising the information
 Lack of utilingness to share context
 - Lack of co-operation between teams doing technical analysis/monitoring and threat-intel
 - The more growth we saw in maturity, the more we tried to match it with our data-model, often against purchase.

- This was both a reflection of our maturity as a community
 - Capabilities for extracting information
 - Capabilities for **utilising** the information
 - Lack of **willingness** to share context
 - Lack of co-operation between teams doing technical analysis/monitoring and threat-intel
- The more growth we saw in maturity, the more we tried to match it with our data-model, often against pushback

THE GROWING NEED TO CONTEXTUALISE DATA

2024-07-0

∞

Turning data into actionable intelligence

└─The growing need to contextualise data

- There were separate factors that made our data-sets less and less useful for detection/defense in general Forowth of our communities
- Growth of our communities
 Distinguish between information of interest and raw dat
- ► False-positive management
- TTPs and aggregate information may be prevalent compare to raw data (risk assessment)
- Increased data volumes leads to be able to prioritise

- There were separate factors that made our data-sets less and less useful for detection/defense in general
 - Growth of our communities
 - Distinguish between information of interest and raw data
 - False-positive management
 - TTPs and aggregate information may be prevalent compared to raw data (risk assessment)
 - Increased data volumes leads to be able to prioritise

OUR INITIAL SOLUTION

2024-07-08

Turning data into actionable intelligence

└─Our initial solution

 Allow users to tag any information created in MISP
 We wanted to be lax with what we accept in terms of data, but be strict on what we fed to our tools, with strong filter options

We had some ideas on how to potentially move forward...

Allow users to tag any information created in MISP

- We wanted to be lax with what we accept in terms of data, but be strict on what we fed to our tools, with strong filter options
- We had some ideas on how to potentially move forward...

OUR INITIAL FAILURES

Turning data into actionable intelligence

└─Our initial failures

- Try to capture different aspects of contextualisation into normalised values (threat level, source reliability, etc)
- Uran't scale with needs other than our own
 Incorporating new types of contextualisation would mean t
- modification of the software
- Getting communities with established naming conventions to use anything but their go-to vocabularies was a pipe-dream blocked assumed to our summaries compensions;

- Try to capture different aspects of contextualisation into normalised values (threat level, source reliability, etc)
 - Didn't scale with needs other than our own
 - Incorporating new types of contextualisation would mean the modification of the software
 - Getting communities with established naming conventions to use anything but their go-to vocabularies was a pipe-dream
 - Heated arguments over numeric conversions

80

HUMAN CREATIVITY

- We tried an alternate approach instead: Free tagging
 - Result was spectacularly painful, at least 7 different ways to spell tlp:amber
 - No canonisation for common terms lead to tagging ultimately becoming a highly flawed tool for filtering within a sharing community

TLP AMBER		
TLP:AMBER		
Threat tlp:Amber		
tip-amber		
tlp::amber		
tlp:amber		

Turning data into actionable intelligence

Human creativity

07-08

HOW WE ENDED UP TACKLING THE ISSUE MORE SUCCESSFULY

- We ended up with a mixed approach, currently implemented by the MISP-taxonomy system
 - Taxonomies are vocabularies of known tags
 - Tags would be in a triple tag format namespace:predicate="value"
 - Create your own taxonomies, recipients should be able to use data you tag with them without knowing it at the first place
 - Avoid any coding, stick to JSON
- Massive success, approaching 100 taxonomies
- Organisations can solve their own issues without having to rely on us

Тад	Events	Attributes	Tags
workflow.state="complete"	11	0	workflow:state="complete"
workflow:state="draft"	0	0	workflow:state="draft"
workflow:state="incomplete"	55	10	workflow:state="incomplete"
workflow:state="ongoing"	0	0	workflow:state="ongoing"

Turning data into actionable intelligence

2024-07

How we ended up tackling the issue more successfuly

HOW WE ENDED UP TACKLING THE ISSUE MOR SUCCESSFULY

 We ended up with a by the MISP-taxon 	omy system			entera
 Taxonomies are Tags would be in 	vocabularies o	e known	tags	
 Tags woodd be n 	:predicate-"y	alma"		
 Create your own data you tag wit Avoid any codin Massive success, aj Organisations can : 	th them without g, stick to JSON oproaching 10	t knowin o taxon	g it at the first p omies	lace
rely on us				
rely on us	farm.	Arributes	-	
	Parts T	Antones 0	Nap. Reality of the second	
0.14				
C MARKAGE CONTRAL			east for state to optimal	

WE WERE STILL MISSING SOMETHING...

- Taxonomy tags often non self-explanatory
- Example: universal understanding of tlp:green vs APT 28
- For the latter, a single string was ill-suited
- So we needed something new in addition to taxonomies Galaxies
 - Community driven knowledge-base libraries used as tags
 - Including descriptions, links, synonyms, meta information, etc.
 - Goal was to keep it **simple and make it reusable**
 - Internally it works the exact same way as taxonomies (stick to JSON)

B Ransor	nware galaxy	
Galaxy ID	373	
Name	Ransomware	
Namespace	misp	
Uuid	3f44af2e-1480-4b6b-9aa8-f9bb	21341078
Description	Ransomware galaxy based on	
Version	4	
Value 4		Synonyms
.CryptoHasYou.		
777		Sevleg
7ev3n		7ev3n-HONE\$T

Turning data into actionable intelligence

ω

2024-

└─We were still missing something...

Galaxies Community d Including des	mething new ir iven knowledge	s ill-suited n addition to taxonomie -base libraries used as ta aynonyms, meta informati
	orks the exact sa	d make it reusable ame way as taxonomies (s
 Goal was to k Internally it w 	orks the exact sa	
 Goal was to k Internally it w 	orks the exact sa	ame way as taxonomies (s

BROADENING THE SCOPE OF WHAT SORT OF CONTEXT WE ARE INTERESTED IN

2024-07-08

Turning data into actionable intelligence

Broadening the scope of what sort of context we are interested in

BROADENING THE SCOPE OF WHAT SORT OF CONTEXT WE ARE INTERESTED IN

Whe can receive our data? What can they do with it?
 Data accuracy, source reliability
 Why is this data relevant to out?
 What can be which is behind it, what tools were used?
 What sort of medications are we dealing with? Who are the targets?
 What can we block/detact/remediate the stack?
 What sort dimeat are we dealing with?

- Who can receive our data? What can they do with it?
 Data accuracy, source reliability
- Why is this data relevant to us?
- Who do we think is behind it, what tools were used?
- What sort of motivations are we dealing with? Who are the targets?
- How can we **block/detect/remediate** the attack?
- What sort of **impact** are we dealing with?

PARALLEL TO THE CONTEXTUALISATION EFFORTS: FALSE POSITIVE HANDLING

- Low quality / false positive prone information being shared
- Lead to alert-fatigue
- Exclude organisation xy out of the community?
- False positives are often obvious **can be encoded**
- Warninglist system¹ aims to do that
- Lists of well-known indicators which are often false-positives like RFC1918 networks, ...

LIST OF KNOWN IPV4 PUBLIC DNS RESOLVERS

ld	89	
Name	List of known IPv4 public DNS resolvers	
Description	Event contains one or more public IPv4 DNS resolvers as attribute with an IDS flag set	
Version	20181114	Warning: Potential false positives
Туре	string	·····
Accepted attribute types	ip-src, ip-dst, domainjip	List of known IPv4 public DNS resolvers
Enabled	Yes (disable)	
Values		Top 1000 website from Alexa
1.0.0.1		List of known google domains
1.1.1.1		
1.11.71.4		

Turning data into actionable intelligence

80

6

2024

Parallel to the contextualisation efforts: False positive handling

PARALLEL TO THE CONTEXTUALISATION EFFORTS: FALS POSITIVE HANDLING

Lon quality / fabs packing spons information being shared
 Locate to alter / default
 Locate to alter / default

¹https://github.com/MISP/misp-warninglists

More complex data-structures for a modern age

- Atomic attributes were a great starting point, but lacking in many aspects
- MISP objects² system
 - Simple **templating** approach
 - Use templating to build more complex structures
 - Decouple it from the core, allow users to define their own structures
 - MISP should understand the data without knowing the templates
 - Massive caveat: Building blocks have to be MISP attribute types
 - Allow relationships to be built between objects

Turning data into actionable intelligence

More complex data-structures for a modern age

More complex data-structures for a modern ag

- Atomic attributes were a great starting point, but lacking i many aspects
 MISP objects² system
- MISP objects' system
 Simple templating approact
- Use templating to build more complex structures
 - Decouple it from the core, allow users to define their own structures
 - MISP should understand the data without knowing the templates
 - Massive caveat: Building blocks have to be MISP attribute types
 - Allow relationships to be built between objects

²https://github.com/MISP/misp-obje

²https://github.com/MISP/misp-objects

80

SUPPORTING SPECIFIC DATAMODEL

+ Date	Org	Calegory	Type	File Network Financial Proposal Value	Correlation Warnings Include Tags	deleted attributes Galaxies	Show context fields Comment	Q Correla	ate Related Events
2018-09-28		Name: bank-acco. References: 0 🖸	m#						
2018-09-28		Other	status-code: text	A - Active		Add			
2018-09-28			report-code: text	STR Suspicious Transaction Report		Add			
2018-09-28		Other	personal-account-type: text	A - Business		Add			
2018-09-28		Financial fraud	swift: bic	HASEHKHH		Add		2	3849 11320 11584
2018-09-28			account: bank-account-nr	788796894883		Add			
2018-09-28		Other	account-name: text	FANY SILU CO. LIMITED		Add			
2018-09-28			currency-code: text	USD		Add			

CHARGE CONCOMPOSITION FORMATION OF CONTRACT OF CONTRAC

Turning data into actionable intelligence

└─Supporting specific datamodel

 1844	A load frank fra	a tunto futur Nel	Colored States Tax and St.		And then
 -	1.50			0	
		•			
	-				
	 -	X	Contract on the local		



08

CONTINUOUS FEEDBACK LOOP

Turning data into actionable intelligence

Continuous feedback loop

- Data ingested by MISP was in a sense frozen in time
 We had a creation data, but lacked a way to use the output
- we had a creation data, but lacked a way to use the output of our detection
- Lead to the introduction of the Sighting system
 The community could sight indicators and convey the time of the system
- The community could sign indicators and convey the time of sighting
 Potentially powerful tool for IoC lifecycle management.
- Potentially powerful tool for IoC inccycle managemen clumsy query implementation default

- Data ingested by MISP was in a sense frozen in time
- We had a creation data, but lacked a way to use the output of our detection
- Lead to the introduction of the **Sighting system**
- The community could sight indicators and convey the time of sighting
- Potentially powerful tool for IoC lifecycle management, clumsy query implementation default

∞

SUPPORTING SPECIFIC DATAMODEL

Ev	ents				
	No	Sightin CIRCL:	gs 2 (2017-03-19 16:17:59)		C
	No	Innent	(2/0/0)	/	C
	No	Inherit	ı& iĢ ≯ (0/ <mark>0/0</mark>)		C
Tags		+			
Date		2016-02-24			
Threat Leve	el	High			
Analysis		Initial			
Distribution	1	Connected co	ommunities		
Sighting) Details	freetext test No			
MISP: 2 CIRCL: 2		4 (2) - restricte	ed to own organisation only.		

Turning data into actionable intelligence

└─Supporting specific datamodel

	verse				
•	NO	CIRCL	2 (2017-03-19 16:17:59)		
۵	790		P#1	_/	
۰	760	interf	4 0 0 (140)		
Taga					
Oute		2015-10-14			
TreatLe	101	High			
Analysis		initial			
Oatributio		Connected of	ummunideo		
Signal	g Cetalo	heriert.hed			
M1071		4 (k) - sobie	led to own organization only.		
CRO		- Dancelor			

08

MAKING USE OF ALL THIS CONTEXT

2024-07-08

Turning data into actionable intelligence

└─Making use of all this context

Most obvious goal: Improve the way we query data

- Unified all export APIs
 Incorporate all contextualisation options into API filters
- Incorporate all contextualisation options into API filters
 Allow for an on-demand way of excluding potential false
- positives
 Allow users to easily build their own export modules feed

Most obvious goal: Improve the way we query data

- Unified all export APIs
- Incorporate all contextualisation options into API filters
- Allow for an on-demand way of excluding potential false positives
- Allow users to easily **build their own** export modules feed their various tools

EXAMPLE QUERY

/attributes/restSearch

```
"returnFormat": "netfilter",
"enforceWarninglist": 1,
"tags": {
  "NOT":
    "tlp:white",
    "type:OSINT"
  1,
  "OR":
    "misp-galaxy:threat-actor=\"Sofacy\"",
    "misp-galaxy:sector=\"Chemical\""
  ј,
```

Turning data into actionable intelligence

Example query

07-08

2024-

attributes/restReach "return/armat": "neffiter", "enforestarningist": 1, "top: Outr" "top: Outr" "ming-galaxy:sectors\"Sofacy\" 1, 1,

SYNCHRONISATION FILTERS

Turning data into actionable intelligence

—Synchronisation filters

- Make decisions on whom to share data with based on
- MISP by default decides based on the information creator
- decision who data gets shared with Community hosts should be able to act as a safety net for
 - Push filters what can I push?
 - Pull filters what are I interested in?

- Make decisions on whom to share data with based on context
 - MISP by default decides based on the information creator's decision who data gets shared with
 - Community hosts should be able to act as a safety net for sharing
 - Push filters what can I push?
 - Pull filters what am I interested in?
 - **Local tags** allow for information flow control

22

80

THE EMERGENCE OF ATT&CK AND SIMILAR GALAXIES

Standardising on high-level TTPs was a solution to a long list of issues

- Adoption was rapid, tools producing ATT&CK data, familiar interface for users
- A much better take on kill-chain phases in general
- Feeds into our filtering and situational awareness needs extremely well
- Gave rise to other, ATT&CK-like systems tackling other concerns
 - attck4fraud ³ by Francesco Bigarella from ING
 - **Election guidelines** ⁴ by NIS Cooperation Group

³https://www.misp-project.org/galaxy.html#_attck4fraud ⁴https:

//www.misp-project.org/galaxy.html#_election_guidelines

Turning data into actionable intelligence

∞

Ģ

2024

—The emergence of ATT&CK and similar galaxies

THE EMERGENCE OF ATT&CK AND SIMILAR GALAXIE

- Standardising on high-level TTPs was a solution to a long lis of issues
 Adoption was rapid, tools producing ATT&CK data, familiar
- Adoption that rapid, cools producing at racic data, initial interface for users
 A much better take on kill-chain phases in general
- Feeds into our filtering and situational awareness needs extremely well
- Gave rise to other, ATT&CK-like systems tackling other concerns

 Attacksfraud > by Francesco Bigarella from ING

³https://www.misp-project.org/galaxy.html#_attcksfraud ⁴https: EXAMPLE QUERY TO GENERATE ATT&CK HEATMAPS

```
/events/restSearch
```

```
"returnFormat": "attack",
"tags": [
    "misp-galaxy:sector=\"Chemical\""
],
"timestamp": "365d"
```

Turning data into actionable intelligence

07-08

2024-

Example query to generate ATT&CK heatmaps

/events/restSear

"returnFormat": "attack",
"tags": [
 "misp-galaxy:sector=\"Chemical\""
],
"timestamp": "t65d"

A SAMPLE RESULT FOR THE ABOVE QUERY

Turning data into actionable intelligence

08

2024-07

└─A sample result for the above query

100.000	Concession in which the		-	_	 _		-		THE R OWNER WHEN
-			And and Address of the Owner, where the	No. of Street, or other	 Terrary Inc.	-	And a state of the local division of the loc	TTO IL	And the other Designment of the local division of the local divisi
100						Automatical States		Arrist Au	
	in hans		Address of the local division of the local d		-				
Statement in the									
		Name of Street, Street					Not here		
00. Aug A.	are not a				And in case of				
				-					

Pre Attack - Attack Pattern	Enterprise Attack - Atta	ck Pattern Mobile Attack	- Attack Pattern					0		11 💆 🏹 Show a
Initial access	Execution	Persistence	Privilege escalation	Defense evasion	Credential access	Discovery	Lateral movement	Collection	Exfiltration	Command and control
Spearphishing Atachment	Scripting	Screensaver	File System Permissions Weakness	Process Hollowing	Securityd Memory	Password Policy Discovery	AppleScript	Data from Information Repositories	Extitution Over Alternative Protocol	Standard Application Layer Protocol
Spearphishing via Service	Command-Line Interface	Login Item	AppCert DLLs	Code Signing	Input Capture	System Network Configuration Discovery	Distributed Component Object Model	Data from Removable Media	Extituation Over Command and Control Channel	Communication Through Removable Media
Trusted Relationship	User Execution	Trap	Application Shimming	Rootkit	Bash History		Pass the Hash	Man in the Browser	Data Compressed	Custom Command and Control Protocol
Replication Through Removable Media	Regsvcs/Regasm	System Firmware	Scheduled Task	NTFS File Attributes	Exploitation for Credential Access	Network Share Discovery	Exploitation of Remote Services	Data Staged	Automated Extilitation	Multi-Stage Channels
Exploit Public-Facing Application		Registry Run Keys / Start Folder	Startup Items	Exploitation for Detense Evasion	Private Keys	Peripheral Device Discovery	Remote Desktop Protocol	Screen Capture	Scheduled Transfer	Remote Access Tools
	Windows Management Instrumentation	LC_LOAD_DYLIB Addition	New Service	Network Share Connection Removal	Brute Force	Account Discovery	Pass the Ticket	Email Collection	Data Encrypted	Uncommonly Used Port
Valid Accounts	Service Execution	LSASS Driver	Sudo Caching	Process Doppelgänging	Password Filter DLL	System Information Discovery	Windows Remote Management	Clipboard Data	Exfiltration Over Other Network Medium	Multilayer Encryption
Supply Chain Compromise	CMSTP	Rc.common	Process Injection	Disabling Security Tools	Two-Factor Authentication Interception	System Network Connections Discovery	Windows Admin Shares	Video Capture	Exfiltration Over Physical Medium	Domain Fronting
Drive-by Compromise	Control Panel Items	Authentication Package	Bypass User Account Control	Timestomp	LLMNR/NBT-NS Poisoning	Network Service Scanning	Remote Services	Audio Capture	Data Transfer Size Limits	Data Obluscation
Hardware Additions	Dynamic Data Exchange	Component Firmware	Extra Window Memory Injection	Modily Registry	Credentials in Files	File and Directory Discovery	Taint Shared Content	Data from Network Shared Drive		Connection Proxy
	Source	Windows Management Instrumentation Event Subscription	Setuid and Setgid	Indicator Removal from Tools	Forced Authentication	Security Software Discovery	Application Deployment Software	Data from Local System		Commonly Used Port
	Space after Filename	Change Default File	Launch Daemon	Hidden Window	Keychain	System Service Discovery	Third-party Software	Automated Collection		Data Encoding

MONITOR TRENDS OUTSIDE OF MISP (EXAMPLE: DASHBOARD)



Turning data into actionable intelligence

-08

Monitor trends outside of MISP (example: dashboard)





DECAYING OF INDICATORS

Turning data into actionable intelligence

∞

-0

2024-

—Decaying of indicators

DECAYING OF INDICATOR

- We were still missing a way to use all of these systems in combination to decay indicators
- Move the decision making from complex filter options to complex decay models
- Decay models would take into account various taxonomies, sightings, the type of each indicator Sightings and Creation date.
- The first iteration of what we have in MISP now took:
 - 2 years of research
- 3 published research pap
 A lot of prototyping

- We were still missing a way to use all of these systems in combination to decay indicators
- Move the decision making from complex filter options to complex decay models
- Decay models would take into account various taxonomies, sightings, the type of each indicator Sightings and Creation date
- The first iteration of what we have in MISP now took:
 - 2 years of research
 - 3 published research papers
 - A lot of prototyping

SCORING INDICATORS: OUR SOLUTION

Turning data into actionable intelligence

∞

2024-07

└─Scoring Indicators: Our solution

SCORING INDICATORS: OUR SOLUTION

ore(streams) = base_score(streams, most) . decay(most, to

- Where,
- score ∈ [0, 100]
- **a** base_score \in [0, 100]
- decay is a function defined by model's parameter controlling decay speed
- Attribute Contains Attribute's values and metadat (Incomplete Contains)
- Model Contains the Model's configuration

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

Where,

- **score** \in [0, 100]
- **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

IMPLEMENTATION IN MISP: Event/view

2+															
ríous ni	« tro	view all													
= 1				-										Enter value to search	Q X
tet (Drg	Category	Туре	Value	Tags	Galaxies	Comment	Correlate			S Distribution	Sightings	Activity	Score	Actions
19-09-12		Network activity	ip-src	5.5.5.5	⊗ + ≗ +	🚱 + 🚨 +					Inherit	697		NIDS Simple Decaying 65.26	• • •
												(uuro)		Model 5 79.88	
19-08-13		Network activity	lp-src			8+ 🛓+					Inherit	691	LLL.	NIDS Simple Decaying 54.6	•
					▼ retendoncexpired × ♥+ ≥+				11 more	11.2		(5000)		Model 5 52.69	
19-08-13		Network activity	lp-src			<u> </u>		×		1:1 @	Inherit	001	MLL.	NIDS Simple Decaying 37.43	• 1 2
					Image: contract of level compactory.contractory Image: contract of level compactory.contractory Image: contract of level compactory.contractory				Show 6 more			(410)		Model 5 0	
						3 · · ·						691			
	9-09-12 9-08-13	e † Org 9-09-12 9-08-13	e T Org Category 9-09-12 Network activity 9-08-13 Network activity	E E Scope toget + Cig Category Type Org Category Type Sol-12 Network activity (p-sec	E M Scope togget * E One t Org Calegory Type Value 30512 Network activity (p-ac: 55.55 Scope 100,000 B.B.B.B. 30513 Network activity (p-ac: 55.55 A	E 26 Stopp tagge Extend to the point of the po	E M Except bugge Extend into Except source Control Contro Control	Corporation in the second	2 Notices log(s* 1 October) 2 Course same Quarters 2 Network log(s* 1 Tellings same Quarters 2 Network log(s* 1 Tellings same Quarters Zellings Zelling Zelling	Image: Source activity Desired Mathematical activity Operation Training activity Tr	E Stopp bogs + Divide: If Zimony www O Control * Totalistic Topp Totalististic Topp <thtop< th=""> Topp</thtop<>	Image: Solution of the solution	Image: State Support support Database Database <thdatabase< th=""> Database Da</thdatabase<>	Image: State State Image: State State State Image: State State State Image: State State State Image: State State State State Image: State State Image: State St	

Decay score toggle button

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

Turning data into actionable intelligence

2024-07-08

└─Implementation in MISP: Event/view

-											
				-							
				-				100			
	-		1919	12/10			217				
			Summer of the local diversion of the local di	- 20			27				
		1					227		And Co.	-	
	1041.416		Second party			-				**	
				12/10			227				

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

IMPLEMENTATION IN MISP: API RESULT

```
/attributes/restSearch
"Attribute ": [
    "category": "Network activity",
    "type": "ip-src",
    "to ids": true.
    "timestamp": "1565703507",
    [...]
    "value": "8.8.8.8",
    "decay score": [
        "score": 54.475223849544456,
        "decayed": false,
        "DecayingModel": {
          "id": "85",
          "name": "NIDS Simple Decaying Model"
```

Turning data into actionable intelligence

∞

2024

└─Implementation in MISP: API result

/Artholies/mediarth //Ittalies/mediarth //Ittalies///Ittalies/ *opsil//istalies/ *opsil//istalies/ *opsil//istalies/ *opsil//istalies/ *opsil/istalies/ *opsil/istalie

IMPLEMENTATION IN MISP: INDEX

Decaying Models

« previous next »

Polynomial		9	1	~	
Polynomial ©	Polynomial •	13	1	~	⊞ & ⊘ Ш

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

Turning data into actionable intelligence

08

2024-07

Implementation in MISP: Index

	nying M	odela						
2								
	-	1001	-	The state of the s	frame (***	
			-	ing harpen at the set of the set of the set (as a set of the set (as a set of the set of				
-		-	Adaptatic Lange I					

IMPLEMENTATION IN MISP: FINE TUNING TOOL

	Dec	aying Of Indicator I	ine	Tuning Tool																	
ecoying Model	II Sho	w All Types B Show MISP Objects	Searc	in Attribute Type	5		Polyno	mial		T 😡											
		Attribute Type		Category	Model ID	î	100	1													
caying Models		aba rhi		Financial traud			90														
		authentihash		Payload delivery			60														
		bank-account-re		Financial traud		Т	71	1 1													
		bic		Financial fraud			60														
		bin		Financial fraud) 54 4				<										
		bro		Network activity	10 11							-						_			
		btc		Financial haud	11		21														
		cc-number		Financial fraud			31														
	0	odhash		Payload delivery						0.5	1.0		1.5		2.0	2.5		20			
	8	community-id		Network activity				0.0		0.5	10		Days		20			8.0			
		domain		Network activity			Life	time :	3				days	Expir	atter ölletime			1 days a	nd 7 hou	5	
	8	domainijo		Network activity	10.84		Decay	speed 3	2.3					Scon	halved after ()	falf-Me)		0 day an	d 6 hours		
	8	domain(p email-attachment		Network activity Phylicad delivery	10.84									Scon	halved after ()	talf-life)			d 6 hours		
				Poyload delivery Network activity	10.84		Cutoff t	neshold 3	90					Score	halved after (falf-life)			d 6 hours		
	8	emailattachment		Payload delivery			Cutoff t		90	Et Sina	Late this mod				halved after (t	1af-life)			d 6 hours		
	0	enal-atachment enal-dit	1 1 1	Poyload delivery Network activity			Cutoff t	unt band so	90	Et Sina	ate this med		ocay *		halved after ()	sat-lite)			d 6 hours		
	0	enal atachment email.dx email.oc		Payload delivery Network activity Payload delivery			Cutoff ti	neshold : ant base no g model	30 are 2	Et Sina	ple model to	rapidly d			halved after ()	taif-life)			d 6 hours		
		enal-attachment email-dat email-soc tilesanne	x x x x	Payload delivery Network activity Payload delivery Payload delivery			Cutoff ti	neshold : ant base no g model	30 are 2	Sirra	ple model to	rapidly d			halved after ()	falf-life)			d 6 hours		
		enal-attachment emal-dit emal-sic Elename Elename[authenthach	T T T T T	Payload delivery Network activity Payload delivery Payload delivery Payload delivery			Cutoff th Ad Phishin	g model available n Medel	are E	Sir	iple model to	napidiy d at models Perenete	rs Decay	Ø Edit	Default			0 day an	,		
		enal atachner. enal ata dit enal ata Besarte Besarte Besarte/phazy Besarte/phazy	T T T T T T	Payload delivery Network activity Payload delivery Payload delivery Payload delivery			Cutoff ti Ad Phishin O Al D	g model available n available n Nedel Name	ane E	© My mode	iple model to is @ Defai	i rapidly d it models Paramete Lifetime	Decay	Eda Threshold	Default basescore	Basescore con		0 day an	,	Enabled	
		enal-atachmerk enal-doc enal-doc enal-doc Elesame Elesame/authenthoch Elesame/authenthoch Elesame/authenthoch Elesame/authenthoch		Phylical delivery Network activity Phylical delivery Phylical delivery Phylical delivery Phylical delivery	11		Cutoff ti Ad Phishin O Al D	g model available n Medel	are E	Sir	iple model to	i rapidly d it models Paramete Lifetime	Decay speed	Ø Edit	Default	Basescore con	fig 5	0 day an	,		lation Lastmodel

Create, modify, visualise, perform mapping

Turning data into actionable intelligence

2024-07-08

Implementation in MISP: Fine tuning tool



IMPLEMENTATION IN MISP: base_score TOOL

Default basescore 80 Taxonomies admiratty-scale + source-reliability +	Weight						
admiralty-scale + source-reliability +	Weight						
source-reliability -							
	Ξ	31					
information-credibility ~		30					
priority-level *							
priority-level -	=	53		admirally-scale source-reliability (27%)			
retention *							
retention -	1	0					
estimative-language ~							
likelihood-probability -		0					
confidence-in-analytic-judgment -	1	0					
misp -							
confidence-level -	8	0					
threat-level -		0		Placeholder for 'Organisation	source confidence'		
automation-level -		0	Example	ø			
phishing -				_			Base
state -	=	0	Attribute Tag your	Tags			score
psychological-acceptability -	1	0	attribute	-			
Excluded A			Attribute 1	admiralty-scale:information-credibility="5"			0.0
			Attribute 2	priority-level:baseline-minor admiralty-sca admiralty-scale:information-credibility="2"	le:source-reliability=	"d"	38.2 🕤
			Attribute 3	priority-level:severe admiralty-scale:inform	nation-credibility="2"		84.6 😧
			Computa	ation steps			
					Comp	utation	
			Tag		Eff. Ratio	Value	Result
			priority-lev	rel:baseline-minor	0.46	* 25.0	
			admiralty-	scale:source-reliability="d"	0.27	* 25.0	0 6.80

Turning data into actionable intelligence

LImplementation in MISP: base_score tool



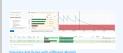
80

2024

IMPLEMENTATION IN MISP: SIMULATION TOOL

Turning data into actionable intelligence

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 0 "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-src 8.8.8.8 admiralty-scales V III NIDS 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

-08

IMPLEMENTATION IN MISP: API QUERY BODY

/attributes/restSearch

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

Turning data into actionable intelligence

Implementation in MISP: API query body

IMPLEMENTATION IN MISP: API QUERY BODY

/attributes/restSearch

fincludeDecayScoref: 1, fincludeFullModel1: 0, mexcludeDecayed1: 0, decayingModel1: [85], modeOlverride51: { threshold1: 30 } scoref: 30,

2024-07-08

TO SUM IT ALL UP...

Turning data into actionable intelligence

└─To sum it all up...

80

2024-07

- Massive rise in user capabilities
- Growing need for truly actionable threat intel
 Lessons learned:
- Context is king Enables better decision making
 Intelligence and situational awareness are natural
 - by-products of context
- Don't lock users into your workflows, build tools that enable theirs

Massive rise in user capabilities

Growing need for truly actionable threat intel

Lessons learned:

- Context is king Enables better decision making
- Intelligence and situational awareness are natural by-products of context
- Don't lock users into your workflows, build tools that enable theirs

GET IN TOUCH IF YOU HAVE ANY QUESTIONS

Turning data into actionable intelligence

Get in touch if you have any questions

Contact us

- https://twitter.com/mokaddem_sa https://twitter.com/islorcka
- https://twitter.com/igloc
 Contact CIRCL
- info@circLlu
- https://twitter.com/circl_l https://www.circl.lu/
- Contact MISPProject
- https://github.com/MISP https://gittup.im/MISP/M
- https://gitter.im/MISP/MISP https://twitter.com/MISPProje

Contact us

- https://twitter.com/mokaddem_sami
- https://twitter.com/iglocska

Contact CIRCL

- ▶ info@circl.lu
- https://twitter.com/circl_lu
- https://www.circl.lu/

Contact MISPProject

- https://github.com/MISP
- https://gitter.im/MISP/MISP
- https://twitter.com/MISPProject

∞